FIELD MANUAL
NO 34-40-2

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 13 September 1990

BASIC CRYPTANALYSIS

TABLE OF CONTENTS

PART ONE ● INTRODUCTION TO CRYPTANALYSIS

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This determination was made on 5 March 1990. Other requests for this document will be referred to Commander, United States Army Intelligence School, Fort Devens, ATTN: ATSI-ETD-PD, Fort Devens, MA 01433-6301.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

*This publication supersedes TM 32-220, 20 August 1970.

PART TWO ● MONOGRAPHIC SUBSTITUTION SYSTEMS

PART THREE ● POLYGRAPHIC SUBSTITUTION SYSTEMS

PART FOUR ● POLYALPHABETIC SUBSTITUTION SYSTEMS

PART FIVE ● TRANSPOSITION SYSTEMS

PART SIX ● ANALYSIS OF CODE SYSTEMS

INTRODUCTION

This manual presents the basic principles and techniques of cryptanalysts and their relation to cryptography. Cryptography concerns the various ways of protecting messages from being understood by anyone except those for whom the messages are intended. Cryptographers are the people who create and use codes and ciphers. Cryptanalytics is the art and science of solving unknown codes and ciphers. Cryptanalysts try to break the codes and ciphers created and used by cryptographers.

This publication is organized into six parts. Part One explains basic principles which apply to all the parts that follow. The following five parts each cover a major type of system and the cryptanalytic techniques that apply to it. Parts Two, Three, and Four each build on the techniques explained in the parts that precede them. A new student should study these in order. Parts Five and Six are largely independent of Parts Two through Four and can be used separately after Part One.

For practice in the techniques explained in this manual, the Army Correspondence Course Program offers a course in basic cryptanalysts. See the References Section at the back of this manual for further information.

PREFACE

This field manual is intended as a training text in basic cryptanalytics and as a reference for cryptanalysts in military occupational specialty (MOS) 98C and related MOSs.

The proponent of this publication is Headquarters, United States Army Training and Doctrine Command (TRADOC). Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, United States Army Intelligence School, Fort Devens (USAISD), ATTN: ATSI-ETD-PD, Fort Devens, MA 01433-6301.

PART ONE

Introduction to Cryptanalyst

CHAPTER 1

TERMINOLOGY AND SYSTEM TYPES

Section I
Basic Concepts

1-1. Cryptology

Cryptology is the branch of knowledge which concerns secret communications in all its aspects. Two major areas of cryptology are *cryptography* and *cryptanalytics.*

1-2. Cryptography

Cryptography is the branch of cryptology concerned with protecting communications from being read by the wrong people. Codes and ciphers that are used to protect communications are called cryptographic systems. The application of codes and ciphers to messages to make them unreadable is called encryption. The resulting messages are called cryptograms. The people who create and use cryptographic systems are called cryptographers.

1-3. Cryptanalytics

Cryptanalytics is the branch of cryptology concerned with solving the cryptographic systems used by others. The objects of cryptanalysts are to read the text of encrypted messages and to recover the cryptographic systems used. The text is recovered for its potential intelligence value. The systems are recovered for application to future messages in the same or similar systems.

1-4. Signal Communications

In military applications most encrypted messages are sent by electronic means rather than physically carried or mailed. The electronic means include those sent by wire and those transmitted by radio. Whether wire or radio is used, they can be sent by telephone, telegraph (Morse code), teletypewriter, facsimile, or computer. The electronic means provide greater speed than physical means, but make the communications more vulnerable to intercept by others.

Section II
Cryptographic Systems

1-5. Ciphers and Codes

There are two major categories of cryptographic systems, called ciphers and codes. Nearly all military systems fall into one or the other of these categories or a combination of the two. Cipher systems are those in which the encryption is carried out on single characters or groups of characters without regard to their meaning. Codes, on the other hand, are more concerned with meanings than characters. The basic unit of encryption in a code system is a word or phrase. When a message is encrypted by a code system, code groups primarily replace words and phrases. Code groups may also replace single characters where necessary, but the substitution for complete words is the key distinction that separates a code from a cipher. Because of this, the cryptanalytic approaches to codes and ciphers are quite different from each other.

a. Messages encrypted by a cipher system are said to be enciphered. Similarly, messages encrypted by a code system are encoded. The resulting text is called ciphertext or code text. When a cryptogram is translated back into readable form or *plaintext,* it is said to be decrypted, or more specifically, decoded or deciphered.

b. The term code in this manual is given the formal meaning as explained above and in more detail in Part Six. You will often see and hear the term *code* used with other meanings that do not apply here. Code, in its more general sense, can mean any cryptographic system or any system of replacing one set of values with another. The terms Morse code, binary code, Baudot code, and computer code are examples of the more general usage of the term.

1-6. Enciphered Codes

Some code systems are further encrypted by a cipher system to produce a hybrid type called enciphered codes. This second encryption process is called superencryption or superencipherment. Such systems are normally much more secure than singly encrypted systems, but because of the added complexity take longer to encrypt and are more prone to errors.

1-7. Other Means of Security Communications

Although most military requirements to secure communications are met through the use of codes and ciphers, there are other approaches that can be used in special situations. One such approach is the use of concealment systems. In a concealment system, the plaintext is hidden within another longer text by a predetermined rule or pattern. Other approaches to concealing messages are to use invisible inks or to reduce a message photographically to a dot-sized piece of film. Another approach is to transmit a message from a tape played so fast that it sounds to the ear like a burst of static on the radio. Security for all these methods depends on concealing the fact that a secret message is being sent at all. Once the existence of the communications is suspected or anticipated, the security is significantly lessened.

1-8. Types of Ciphers

There are hundreds of types of cipher systems ranging from very simple paper-and-pencil systems to very complex cipher machine or computer enciphered systems. These can be categorized as either transposition or substitution or a combination of the two.

a. **Transposition.** In a transposition system, the plaintext characters of a message are systematically rearranged. After transposing a message, the same characters are still present, but the order of the letters is changed.

b. **Substitution.** In a substitution system, the plaintext characters of a message are systematically replaced by other characters. After the substitution takes place, the order of the underlying plaintext is unchanged, but the same characters are no longer present. In the simplest substitution systems, the replacement is consistent; a given plaintext character always receives the same replacement character or characters. More secure systems change the replacements so that the equivalents change each time the same character is encrypted.

1-9. Substitution Cipher Alphabets

In everyday usage, an alphabet is a list of the letters used by a language. They vary by language. Many European and Latin American languages share the same alphabet as ours or have minor variations. Russian, Greek, Arabic, and Oriental languages have recognizably different alphabets. The term *cipher alphabets* has a slightly different meaning. Instead of a list of characters, a cipher alphabet has two parts; a list of plaintext characters and their cipher equivalents. In the simplest ciphers, an English cipher alphabet will have 26 plaintext letters and 26 ciphertext equivalents, as in the example below.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W

p: send help
c : BLMI ULGS

In the example, *p:* designates plaintext and *c:* designates ciphertext. For clarity, the plaintext is shown in lower case and the ciphertext in capitals. A more secure alphabet may have more ciphertext equivalents than plaintext characters to provide for some variation in encipherment. Whether or not there is variation, a single alphabet system is called a *monoalphabetic* system. A system which gains more security by systematically using more than one alphabet is called a *polyalphabetic* system.

CHAPTER 2

SECURITY OF CRYPTOGRAPHIC SYSTEMS

Section I
Requirements of Military Systems

2-1. Practical Requirements

Military cryptographic systems must meet a number of practical considerations.

a. An ideal cryptographic system for military purposes is a single all-purpose system which is practical for use from the highest headquarters to the individual soldier on the battlefield. It is secure no matter how much message traffic is sent using the system. It is easy to use without special training. It presents no logistics problems in keeping the users supplied with the system's keys. It operates under all weather conditions, on all means of communication, and in the dark. Little of value is compromised if the enemy captures the system. No system exists that meets all these requirements.

b. Cryptographic system selection for military use depends on much more than its degree of security. While protecting information from unfriendly eyes, a system must still allow communications to take place rapidly, to be reliable, and to be usable by all who need to conduct communications. It must be usable under all conditions that the communications must take place. For example, a system requiring an hour of pains-taking encryption would go unused by a combat military force on the move. A system that has no tolerance for errors in its use would be inappropriate for soldiers under fire in severe weather conditions. A system that only supports a low volume of messages would be inappropriate for a major message center handling thousands of messages daily. A system that requires expensive, sophisticated equipment would be inappropriate for a military force that can barely afford to buy ammunition. No single system meets all the requirements of security, speed, reliability, flexibility, and cost. The need for security must be balanced against the practical requirements when systems are selected for use. Breakable systems are found today, despite technological advances, because of these practical requirements.

2-2. Security Requirements of Military Systems

When security must be balanced against practical considerations, how much security is enough security?

a. Almost any cryptographic system, given enough time and resources can eventually be solved. The only exception to this is a system which uses absolutely random changing keys with every character encrypted and never repeated. Such a system can be achieved under very limited conditions, but is in practice impossible on any large scale.

b. Even the most sophisticated machine or computer based cryptographic system cannot produce random, nonrepeating keys. The requirement for each communicating machine to generate the same keys prevents truly random keys. At best, a machine system can produce keys by so sophisticated a process that it appears to be random and resists efforts to recover the key generation process.

c. Given the practical considerations, a military system is expected to delay successful analysis, not prevent it. When the system is finally solved, the information obtained has lost most of its value.

2-3. Factors Affecting Cryptographic Security

As discussed above, given enough time and resources, almost any system can be solved. No nation has unlimited resources to devote to the effort. If the potential intelligence payoff is timely enough and valuable enough and the resource costs reasonable, the necessary resources will usually be devoted to the effort. A number of factors affect the vulnerability of cryptographic systems to successful cryptanalytic attack.

a. The most obvious factor is the cryptographic soundness of the system or systems in use. Systems with minimal key repetition and limited orderly usage patterns provide the most resistance.

b. The volume of traffic encoded or enciphered with a given set of keys affects system security. The longer the keys are used without change, the more chance an analyst has of finding exploitable repetition and patterns to build the attack upon.

c. The discipline of system users can play a major role in system security. A system that is very sound when used correctly can often be quickly compromised when rules are broken. An obvious example is when a user retransmits a message in the clear that has also been transmitted in encrypted form. When it is recognized, the comparison of the plaintext message with its encrypted form makes key recovery much easier. Other typical examples of undisciplined usage are–

- To mix plaintext and encrypted text in the same transmission.
- To use the same keys longer than prescribed.

- To make unauthorized changes or simplifications to the system.
- To openly discuss the contents of an encrypted message.
- To openly discuss the system or its keys.

d. The amount of collateral information available about the message sender and the situation under which the message was sent affect the security of a system. The more that is known about the sender, the more likely the contents of a message can be determined.

Section II
Cryptanalytic Attack

2-4. Role of Cryptanalysts in Communications Intelligence Operations

Communications intelligence (COMINT) operations study enemy communications for the purpose of obtaining information of intelligence value. COMINT includes the collection, processing, evaluation, and reporting of intelligence information gathered from enemy communications. When cryptanalysts is successful on a timely basis, it provides the most direct indication of the enemy's intentions. Cryptanalysis is most likely to be successful when other COMINT techniques are also productive. Collection of communications signals, transmitter location and identification, traffic analysis, and translation and analysis of cleartext transmissions all play a part in the production of COMINT.

2-5. Comparison Between Cryptanalysts and Traffic Analysis

Cryptanalysis is the study of encrypted messages. These messages, when passed as part of radio communications, or traffic, are considered the internals of the communications. Traffic analysis is the study of the externals of the communications.

a. The externals of a communications include the following:

- Call signs and call words.
- Call up procedures between operators.
- Radio frequencies.
- Times of transmissions and total volume of traffic.
- Routing information indicating where a message is to be sent.

- Chatter between radio operators.
- Serial numbers or other filing information.
- Indications of precedence or importance of the messages.
- Indicators designating what cryptographic systems or what key settings are in use.

These externals can be a rich source of information about an enemy, regardless of encrypted message recovery. The systems that communicators use to provide this external information can give substantial clues to unit type, organization, and the purpose of communications.

b. The last category of externals mentioned above, indicators of the cryptographic systems or keys in use, is of particular interest to both the traffic analyst and the cryptanalyst. For the traffic analyst, the indicators help establish patterns of usage which give clues to the enemy's organization and structure. For the cryptanalyst, the indicators help group messages into those encrypted by the same system or keys. In some cases, they may even aid directly in the solution of the system.

2-6. Steps in Cryptanalysis

The solution of nearly every cryptogram involves four basic steps–

- Determination of the language used.
- Determination of the general system used.
- Reconstruction of the specific keys to the system.
- Reconstruction of the plaintext.

a. Determination of the language used normally accompanies identification of the sender through traffic analysis or radio direction finding. If these forms of support are unavailable, or if an enemy uses several languages, the determination of the language may have to be made at a later stage of analysis.

b. Determination of the general system can come from several sources, such as–

- A detailed study of the system characteristics, aided where necessary by character frequency counts, searches for repeated patterns, and various statistical tests. The study can extend beyond single messages to searching for patterns and repetitions between different messages with similar characteristics. This single step of system determination can be the most time consuming part of the analysis.
- Past history of system usage by the sender. In most cases, the user does not change systems regularly but uses the same system or set of systems from one day to the next. The specific keys may change regularly, but the general systems remain unchanged except at longer intervals.

- System indicators included with the traffic. Whenever the user has a choice of systems or a choice of keys within the system, the choice must be made known to the receiving cryptographer. The choice is usually communicated by some form of indicators, which can appear within the text of a message or as part of the externals. When the indicators reveal the choice of system, they are called system indicators or discriminants. When they denote specific frequently changing keys to the system, they are called message indicators. Once you learn just how indicators are used from day to day, they can provide a substantial assist to cryptanalysts.

c. Reconstruction of the specific keys to the system is an important step. Although the following step of plaintext recovery produces the most intelligence information, the full key reconstruction can speed recovery of future messages. The approach used to recover keys will vary greatly from system to system.

d. Reconstruction of the plaintext, although listed as the final step, will usually proceed simultaneously with the key reconstruction. Either step can come first, depending on the system and situation. Partial recovery of one aids in the recovery of the other. The two steps often proceed alternately, with each recovery of one helping in recovery of the other until a full solution is reached.

Section III
Analytic Aids

2-7. Analytic Aids to Identification and Solution

There are a number of aids to identification and solution available to help you as a cryptanalyst. By preparing character frequency counts, performing statistical tests, and recording observed repetitions and patterns in messages, you can compare the data to established norms for various systems and languages. The appendixes to this manual include charts, lists, and tables of normal data for the English language. Similar data are available for other languages. The counting of character frequencies, performance of statistical tests, and search for repetition and patterns can be done manually or with computer assistance, where available. This section outlines the aids that apply to many types of systems. Procedures that apply to specific systems are explained in individual sections.

2-8. Language Characteristics

Each language has characteristics that aid successful cryptanalysts.

a. The individual letters of any language occur with greatly varying frequencies. Some letters are used a great deal. Others are used only a small percentage of the time. In English, the letter *E* is the most common letter used. It occurs about 13 percent of the time, or about once in every eight letters. In small samples, other letters may be more common, but in almost any sample of 1,000 letters of text or more, E will be the most frequent letter. In other languages, other letters sometimes dominate. In Russian, for example, O is the most common letter. The eight highest frequency letters in English, shown in descending order, are *E, T, N, R, O, A, I* and *S*. The eight highest frequency letters make up about 67 percent of our language. The remaining 18 letters only make up 33 percent of English text. The lowest frequency letters are J, K, Q, X, and Z. These five letters makeup only a little over 1 percent of English text. The vowels, A, E, I, O, U and Y, make up about 40 percent of English text. In many cryptographic systems, these frequency relationships show through despite the encryption. The analysis techniques explained in the following chapters make repeated use of these frequency relationships. In particular, you should remember the high frequency letters, ETNROAIS, and the low frequency letters, JKQXZ, for their repeated application. The word *SENORITA,* which includes the high frequency letters is one way to remember them. Some people prefer to remember the pronounceable ETNORIAS as a close approximation of the descending frequency order. Choose the method you prefer. The high frequency letters are referred to frequently.

b. Just as single letters have typical frequency expectations, multiple letter combinations occur with varying, but predictable frequencies, too. The most common pair of letters, or digraph, is EN. After EN, RE and ER are the most common digraphs. There are 676 different possible digraphs in English, but the most common 18 make up 25 percent of the language. Appendix A lists the expected frequencies of English language digraphs. Some cryptographic systems do not let individual letter frequencies show through the encryption, but let digraphic frequencies come through. The systems explained in Part Three of this manual show this characteristic.

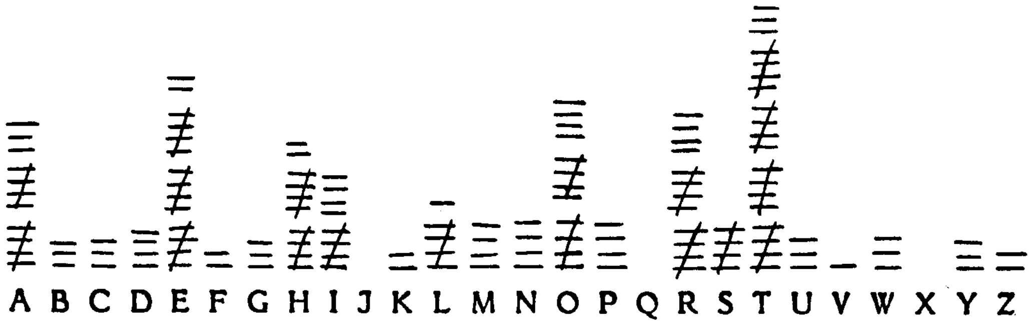
c. Appendixes B and C list frequency expectations for sets of three letters (trigraphs) and four letters (tetragraphs). Each of these can be useful when studying cryptograms in which three and four letter repeated segments of text occur.

d. Repeated segments of two to four letters will often occur because they are common letter combinations, whether or not they are complete words by themselves. Longer repeated segments readily occur when words and phrases are reused in plaintext. When words are reused in plaintext, they may or may not show up as repeated segments in ciphertext. For a word to show through as a repeat in ciphertext, the same keys must be applied to the same plaintext more than once. Even complex systems which keep changing keys will sometimes apply the same keys to the same plaintext and a repeated ciphertext segment will result. Finding such repeats gives many clues to the type of system and to the plaintext itself. The search can extend beyond single messages to all messages that you believe may have been encrypted with the same set of keys. If computer support is available to search for repeats for you, a great deal of time can be saved. If not, time spent scanning text to search for repeats will reward you for your time when you find them.

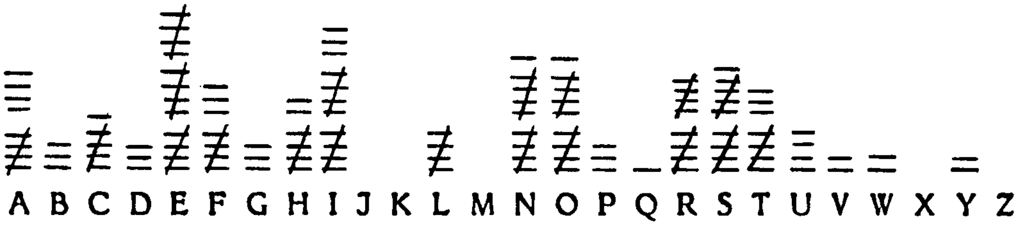
2-9. Unilateral Frequency Distribution

The most basic aid to identification and solution of cipher systems is the unilateral frequency distribution. The term unilateral means one letter at a time. A unilateral frequency distribution is a count of all the letters in selected text, taken one letter at a time.

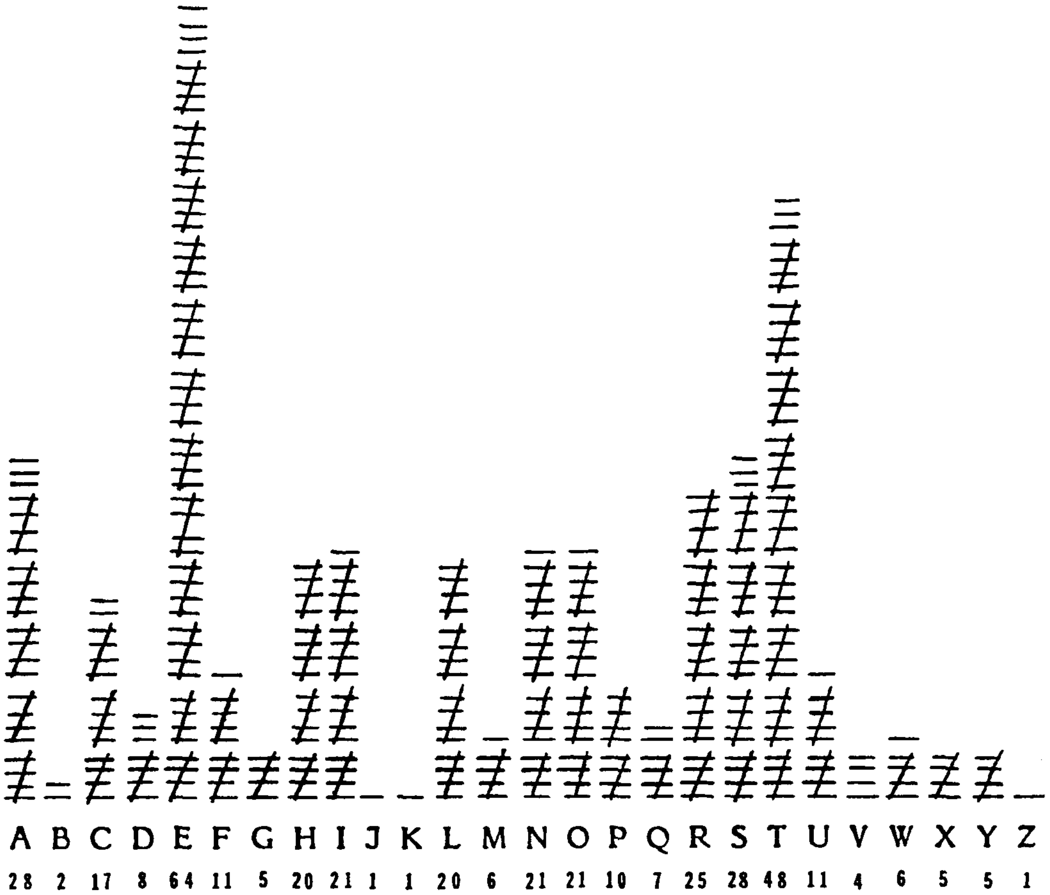
a. The customary method of taking the distribution is to write the letters A through Z horizontally and mark each letter of the cryptogram with a dash above or below the appropriate letter. Proceed through the message from the first letter to the last, marking each letter in the distribution. Avoid the alternate method of counting all the As, Bs, Cs, and so forth, which is very subject to errors. For convenience, each group of five is crossed off by a diagonal slash. The unilateral frequency distribution for the first sentence in this paragraph is shown below.



For comparison, the next example shows the frequency count for the fourth and fifth sentences in paragraph 2-9a.



b. Although individual letter frequencies differ, the pattern of high and low frequency letters is quite similar. The letters that stand above the others in each tally are, with few exceptions, the expected high frequency letters—ETNROAIS. The expected low frequency letters, JKQXZ, occur once or twice at most. Even in as small a sample as one or two sentences, expected patterns of usage start to establish themselves. Compare this to a frequency count of all letters in this paragraph.



c. When a larger sample is taken, such as the above paragraph, the letters occur much closer to the expected frequency order of ETNROAIS. As expected, E and T are the two highest frequency letters. but the next series of high frequency letters in descending order of occurrence, ASRINO, differs slightly from the expected order of NROAIS. It would take a sample thousands of letters long to produce frequencies exactly in the expected order. Even then, differences in writing style between a field manual and military message texts could produce frequency differences. For example, the word *the* is often omitted from military message traffic for the sake of brevity. More frequent use of *the* raises the expected frequency of the letter H.

2-10. Letter Frequencies in Cryptograms

As different cipher systems are explained in this manual, the ways in which letter frequencies can be used to aid identification and solution will be shown. Some basic considerations should be understood now.

a. In transposition systems, the letter frequencies of a cryptogram will be identical to that of the plaintext. A cryptogram in which the ciphertext letters occur with the expected frequency of plaintext will usually be enciphered by a transposition system.

b. In the simplest substitution systems, each plaintext letter has one ciphertext equivalent. The ciphertext letter frequencies will not be identical to the plaintext frequencies, but the same numbers will be present in the frequency count as a whole. For example, if there are 33 Es in the plaintext of a message, and if E is enciphered by the letter K, then 33 Ks will appear in the ciphertext frequency count.

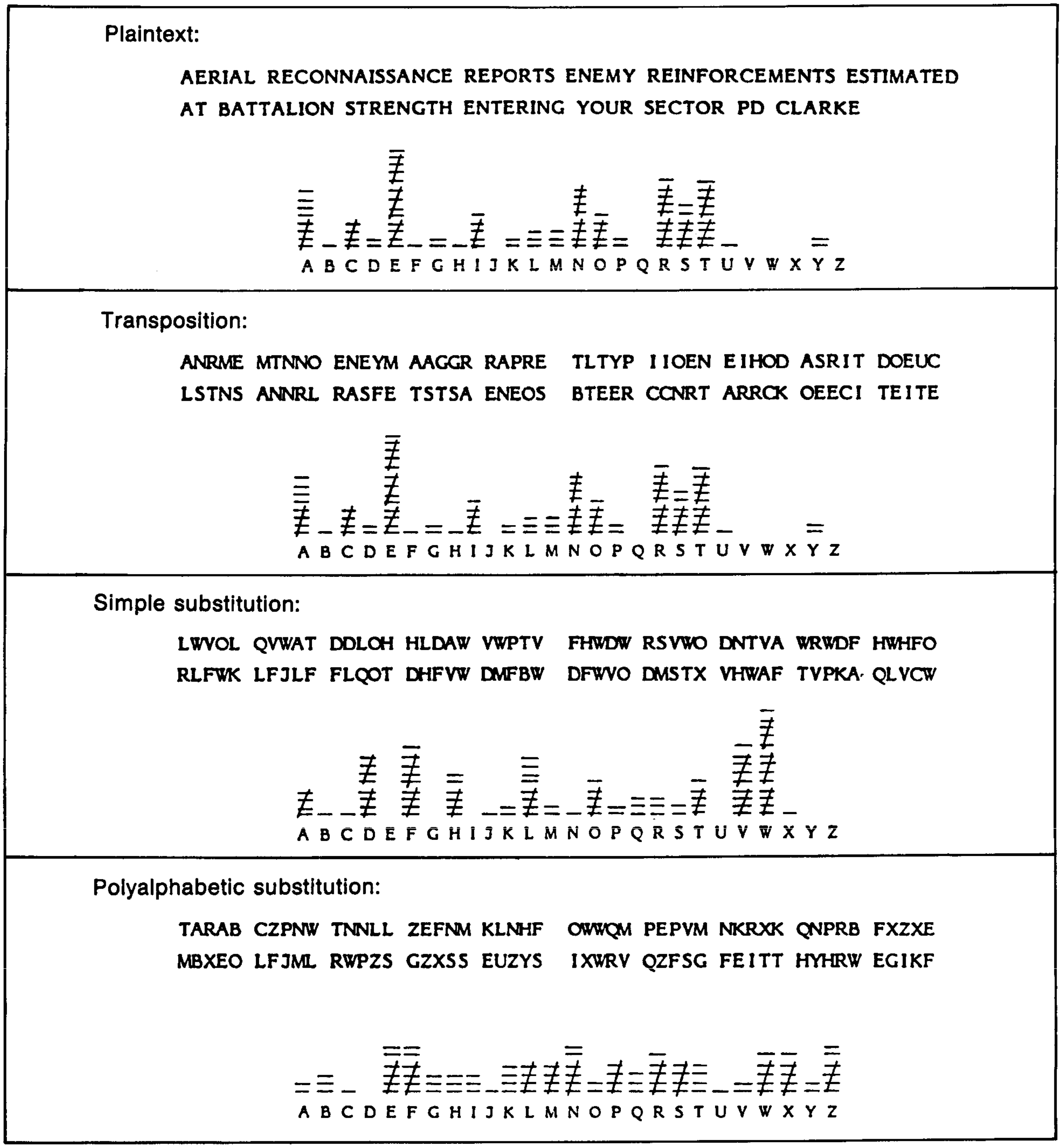
c. More complex substitution cipher systems, such as the polyalphabetic systems in Part Four of this manual, will keep changing the equivalents. E might be enciphered by a K the first time it occurs and by different cipher letters each time it recurs. This will produce a very different looking frequency count.

d. To illustrate the differences in appearance of frequency counts for different types of systems, examine the four frequency counts in Figure 2-1. Each one is a frequency count of the message listed above it. The four messages are different, but each has the same plaintext. The first shows the plaintext and its frequency count. The second shows the frequencies of the same message enciphered by a transposition system. The third shows a simple substitution system encipherment. The fourth shows a polyalphabetic substitution encipherment.

2-11. Roughness

The four examples in Figure 2-1 show another characteristic of frequency counts which is useful in system identification. The first three distributions all contain the same letter frequencies. In the first two, the plaintext and the transposition examples, there are 16 Es. In the third, where E has been replaced by W, there are 16 Ws. Where there were 9 As, there are now 9 Ls. Where there was 1 K, there is now 1 C. The first three distributions show the same wide differences between the highest frequency letters and the lowest. The fourth distribution is very different. The distribution lacks the wide differences between the highest and lowest frequency letters. Where the first three showed distinct highs and lows, or peaks and troughs, in the distributions, the fourth is relatively flat.

a. Frequency counts which show the same degree of difference between peaks and troughs as plaintext are considered to be rough distributions. Systems which suppress the peaks and troughs of plaintext letters by changing their equivalents produce flatter distributions. If letters were selected randomly from the 26 letters of the English alphabet, the resulting distribution would look very much like the fourth example. Random selection will not produce a perfectly level distribution, but it will appear quite flat in comparison to plaintext.



Plaintext:

AERIAL RECONNAISSANCE REPORTS ENEMY REINFORCEMENTS ESTIMATED
AT BATTALION STRENGTH ENTERING YOUR SECTOR PD CLARKE

Transposition:

ANRME MTNNO ENEYM AAGGR RAPRE TLTYP IIOEN EIHOD ASRIT DOEUC
LSTNS ANNRL RASFE TSTSA ENEOS BTEER CCNRT ARRCK OEECI TEITE

Simple substitution:

LWVOL QVWAT DDLOH HLDAW VWPTV FHWDW RSVWO DNTVA WRWDF HWHFO
RLFWK LFJLF FLQOT DHFVW DMFBW DFWVO DMSTX VHWAF TVPKA· QLVCW

Polyalphabetic substitution:

TARAB CZPNW TNNLL ZEFNM KLNHF OWWQM PEPVM NKRXK QNPRB FXZXE
MBXEO LFJML RWPZS GZXSS EUZYS IXWRV QZFSG FEITT HYHRW EGIKF

Figure 2-1. Frequency count comparison.

b. The simplest substitution systems tend to produce rough distributions. The most secure tend to produce flat distributions. Many other systems tend to fall in between. You can use the degree of roughness as one of the aids to system identification.

2-12. Coincidence Tests

Judging whether a given frequency distribution has the same degree of roughness as plaintext or random text is not easy to do by eye alone. To help you make this determination, a number of statistical tests have been developed for your use. The tests are based in probability theory, but you can use the tests whether or not you understand the underlying theories. The most common tests are called coincidence tests.

a. If you pick any two letters from a message, compare them together, and they happen to be the same letter, they are said to coincide. A comparison of the same letters, for example, two As is a coincidence. This comparison can be made of single letters or pairs of letters or longer strings of letters.

b. If you compare two single letters selected at random from the English alphabet, the probability of their being the same is 1 in 26. One divided by 26 is .0385. Expressed as a percentage, 1/26 is slightly less than 4 percent. You would expect to find a coincidence 3.85 times on the average in every 100 comparisons.

c. If you select two letters from English plaintext, however, the probability of their being the same is higher than 1 in 26. Frequency studies have shown that the probability of a coincidence in English plaintext is .0667. In other words, in every 100 comparisons, you would expect to find 6.67 coincidences in plaintext. Each language has its own probabilities, but similar traits occur in each alphabetic language.

d. Different coincidence tests use different methods of comparing letters with each other, but each rests on the probabilities of random and plaintext comparisons. The actual number of coincidences in a cryptogram can be compared with the random and plaintext probabilities to help make judgments about the cryptogram.

2-13. Index of Coincidence

A common way of expressing the results of a coincidence test is the index of coincidence (XC). The index of coincidence is the ratio of observed coincidences to the number expected in a random distribution. For plaintext, the expected index of coincidence for single letters in English is the ratio of .0667 to .0385, which is 1.73.

2-14. Monographic Phi Test

The most common coincidence test is the monographic phi test, which provides a mathematical way of measuring the roughness of a frequency count. *Monographic* is a fancy synonym for *one letter*. The term monographic distinguishes the test from the digraphic phi test, performed on two letter pairs, and other forms of the phi test. Phi is the English spelling of the Greek letter ϕ. The monographic phi test is based on the coincidence probabilities that occur when every letter in a cryptogram is compared with every other letter in the cryptogram.

a. Fortunately, the phi test can be calculated without actually comparing every letter with every other letter. Both the total number of comparisons and the total number of coincidences can be calculated from the frequency count.

b. The total number of comparisons when every letter is compared with every other letter is the total number of letters multiplied by the total number minus one. Expressed as a formula, it looks like this–

$$\text{Comparisons} = N\ (N - 1).$$

c. Since one out of every 26 comparisons in a random distribution is expected to be a coincidence, the formula for the expected random value of phi is as follows:

$$\phi r = \frac{N\ (N - 1)}{26}$$

or

$$\phi r = .0385\ N\ (N - 1).$$

d. The expected value for plaintext coincidences is–

$$\phi p = .0667\ N\ (N - 1).$$

e. Just as the total number of comparisons is N (N – 1), the total number of coincidences for each letter is f (f – 1), where f is the frequency of the individual letter. The total number of coincidences is the sum of the coincidences for all the letters. The total number of coincidences is labeled phi observed or øo, and can be expressed as either–

$$\phi o = \phi A + \phi B + \phi C + \ldots + \phi Z$$

or

$$\phi o = \Sigma f\ (f - 1).$$

(The Greek letter sigma (Σ)is used to mean *sum of.)*

f. To calculate ϕo, take each letter frequency greater than 1 and multiply it times the frequency minus 1, as the formula suggests. (You can ignore letters with a frequency of 1, because they will be multiplied by 0.) Then add the results of all the multiplications.

g. The index of coincidence for the phi test is called the delta IC. The delta IC is the ratio of phi observed to phi random. It can be expressed using the Greek letter delta (Δ).

$$\Delta IC = \frac{26\ \Sigma f\ (f-1)}{N\ (N-1)}$$

h. The results of a phi test can be expressed in terms of ϕo, ϕp, and or as the ΔIC. Where computer support is available to perform the calculations, the ΔIC is the form usually shown. Where paper and pencil methods are used, either form may be used. Both methods are shown in the next example.

Letters:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
f:	3	3	0	7	2	1	1	4	0	0	1	0	0	0	4	1	6	3	0	4	1	0	5	1	0	3
f-1:	2	2		6	1			3							3		5	2		3			4			2
f(f-1):	6	6		42	2			12							12		30	6		12			20			6

$$\begin{aligned} \phi o &= \Sigma f\,(f-1) \\ &= 6+6+42+2+12+12+30+6+12+20+6 \\ &= 154 \end{aligned}$$

$$\begin{aligned} \phi p &= .0667\ N\,(N-1) \\ &= .0667 \times 50 \times 49 \\ &= 163 \end{aligned}$$

$$\begin{aligned} \phi r &= .0385\ N\,(N-1) \\ &= .0385 \times 50 \times 49 \\ &= 94 \end{aligned}$$

$$\begin{aligned} \Delta IC &= \phi o/\phi r \\ &= 154/94 \\ &= 1.64 \end{aligned}$$

2-15. Interpreting the Phi Test

The previous example showed results close to the expected value for plaintext. This indicates the frequency count it was based on had the same approximate degree of roughness as expected for plaintext. It does not show that it was plaintext or that it was enciphered in a simple substitution system, although the latter is possible. It must be considered as just one piece of evidence in deciding what system was used.

a. In plaintext of 50 to 200 letters, the delta IC will usually fall between 1.50 and 2.00. Shorter text can vary more, and longer text will be consistently closer to 1.73. Since simple monoalphabetic systems have the same frequency distribution as plaintext, these simple systems follow the same guidelines as plaintext.

b. Random text centers around a IC of 1.00 but is subject to the same variability as plaintext. Small samples of under 50 letters vary widely. Samples in the 50 to 200 letter range will usually fall between 0.75 and 1.25. Larger samples approach 1.00 more consistently.

c. Polyalphabetic systems tend to resemble random text, and the more different alphabets that are used, the more likely the ΔIC is to approach 1.00.

d. The four frequency counts in Figure 2-1 follow these guidelines closely. Each one is 100 letters long. The first three, the plaintext, the transposed text, and the simple monoalphabetic substitution each have a ΔIC of 2.00. The fourth example, the polyalphabetic substitution example, has a ΔIC of 1.05. The system used in the example has 26 different alphabets, and the underlying plaintext frequencies have been thoroughly suppressed.

PART TWO

Monographic Substitution Systems

CHAPTER 3

MONOALPHABETIC UNILATERAL SUBSTITUTION SYSTEMS USING STANDARD CIPHER ALPHABETS

Section I
Basis of Substitution Systems

3-1. Substitution Systems

The study of analysis of substitution systems begins with the simplest of systems. The systems explained in Part Two are monographic substitution systems. The systems in Chapters 3 and 4 are further categorized as monoalphabetic unilateral substitution systems.

a. Both *monographic* and *unilateral* mean *one letter* by their construction. The prefixes *mono*- and *uni*- mean one, and *graphic* and *literal* refer to *letters* or other characters. Monographic systems are those in which one plaintext letter at a time is encrypted. Unilateral systems are those in which the ciphertext value is always one character long. Note that the term monographic refers to single plaintext letters and the term unilateral refers to single ciphertext letters.

b. Monoalphabetic systems are those in which a given ciphertext value always equals the same plaintext value. One alphabet is used. “

c. Chapter 5 deals with monoalphabetic multilateral systems, which substitute more than one ciphertext character for each plaintext character. Later parts of this manual present the analysis of polygraphic and polyalphabetic systems. Polygraphic systems substitute values for more than one plaintext letter at a time. In polyalphabetic systems, a given ciphertext character will have different plaintext equivalents at different times through the use of multiple alphabets.

d. The techniques used with these simplest of systems carry over to the more complicated systems. Whether or not you will ever see the very simple systems in use, the same skills are used in combination with other techniques to solve more secure systems as well.

3-2. Nature of Alphabets

A cipher alphabet lists all the plaintext values to be enciphered paired with their ciphertext equivalents. Cipher alphabets can take many different forms from a simple listing of 26 letters with 26 equivalent letters to much more complex charts. Chapters 3 and 4 deal with the simple 26 letter for 26 letter types and Chapter 5 introduces some of the more complex chart type multilateral systems.

a. The simple 26 letter for 26 letter cipher alphabets are composed of two sequences of letters: the plain component sequence and the cipher component sequence. The letter sequences can be in standard A through Z order, systematically mixed order, or randomly sequenced. Alphabets are classed as standard, mixed, or random according to the types of sequences they contain. The techniques used to solve the system depend to some extent on the type of alphabet. Alphabets in which both components are standard A through Z sequences are called standard alphabets.

b. A standard sequence does not have to be written beginning with A and ending with Z. A sequence is considered to have no beginning or ending, but continues as if it were written in a circle. The letter that follows Z in a standard sequence is A. Each of the following examples is a standard sequence.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

J K L M N O P Q R S T U V W X Y Z A B C D E F G H I

c. If the alphabetic progression is in the normal left to right order, it is called a direct standard sequence. If the alphabetic progression proceeds from right to left, it is called a reverse standard sequence. Each of the following examples is a reverse standard sequence.

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

D C B A Z Y X W V U T S R Q P O N M L K J I H G F E

d. Standard alphabets are also classed as direct or reverse. If the two standard sequences (plaintext and ciphertext) run in the same direction, the alphabet is called a direct standard alphabet. Each of the following alphabets is a direct standard alphabet. Notice that the second one has the identical equivalents to the first and can be rewritten in left to right order without changing its substitution at all.

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

p: z y x w v u t s r q p o n m l k j i h g f e d c b a
c: Q P O N M L K J I H G F E D C B A Z Y X W V U T S R

p: j i h g f e d c b a z y x w v u t s r q p o n m l k
c: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

e. If the two standard sequences (plaintext and ciphertext) run in opposite directions, the alphabet is called a reverse standard alphabet. Notice that the two following examples of reverse standard alphabets are also equivalent.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H

p:	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h
c:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

f. An alphabet, in which the plain component is shown in A through Z order, is called an enciphering alphabet. The first alphabet after paragraph 3-2e is an enciphering alphabet. If the cipher component is in A through Z order, it is called a deciphering alphabet. The second alphabet is a deciphering alphabet.

g. Standard alphabet cryptograms are the easiest to solve. The rest of Chapter 3 explains the techniques of cryptography and cryptanalysts of standard monoalphabetic ciphers.

Section II
Monoalphabetic Unilateral Substitution

3-3. Cryptography

The users of a monoalphabetic unilateral substitution system must know three things about the keys to the system. They must know what sequence of letters is used for the plain component, what sequence is used for the cipher component, and how the two components line up with each other. The alignment is termed the *specific key*. Whatever keys are put into use by the originating cryptographer must be known by the receiving cryptographer, too. The key selection must either be prearranged or sent along with the cryptogram itself.

a. Prearranged keys are normally included in published operating instructions, known variously as the Signal Operation Instructions (S0I) or Communications-Electronics Operation Instructions (CEOI). For example, an SOI might specify the use of direct standard sequences for an extended period and a new alignment of the two sequences at regular shorter intervals. A portion of an SOI might look like this example.

31 May 1989, 0001-0600Z

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R

31 May 1989, 0601-1200Z

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U

Another way to provide exactly the same information in a more abbreviated form is shown below.

31 May 1989

Plain component: Direct standard sequence.
Cipher component: Reverse standard sequence.

0001-0600Z: Ap = Qc
0601-1200Z: Ap = Tc

In this example, the alphabet construction is left to the cryptographer, who writes out the sequences and aligns them with each other according to the specific keys for each key period.

b. Transmitted keys are used whenever the cryptographer is given some choice of the specific key selections. For example, if the alignment of the sequences were left to the cryptographer, the alignment would need to be transmitted. One way to do this is to agree that the first group of the message is always the cipher equivalent of plaintext A repeated five times. This group then tells the receiving cryptographer how to align the alphabet. The example is simple, but more complex systems can be used for greater security.

3-4. Message Preparation

The cryptographer normally prepares a message for encryption by writing the plaintext in regular length groups. Four or five letter groups are common for this type of system.

a. Word lengths are not preserved normally, because they provide strong clues to the plaintext when they appear. It is easier for a cryptanalyst to figure out the plaintext for example 1 in Figure 3-1 than example 2.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Plaintext to be enciphered: ATTACK AT DAWN

● Example 1: Word length encipherment.

p: attack at dawn
c: JCCJLT JC MJFW

Resulting cryptogram: JCCJLT JC MJFW

● Example 2: Four letter group encipherment.

p: atta ckat dawn
c: JCCJ LTJC MJFW

Resulting cryptogram: JCCJ LTJC MJFW

Figure 3-1. Word and group length encipherment.

b. In writing out the message for encipherment with a simple system, any numbers in the text must be spelled out or left in the clear. Punctuation must be spelled out or omitted. At the end of sentences, PD or STOP is often used in English. Commas are replaced by COMMA or CMA.

c. Whenever the text does not break evenly into groups, the text will generally be padded to fill out the groups. The filler letters are usually added at the end of the last group. For clarity, they are often just a repeated low frequency letter such as X or Z. The above cryptogram, broken into five letter groups, appears below.

JCCJL TJCMJ FWXXX

Section III

Solution of Monoalphabetic Unilateral Ciphers Using Standard Cipher Alphabets

3-5. Methods of Solution

Because of the extreme simplicity of standard alphabets, cryptograms enciphered with them can always be solved. There are two general approaches to solving these simple ciphers. One makes use of the frequency characteristics discussed in Chapter 2. The other uses the orderly progression of the alphabet to generate all possible decipherments from which you can pick the correct plaintext. Each method is explained in the following paragraphs.

3-6. Frequency Matching

The first approach consists of matching expected plaintext letter frequencies with the observed ciphertext letter frequencies.

a. As explained in Chapter 2, monoalphabetic unilateral ciphers preserve exactly the same letter frequencies as found in plaintext. The frequencies occur with the cipher equivalents, not the plaintext letters, but the numbers are unchanged. If E was the most common plaintext letter in a cryptogram, then E's replacement will be the highest frequency ciphertext letter.

b. With standard alphabets, another characteristic is preserved in addition to the individual letter frequencies. The order of highs and lows is also preserved. With a direct standard alphabet, the pattern of peaks and troughs remains, although shifted to the right or left. With a reverse standard alphabet, the pattern also remains, but it runs in the opposite direction. Figure 3-2 illustrates the expected frequency distribution of 100 letters of plaintext. It then shows what happens to the distribution when it is enciphered by a direct and a reverse standard alphabet.

c. As shown in Figure 3-2, there are several recognizable patterns in plaintext. First is the three peak pattern formed by the letters A through I. The pattern is a peak (A), a three letter trough (BCD), a peak (E), a three letter trough (FGH), and a peak (I). The second easy to recognize pattern is formed by the letters N through T. The pattern is a double peak (NO), a trough (PQ), and a triple peak (RST). When you compare the plaintext distribution with the two ciphertext distributions, the patterns are still evident.

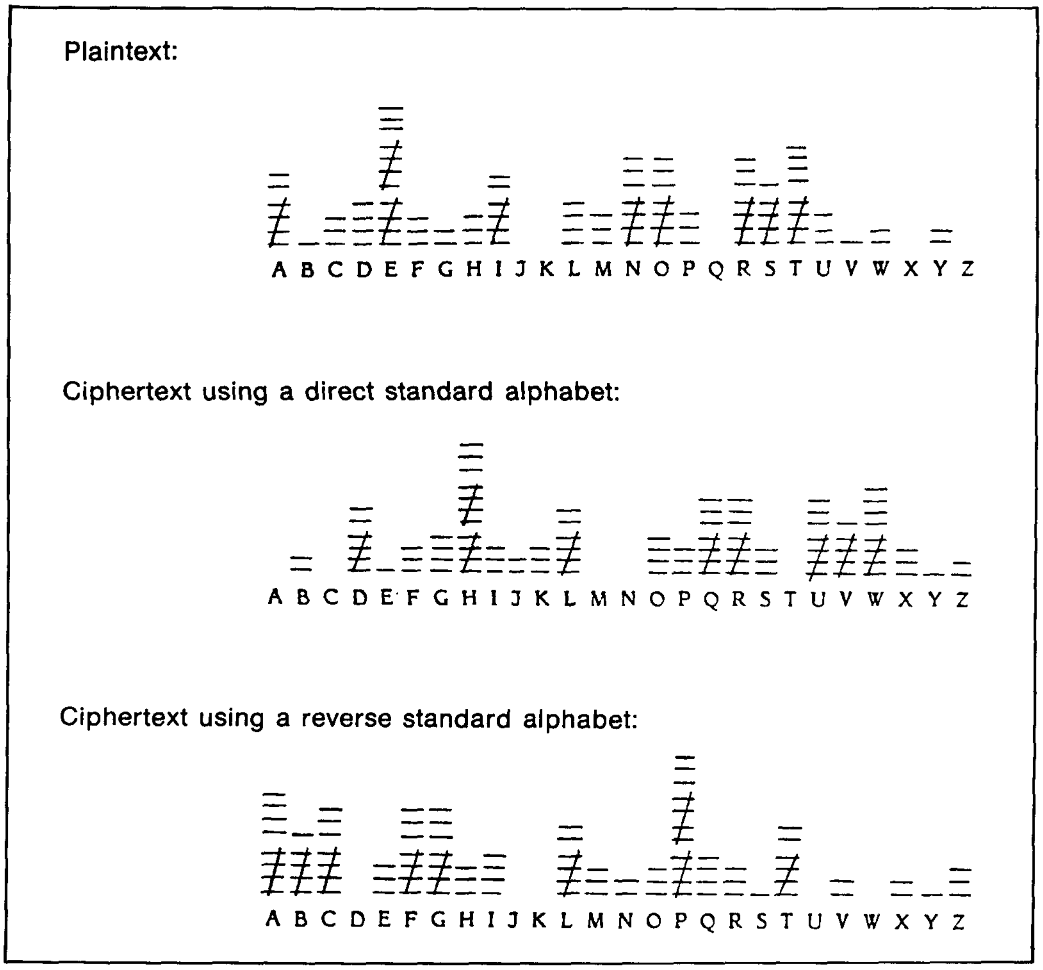
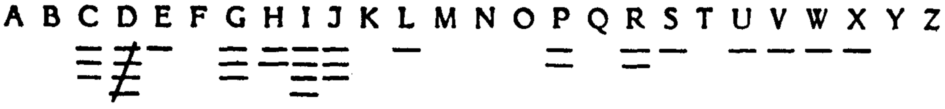


Figure 3-2. Frequency distributions.

d. Not all plaintext frequency distributions show the patterns clearly. The examples in Figure 3-2 show a perfect 100 character frequency distribution with every letter appearing exactly as many times as expected. Actual frequency counts will vary considerably, particularly with small samples. It is easier to recognize the overall patterns by their frequency than it is to recognize individual letters, however. If you can recognize even a partial pattern, it is easy to write the whole alphabet and see if the frequencies are close to expectations. Consider the cryptogram shown below.

CDRDC IPRIS JGXCV EPHII LDUDJ GWDJG HXXXX



The four Xs at the end are almost certainly fillers, so they are not counted. The cryptogram is too short for the complete pattern to appear. The cluster of higher frequency letters from C through I could represent the N through T pattern, though. We will write the full sequence of letters on that assumption.

p:	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
c:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

The frequency match fits the plaintext letters reasonably well. E does not appear at all, but other vowels make up for it, keeping the vowels near the expected 40 percent. No low frequency letters appear with unexpectedly high frequency. The confirmation of the match occurs when the alphabet is tried with the cryptogram.

nocon tactd uring pastt wofou rhour s
CDRDC IPRIS JGXCV EPHII LDUDJ GWDJG HXXXX

or

NO CONTACT DURING PAST TWO FOUR HOURS

e. This method depends on knowing or suspecting that standard alphabets are used. With a long message, the frequency count will usually make it obvious. The A-E-I and the NO-RST peaks will stand out. With a short message like the above example, it is not obvious, but it is an easy step to try if you think you spot a partial match.

3-7. Generating All Possible Solutions

The frequency matching technique only works if the text is long enough to produce a recognizable frequency count. A second technique always leads to the solution. With a known standard alphabet, there are only 26 different ways the alphabet can be aligned. It does not take very long to try all 26 settings to find the correct solution.

a. As an example, consider the solution of the following cryptogram.

SIZUX VJFLK

With no repeated letters, frequency matching is not likely to help. Suppose the alphabet was a direct standard with p:a=c: Z.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Using the above alphabet, SIZUX VJFLK *deciphers* as TJAVY WKGML. Obviously, this is not the correct plaintext. The text the trial decipherment produces is called *pseudoplaintext* or *pseudotext.* Suppose the alphabet used p:a=c:Y.

p:	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
c:	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**

This alphabet produces **UKBWZ XLHNM.**
The next alphabet with p:a=c:X gives the text **VLCXA YMION.**
The next alphabet with p:a=c:W gives the text **WMDYB ZNJPO.**
The next alphabet with p:a=c:v gives the text **XNEZC AOKQP.**

Clearly, not one of these is the correct setting, but notice the effect of trying each alphabet in turn. The columns of letters from each successive trial alphabet are in alphabetical order. You can achieve the same effect as trying each alphabet in turn by listing the letters vertically in alphabetical order. Figure 3-3 lists the results of trying all possible alphabets.

```
SIZUX VJFLK

TJAVY WKGML
UKBWZ XLHNM
VLCXA YMION
WMDYB ZNJPO
XNEZC AOKQP
YOFAD BPLRQ
ZPGBE CQMSR
AQHCF DRNTS
BRIDG ESOUT
CSJEH FTPVU
DTKFI GUQWV
EULGJ HVRXW
FVMHK IWSYX
GWNIL JXTZY
HXOJM KYUAZ
IYPKN LZVBA
JZQLO MAWCB
KARMP NBXDC
LBSNQ OCYED
MCTOR PDZFE
NDUPS QEAGF
OEVQT RFBHG
PFWRU SGCIH
QGXSV THDJI
RHYTW UIEKJ
```

Figure 3-3. All possible decipherments.

The plaintext, *BRIDGES OUT*, appears about halfway down the columns. In practice, you would only write enough to recognize the plaintext. Generally, write a column at a time, and only write as many columns as you need. Once you have spotted plaintext, set up the alphabet and complete the decipherment.

b. With a reverse standard alphabet, another step must be added. You cannot generate the columns until you try deciphering first at any alphabet setting of your choice. Then generate the columns starting with your trial decipherment. As you will see in the following chapters, this technique can be used with any known alphabets, not just standard ones. The procedures, which will be illustrated in Chapter 4, are—

- Set up the known alphabet at any alignment.
- Perform a trial decipherment to produce pseudotext.
- Using the trial decipherment as the letters at the head of the columns, generate all possible decipherment by listing the plain component sequence vertically for each column.

CHAPTER 4

MONOALPHABETIC UNILATERAL SUBSTITUTION SYSTEMS USING MIXED CIPHER ALPHABETS

Section I
Generation and Use of Mixed Cipher Alphabets

4-1. Mixed Cipher Alphabets

Mixed cipher alphabets differ from standard alphabets in that one or both sequences are mixed sequences. A mixed sequence is any sequence not in normal alphabetical order. The two main types of mixed sequences are systematically mixed and random mixed sequences.

a. Systematically mixed sequences are produced by an orderly process based on easily remembered keywords, phrases, or simple rules. There are a number of mixed sequence types, which will be explained in this section. Their advantage is that the keys can be easily memorized and reconstructed for use when needed. Their disadvantage is that the orderliness in construction can be used by the opposing cryptanalyst to aid in their recovery.

b. Random mixed sequences are not based on any orderly generation process. They can be produced by various means ranging from pulling the 26 letters out of a hat to complex machine generation. Their advantage is that their structure offers no help to the opposing cryptanalyst. Their disadvantage is that the keys cannot be memorized easily or produced from simple directions as systematically mixed sequences can. They must be printed out in full and supplied to every user.

4-2. Keyword Mixed Sequences

One of the simplest types of systematic sequences is the keyword mixed sequence. The sequence begins with the keyword, which may be a word or a phrase. Any letters repeated in the keyword are used only once, dropping the repeating letters. After the keyword, the rest of the letters are listed in alphabetic order, omitting those already used.

Keyword— **CRYPTOGRAPHIC**

Repeated letters dropped: **CRYPTOGAHI**

Remaining letters added in normal order:

CRYPTOGAHIBDEFJKLMNQSUVWXZ

Keyword— **MILITARY INTELLIGENCE**

Repeated letters dropped: **MILTARYNEGC**

Remaining letters added in normal order:

MILTARYNEGCBDFHJKOPQSUVWXZ

4-3. Transposition Mixed Sequences

Transposition mixed sequences are produced by writing a letter sequence into a matrix and extracting it from the matrix by a different route. The most common types are called simple columnar, numerically keyed columnar, and route transposition sequences.

a. Simple columnar transposition is usually based on a keyword mixed sequence. The keyword determines the width of the matrix that is used. The keyword is written as the first row of a matrix and the rest of the sequence is written beneath it, taking as many rows as necessary. The transposition mixed sequence is then produced by extracting the columns of the matrix from left to right.

Keyword— **ARTILLERY**

Keyword mixed sequence in matrix:

A	R	T	I	L	E	Y
B	C	D	F	G	H	J
K	M	N	O	P	Q	S
U	V	W	X	Z		

Resulting sequence:

ABKURCMVTDNWIFOXLGPZEHQYJS

Keyword– **MORTAR**

Keyword mixed sequence in matrix:

M	O	R	T	A
B	C	D	E	F
G	H	I	J	K
L	N	P	Q	S
U	V	W	X	Y
Z				

Resulting sequence:

MBGLUZOCHNVRDIPWTEJQXAFKSY

b. The numerically keyed columnar transposition mixed sequence differs from the simple columnar only in the way it is extracted from the matrix. Instead of extracting the columns left to right, the order of the columns is determined by a numerical key based on the keyword. After constructing the matrix, the letters in the keyword are numbered alphabetically. The columns are then extracted according to the resulting numerical key.

Keyword– **CALIFORNIA**

2	1	5	4	3	7	8	6
C	A	L	I	F	O	R	N
B	D	E	G	H	J	K	M
P	Q	S	T	U	V	W	X
Y	Z						

Resulting sequence:

ADQZCBPYFHUIGTLESNMXOJVRKW

Keyword– **VERMONT**

7	1	5	2	4	3	6
V	E	R	M	O	N	T
A	B	C	D	F	G	H
I	J	K	L	P	Q	S
U	W	X	Y	Z		

Resulting sequence:

EBJWMDLYNGQOFPZRCKXTHSVAIU

c. Route transposition sequences are formed by any other systematic way of entering sequences into a matrix and extracting them from a matrix. They can be based on standard or keyword mixed sequences. The samples in Figure 4-1 show some of the common routes that can be used. The last two omit the letter J for the convenience of a square matrix.

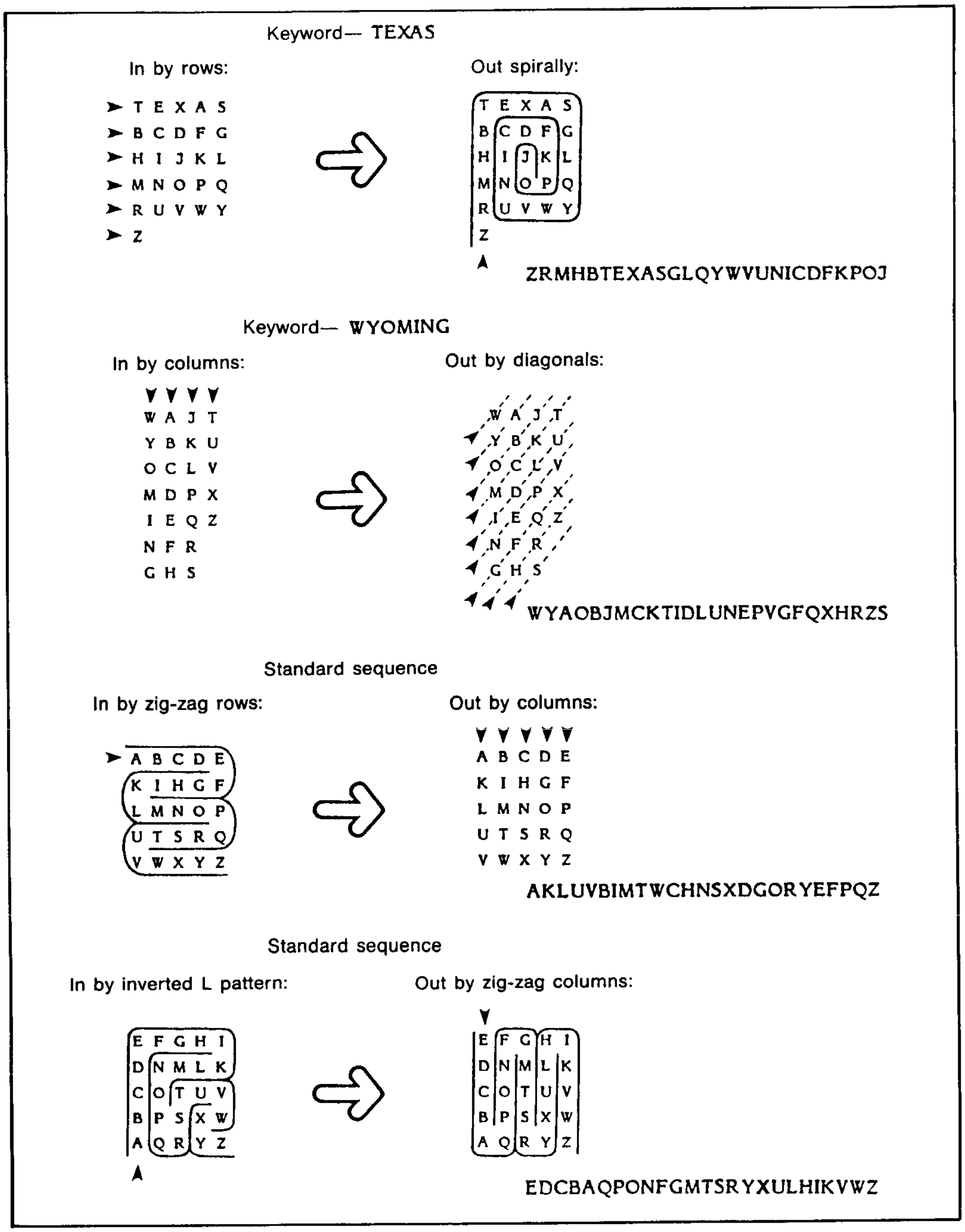


Figure 4-1. Route transposition.

4-4. Decimation Mixed Sequences

Decimation mixed sequences are produced from a standard or keyword mixed sequence by counting off letters at a regular interval.

a. As an example, consider decimating a standard sequence at an interval of 3. The new sequence begins with the first letter of the basic sequence, in this case, A. The second letter of the new sequence is the third letter that follows from the basic sequence, D. Every third letter is selected until the end of the basic sequence is reached.

Basic sequence:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Resulting decimated sequence:

A D G J M P S V Y ...

The count then continues as if the sequence were written in a circle. The next letter after Y, skipping Z and A, is B. The complete resulting sequence is shown below.

A D G J M P S V Y B E H K N Q T W Z C F I L O R U X

b. The interval should have no common factors with the length of the sequence. Since any even number has a common factor of 2 with 26, only odd numbers are selected with 26 letter sequences. Intervals with common factors are not selected, because the count will return to the starting point again before all the letters are used. The interval should also be less than half the length of the sequence, because larger numbers will just duplicate in reverse order the sequence produced by a smaller number. An interval of 23, for example would produce the same sequence as an interval of 3, but in the reverse order. For a 26 letter sequence, the only usable intervals are 3, 5, 7, 9, and 11. By counting either left to right or right to left, all the basic decimated sequences can be produced.

c. Study of this method of decimation is particularly significant, because the solution of some types of polyalphabetic ciphers can yield sequences in a decimated order instead of the original order.

d. An alternate method of decimation is occasionally encountered. In the alternate method, each letter is crossed off as it is selected and that letter is not counted again. The restrictions on intervals do not apply to this method, because the starting letter can never be reached again. This method is used less, because it is subject to mistakes in the counting process that are hard to detect and correct.

4-5. Types of Mixed Cipher Alphabets

As mentioned at the beginning of this section, a mixed alphabet is any alphabet that uses one or more mixed sequences. The simplest types are those which use a standard sequence in one component and a mixed sequence in the other. These are the easiest for a cryptanalyst to reconstruct. Next in order of difficulty are those in which the same mixed sequence is used in the plain and cipher components. Most difficult are those in which two different mixed sequences are used. The next section shows how to recover each of these types of alphabets.

Section II
Recovery of Mixed Cipher Alphabets

4-6. Alphabet and Plaintext Recovery

Although this manual separates the techniques of alphabet recovery from plaintext recovery, the two processes will usually occur simultaneously, each supporting the other. When an orderly structure is found in an alphabet as individual letters are recovered, the orderly structure often helps make more plaintext recoveries. The techniques explained in this section will be used in the next section.

a. You usually begin reconstruction by recording recoveries in the form of an enciphering alphabet. An enciphering alphabet is one in which the plaintext component is arranged in A through Z order. Ciphertext letters are written in the cipher component paired with their plaintext equivalents in the plain component. The plaintext can be either the top or bottom letters, but whichever you select, you should follow it consistently in the alphabet as well as the cryptogram. Inconsistency leads to errors. In this manual, plaintext is placed above ciphertext.

b. A deciphering alphabet is one in which the ciphertext is written in A through Z order. Rearranging the alphabet into deciphering order is sometimes helpful in alphabet recovery.

c. Whenever systematically mixed alphabets are used, you should attempt to recover the systems and keys in use. The same sequences are often reused, either at different alignments of the same alphabet or in combination with other sequences. The solution can be reached much quicker when you recognize and take advantage of previous recoveries.

4-7. Reconstruction of Alphabets With One Standard Sequence

Whenever one of the two sequences is a standard sequence, recovery of the system used to produce the other sequence is made much easier.

a. The easiest type to recognize is the keyword mixed sequence. Any keyword mixed sequence has two parts—the keyword and the alphabetic progression. If you find that recovered letters are falling in alphabetic progression consistently in a portion of the sequence, it is probably a keyword mixed sequence. In this case, you can narrow down the possibilities of unrecovered letters. Consider the following partially recovered alphabet.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	S				Z				V					T	H			D	F	G	I					

(1) The letters DFGI appear to be part of the alphabet section of the cipher sequence. The alphabetic progression continues at the left with the letters S and Z. All the other recovered letters appear to be part of the keyword. Between the H and the D there is room for only two of the letters at the beginning of the alphabet—A, B, and C. At least one of these must be in the keyword, leaving the other two as probable equivalents of plaintext P and Q. Similarly, there is space for only three letters between S and Z. T and V already appear, so the spaces must be filled by three of the four letters, U, W, X, and Y. Given these limitations, recovery of more plaintext is likely. Continuing the example, consider that plaintext C, F, L, P, W, and Y are recovered next.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	S		X		Z	L			V			O		T	H	B		D	F	G	I		K		P	

(2) These recoveries enable several more probable letters to be placed by alphabetical progression.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	S		X	Y	Z	L			V			O		T	H	B	C	D	F	G	I	J	K		P	

(3) At this point, we can see that A and E must be in the keyword, because there is no room for them in the alphabetic progression. U or W must be in the keyword, because there is only room for one of them between S and X, and V is already placed. Similarly, M or N and Q or R must be in the keyword. Q is unlikely, even though U is available to pair with it. Placing Q and U anywhere in the blanks in the keyword suggests nothing further. R must be in the keyword, then.

(4) The letter after L in the keyword must certainly be a vowel or the keyword would be unpronounceable, and that vowel represents plaintext G. With the possibilities narrowed down this far, you might be able to spot the keyword

without referring back to the cryptogram that produced the partially recovered alphabet. The complete alphabet looks like this.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q

b. Recovery of decimated sequences is a straightforward process of trying out intervals. Just as a decimated sequence is produced by counting at a regular interval, the original sequence can be recovered by counting at a regular interval, too. A partially recovered alphabet with a suspected decimated sequence in the cipher component could look like this example.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	N	.	.	.	D	.	.	.	X	.	.	F	.	W	H	.	.	M	V	.	.	.	K	.	.	.

(1) To determine if this is a decimated sequence, various intervals can be tried. The recovered letters suggest one obvious possibility. The letters V, W, and X all appear among the recovered letters. If they were in order in the base sequence used to generate the decimated sequence, they should reveal the interval. The interval from V to W and from W to X is -5 in each case. A trial decimation at -5, beginning with V produces the following sequence.

VWX...H.D.....N..F..KM....

(2) This sequence of letters appears to be a keyword mixed sequence. The keyword appears after the VWX and alphabetic progression resumes with the F and the KM. Once you recognize this structure, you can use it to assist in further plaintext recoveries just as in the first example shown in paragraph 4-7a. The original basic sequence used to produce the decimated sequence is shown below.

RHODEISLANBCFGJKMPQTUVWXYZ

c. Simple transposition mixed sequences often resemble decimated sequences. You will often see a regular spacing of adjacent low frequency letters, just as we saw VWX in the previous example. This is not caused by a decimation interval, but by the regular length of columns separating the letters. Recovery of the generation method of transposition mixed sequences is accomplished by rebuilding the original matrix.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	U		F	O	V			P	X			K		Y	I			R	Z	G	D		T		E	

The almost regular spacing of the letters V, X, Y, and Z resembles a decimated sequence, but the interval is not constant. This almost, but not quite, regular spacing is an indication of simple columnar transposition. The letters V, X, Y, and Z are probably the bottom letters in their columns of the original matrix. W, which has not been recovered, probably occurs in the keyword, because there does not appear to be room for a column ending with W. Analysis of this type of sequence proceeds by rebuilding the columns. Placing the letters V, X, Y, and Z in sequence with their preceding letters as their columns, produces this partial result.

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
U . F O V/. . P X/. . K . Y/I . . R Z/G D . T . E .
```

U		.	I
.	.	.	.
F	.	K	.
O	P	.	R
V	X	Y	Z

Now the initial reconstruction appears successful. The rows above VXYZ also show alphabetic progression developing. Q can be inserted in the next to last row with confidence. The next step is to place the rest of the letters into columns that would continue the structure in a logical way. A little trial and error will show that the columns before the V column end with T and U. The U was not the top of the V column, but the bottom of the preceding column.

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: U/. F O V/. . P X/. . K Q Y/I . . R Z/G D . T/. E .
```

				.	I
G	.	.	.	.	.
D	E	F	.	K	.
.	.	O	P	Q	R
T	U	V	X	Y	Z

The longer columns belong on the left. Shifting these columns produces this result.

.	I	G	.	.	.
.	.	D	E	F	.
K	.	.	.	O	P
Q	R	T	U	V	X
Y	Z				

The matrix is now in its original form. L, M, and N can be placed between K and O. Either H or J can be inserted between F and K and the remaining letter belongs in the keyword in the top row. S and W are in the keyword, because they are missing from the alphabetical progression. That leaves A, B, or C for the remaining letter of the keyword, with the other two on the second row. Since only one vowel has been found in the keyword up until now, A probably belongs in the keyword with B and C filling the blanks in the second row. Trial placements of A, S, and W together in the first row blanks, together with either H or J in the remaining space leads to the conclusion of JIGSAW as the keyword.

J	I	G	S	A	W
B	C	D	E	F	H
K	L	M	N	O	P
Q	R	T	U	V	X
Y	Z				

d. The recovery of numerically keyed columnar transposition sequences is the same as for simple columnar transposition, except the columns are not in order in the sequence. The next example shows the recovery of this kind of transposition mixed sequence.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	X	M	D	B	Z	P	.	T	Y	.	.	S	U	I	R	W	.	C	O	V	J	.	L	.	H	.

This problem is again best approached through the end of alphabet letters. V, W, X, Y, and Z have all been recovered, and they make a good starting point. V, W, X, Y, and Z are placed in a row with their preceding letters above them in columns.

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X/M D B Z/P . T Y . . S U I R W/. C O V/J . L . H .
```

.	U	.	P	M
C	I	H	.	D
O	R	.	T	B
V	W	X	Y	Z

This time no alphabetic progression appears, even if we consider that one or two of the columns might be misplaced. In this case, the next thing to consider is that the sequence may be reversed. Selecting the letters to the right of V, W, X, Y, and Z instead of the left produces the following example.

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
X M D B/Z P . T/Y . . S U I R/W . C O/V J . L . H .
```

L	O	B	S	T
.	C	D	.	.
J	.	M	.	P
V	W	X	Y	Z

This setup is clearly correct. Next, we add the two short remaining segments.

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
X M D B/Z P . T/Y . . S/U I R/W . C O/V J . L/. H ./
```

		L	O	B	S	T
.	R	.	C	D	.	.
H	I	J	.	M	.	P
.	U	V	W	X	Y	Z

Moving the short columns to the right and filling in the missing letters produces the following matrix.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	X	M	D	B/	Z	P	G	T/	Y	N	F	S/	U	I	R/	W	K	C	O/	V	J	A	L/	Q	H	E/

L	O	B	S	T	E	R
A	C	D	F	G	H	I
J	K	M	N	P	Q	U
V	W	X	Y	Z		

The final step is to recover the numerical key. If normal methods are used, it should be produced by the keyword and should show the actual order in which the columns were extracted. Numbering the letters in the keyword in alphabetical order and comparing them with the cipher sequence in the alphabet confirms that this method was used. Since the sequence was reversed, the order of columns in the cipher sequence appears in right to left order beginning with the cipher letter B.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	X	M	D	B/	Z	P	G	T/	Y	N	F	S/	U	I	R/	W	K	C	O/	V	J	A	L/	Q	H	E/
				1				7				6			5				4				3			2

3	4	1	6	7	2	5
L	O	B	S	T	E	R
A	C	D	F	G	H	I
J	K	M	N	P	Q	U
V	W	X	Y	Z		

e. One type of transposition sequence remains to be considered. When a route transposition process is used, the solution is to try to reconstruct the original routes. In examining attempts to solve the matrix by rebuilding columns, be alert to entry routes other than by rows. Look for spirals, diagonals, and alternate horizontals or verticals. If rebuilding the columns produces no results, consider rebuilding spiral, diagonal, or alternate row or column routes. This manual does not show examples of these approaches, but if you encounter this situation, approach it logically and try various approaches until one succeeds. The techniques of solving route transposition ciphers explained later in this manual will help in this process.

f. Each of the preceding examples was approached as if we knew, perhaps from past history, what types of sequences were used. We assumed that the plain component was a standard sequence, and the cipher sequence could then be readily reconstructed by itself. It is common, in approaching a cryptanalytic problem, to assume the simplest case and only to move on to more complex possibilities when the simplest case must be rejected. A great deal of time can be wasted by assuming something is more complicated than it is.

g. The next simplest case is where the cipher sequence is a standard sequence and the plain sequence is mixed. When reconstruction attempts fail because you started with an enciphering alphabet, rearranging the alphabet into a deciphering alphabet may yield results. Once rearranged, the solution is approached just as we did in the above examples. Look for short alphabet progression to indicate keyword mixed sequences. If that is not found, see if a decimation was used. If decimation was not used, try reconstructing the columns of a columnar transposition. Remember to try forward and reversed sequences.

h. If none of these approaches yields results, either with an enciphering alphabet or a deciphering alphabet, other approaches are called for. Either there are two mixed sequences, a more complex process was used, or random sequences were used.

4-8. Reconstruction of Alphabets With Two Mixed Sequences

Recovering alphabet structure when both sequences are mixed is more difficult than the previous examples. You are much less apt to be successful with only partial recoveries. Where the alphabet could be reconstructed during the solution of the plaintext in the previous examples, reconstruction of an alphabet with two mixed sequences must usually wait for the full solution of the plaintext. The examples in this section will begin with a fully recovered, but not reconstructed, alphabet.

a. The easiest type to recover with two mixed sequences occurs when both sequences are keyword mixed, as in the next example.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	W	X	Y	Z	U	B	P	T	A	D	G	E	R	C	Q	S	F	V	H	I	J	K	L	M	N	O

p:	i	f	n	j	l	q	k	s	t	u	v	w	x	y	z	g	o	m	p	h	e	r	a	b	c	d
c:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Enciphering and deciphering forms of the same alphabet are shown. The underlined portions show substantial alphabetic progression in both, which is typical of alphabets with keyword mixed sequences. A transposition or decimation would not produce such an obvious progression. The underlined portions in both alphabets are probably in their original form. The remaining plain-cipher pairs are out of order. Your task is to reconstruct the original order. The usual approach at this point is to try to extend the alphabetic progression outward from the obvious progression. In this case, the enciphering alphabet shows two long alphabetic strings of cipher letters, HIJKLMNO and WXYZ, which must have some or all of the letters PQRSTUV in between. Similarly, the deciphering alphabet shows plaintext strings ABCD and STUVWXYZ, and some or all of the letters EFGHIJKLMNOPQR must be in between. Suppose the cipher letters PQRSTUV belong in exactly that order. If that is the case, then the plaintext letters GOMPHER must also be in the right order, preceding ABCD. We expect to find the keyword immediately before the beginning of the alphabetic sequence. GOMPHER, while not a recognizable word may be close to it. If we try GOMPHER as a keyword, then the remaining letters must be in alphabetical order. Adjusting the alphabet so GOMPHER is a trial keyword will produce this arrangement.

p:	f	i	j	k	l	n	q	s	t	u	v	w	x	y	z	g	o	m	p	h	e	r	a	b	c	d
c:	B	A	D	G	E	C	F	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Now the cipher sequence shows a recognizable word, BADGE, but the solution is incomplete. If we move the M-R pair so that plaintext M fits in alphabetic order instead of the keyword, we see the following alphabet.

p:	f	i	j	k	l	m	n	q	s	t	u	v	w	x	y	z	g	o	p	h	e	r	a	b	c	d
c:	B	A	D	G	E	R	C	F	H	I	J	K	L	M	N	O	P	Q	S	T	U	V	W	X	Y	Z

This rearrangement is the original sequence of the alphabet.

b. When transposed or decimated sequences are used in the alphabet, the solution is much more difficult. The alphabetic progression used in the previous example is not available to assist with reconstruction. A solution is still possible in many cases, however. When both sequences are the same sequence in the same direction, the alphabet can often be recovered quite readily.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	L	Q	M	N	I	P	X	S	T	V	G	W	Z	U	R	A	K	F	E	D	J	Y	B	C	O	H

(1) Reconstruction begins with a process called chaining. Use the plain-cipher pairs to create a 26 letter chain by linking the cipher letter of each pair to the pair with the same plaintext letter. Any pair can be used as the starting point. Beginning with the plaintext A-ciphertext L pair (abbreviated Ap-Lc) next find plaintext L. Plaintext L equals ciphertext W (Lp-Wc), producing a partial

chain of ALW. Continuing with Wp-Bc, the chain is extended to ALWB. Continue adding links to the chain until you return to the original letter A. The complete chain is shown below.

A L W B Q K G X C M Z H S E I T D N U J V Y O R F P

(2) Since we were able to produce a 26 letter chain, there is a strong indication that the same sequence was used in both components. With different sequences, the chances of producing such a chain are very low. Unrelated sequences will almost always return to the starting point before using all 26 letters. The alphabet in paragraph 4-8a, for example, produces separate 23 and 3 letter chains.

(3) The sequence produced by chaining an alphabet with two identical sequences in the same direction will always either be the original sequence or a decimation of the original sequence. This narrows the possibilities for the original sequence down to six. The chained sequence and its five possible decimations are listed below.

Chain:
A L $\underline{W}$ B Q K G $\underline{X}$ C M $\underline{Z}$ H S E I T D N U J $\underline{V}$ $\underline{Y}$ O R F P

Decimation 3:
A B G M S T U $\underline{Y}$ F L Q $\underline{X}$ $\underline{Z}$ E D J O P $\underline{W}$ K C H I N $\underline{V}$ R

Decimation 5:
A K $\underline{Z}$ T $\underline{V}$ P Q M I J F B C E U R $\underline{W}$ $\underline{X}$ S N O L G H D $\underline{Y}$

Decimation 7:
A $\underline{X}$ I $\underline{Y}$ $\underline{W}$ M D R Q H U P G E $\underline{V}$ L C T O B $\underline{Z}$ N F K S J

Decimation 9:
A M U L $\underline{Z}$ J $\underline{W}$ H $\underline{V}$ B S $\underline{Y}$ Q E O K I R G T F $\underline{X}$ D P C N

Decimation 11:
A H O $\underline{X}$ U B I P $\underline{Z}$ $\underline{Y}$ G N $\underline{W}$ E F M $\underline{V}$ K D L S R C J Q T

(4) If the original sequence was a decimated sequence, the basic keyword or standard sequence used to generate the decimated sequence would be one of the above. Since none of them are either standard or keyword mixed, the original sequence was probably transposed. Approaching each sequence above with transposition in mind, the letters V, W, X, Y, and Z have been underlined in each, searching for a basis to rebuild the columns. The last sequence (decimation 11) yields the following matrix.

T	U	R	K	E	Y
A	B	C	D	F	G
H	I	J	L	M	N
O	P	Q	S	V	W
X	Z				

(5) When the same sequence is used in the same direction in both components of the alphabet, a 26 letter chain will only be produced half of the time. When the two sequences are staggered by an odd number of letters, a 26 letter chain results. When the two sequences are staggered by an even number of letters, two separate 13 letter chains result. These can sometimes be recovered, too, but the solution is more difficult.

c. The chaining technique can also be used with alphabets with different sequences in the two components if they are reused at different alignments. Consider the next two alphabets, recovered at different times on the same day.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Y	P	U	Z	G	E	A	B	H	Q	V	M	C	L	K	I	R	T	W	O	D	J	S	X	N	F

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	F	L	A	G	Y	P	T	U	Z	E	B	H	Q	K	X	V	M	N	C	I	R	W	O	D	J	S

(1) To test if the same alphabet was used, chain the cipher sequences against each other. In the example, chain A of the first to T of the second, T of the first to N of the second, and so on. This produces the following chain.

A T N J W C Q E P L K X D R M H Z G Y F S O I V B U

(2) This confirms that the two alphabets used the same sequences at different alignments. If chaining produced anything but one 26 letter sequence or two 13 letter sequences, they are not the same alphabet.

(3) Write all possible decimations, as before.

Chain:
A T N J W C Q E P L K X D R M H Z G Y F S O I V B U

Decimation 3:
A J Q L D H Y O B T W E K R Z F I U N C P X M G S V

Decimation 5:
A C K H S U W L M F B J P R Y V N E D G I T Q X Z O

Decimation 7:
A E M O N L Z V W X Y U Q R S T P H I J K G B C D F

Decimation 9:
A L Y T K F N X S J D O W R I C M V Q H B E Z U P G

Decimation 11:
A X I E Y J M U K O Q G N R B L S C Z T D V P F W H

(4) The decimation of 7 produces a sequence that almost looks as if it were the original. This can happen when the decimation interval and the column length of a transposed sequence are the same except for one long column. The correct sequence is a decimation of 9 read in reverse.

L	E	M	O	N
A	B	C	D	F
G	H	I	J	K
P	Q	R	S	T
U	V	W	X	Y
Z				

The sequence used to generate the simply transposed sequence was a keyword mixed sequence based on LEMON.

(5) The plaintext component can be reconstructed now that the correct ciphertext sequence is known. We start with the decimated sequence. Since the sequence with a decimation of 9 was used in reverse to recover the keyword LEMON, we will list it in reverse.

c: G P U Z E B H Q V M C I R W O D J S X N F K T Y L A

Either of the two alphabets given at the start of this problem can be used to reconstruct the plaintext sequence. The first alphabet is repeated for reference.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c:	Y	P	U	Z	G	E	A	B	H	Q	V	M	C	L	K	I	R	T	W	O	D	J	S	X	N	F

We now rearrange this alphabet so that the cipher sequence is in the same order as the recovered decimated sequence.

p:	e	b	c	d	f	h	i	j	k	l	m	p	q	s	t	u	v	w	x	y	z	o	r	a	n	g
c:	G	P	U	Z	E	B	H	Q	V	M	C	I	R	W	O	D	J	S	X	N	F	K	T	Y	L	A

d. The chaining techniques introduced in this section are also used in the solution of polyalphabetic ciphers. They will be further developed in Part Four.

Section III

Solution of Monoalphabetic Unilateral Ciphers Using Mixed Cipher Alphabets

4-9. Preparation for Analysis

The first step in approaching the unsolved cryptogram is to prepare a worksheet.

a. If prepared by hand, one-fourth inch or one-fifth inch cross section paper (graph paper) should be used if possible. Hand lettering should be clearly printed in ink. The cryptogram should be triple spaced vertically to leave room for writing. If a copying machine is available and local security rules permit, the worksheet should be copied after preparation to permit a restart with a clean worksheet whenever needed.

b. Generally, you will want to prepare at least a unilateral frequency count. Other special frequency counts may be needed also, as will be explained later. If you are unsure of system identification, you may want to calculate the ϕIC. Computer support, if available, can save a lot of time at this step.

c. Next, you should scan the text searching for repeated segments of ciphertext. Underline all repeats you find of at least three letters in length. You may find it useful to underline two letter repeats, too.

d. If you have more than one cryptogram that appears to have been enciphered with the identical system, prepare a worksheet for each. Compare peaks and troughs of frequency counts to see if they are similar. If so, look for repeats between messages as well as within messages. Repeats between messages are another indication that the identical system was used. The more repeats you find, the easier the solution will be.

e. If you are still in doubt whether two cryptograms have been enciphered by the same system, there is a simple statistical test available, similar to the phi test. The chi test or cross product test compares two frequency distributions to determine the probability that they are from the same alphabet. The frequency of each letter in one distribution is multiplied by the frequency of the same letter in the other distribution. The results of all the multiplications are added to produce the chi value. Chi is the Greek letter that looks like an X. The formula for the chi value is—

$$X = \Sigma\ (f)(f2).$$

The expectation with a random match is 1/26th of the product of the total letters of each, or—

$$Xr = .0385\ (N1)(N2).$$

With a correct match, the expected value is .0667 times the products of the total letters, or—

$$Xp = .0667\ (N1)(N2).$$

The results can also be expressed as an index of coincidence, the usual form if produced by computer support. The formula for the cross IC, as it is called is—

$$X\ IC = \frac{Xo}{Xr} = \frac{26\ \Sigma\ (f1)(f2)}{(N1)(N2)}.$$

With a correct match, the expected IC value, as with the phi text is 1.73. If you match two alphabets and the X IC is close to 1.73, the chances are that they were enciphered with the same alphabet. Figure 4-2 illustrates a completed chi test.

PROBLEM: To determine if the two frequency counts below were from cryptograms enciphered with the same alphabet.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
c1:	-	3	2	6	1	13	-	3	3	-	3	-	6	2	3	3	4	1	-	-	10	-	1	-	4	1	N=69

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
c2:	4	2	1	6	1	7	-	4	-	1	2	-	5	1	3	4	4	3	-	1	8	-	1	1	2	-	N=61

Product:

-	6	2	36	1	91	-	12	-	-	6	-	30	2	9	12	16	3	-	-	80	-	1	-	8	-

$Xo = \Sigma\ (f)(f2) = 6 + 2 + 36 + \ldots + 8 = 315$

$Xr = .0385\ (N1)(N2) = .0385\ (69)(61) = 162$

$X\ IC = Xo/Xr = 315/162 = 1.94$

The results indicate the same alphabet was used.

Figure 4-2. Chi test.

f. As with any statistical test, you should use this as a guide only, and take all other available information into consideration, too, For example, if you find several long repeated segments of text between two cryptograms, it is probably a waste of time to calculate a chi test by hand. You already have the evidence you need to make a decision as to what approach you will use to reach a solution.

4-10. Approaches to the Solution

There are two basic approaches to the solution—the probable word method and the brute force approach. The probable word method is to try to gain a quick entry into the system by correctly assuming a portion of the plaintext. The brute force approach is to systematically narrow down the possible keys to the system and then force a solution by exhaustively trying all those possible keys. The method in the previous chapter of solving standard alphabet systems through trying all possible decipherment is a good example of the brute force approach. In practice, the solution of any given system is likely to use a combination of the two approaches.

4-11. Solution With Known Sequences - Completing the Plain Component Sequence

When the sequences used in an alphabet are known, a quick forced solution is possible.

a. Although mixed alphabets are used instead of standard ones, the solution is exactly the same as that explained in paragraph 3-7b.

(1) Set up the known alphabet at any alignment.

(2) Perform a trial decipherment (pseudotext).

(3) Using the trial decipherment as the letters at the head of the columns, generate all possible decipherment by listing the plain component sequence vertically for each column.

b. Figure 4-3 illustrates the solution of a cryptogram with known sequences using the above steps.

Solve: LIZWF QFMYK LOILX

Plain component—keyword mixed sequence based on SEA URCHIN.

Cipher component—standard sequence.

Step 1. Set up the alphabet at any alignment.

```
p: s e a u r c h i n b d f g j k l m o p q t v w x y z
c: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

Step 2. Perform a trial decipherment.

```
p: fnzwc mcgyd fknfx
c: LIZWF QFMYK LOILX
```

Step 3. Complete the plain component sequence.

```
FNZWC MCGYD FKNFX
GBSXH
JDEYI
KFAZN
LGUSB
MJRED
OKCAF
PLHUG
QMIRJ
TONCK
VPBHL
WQDIM
XTFNO
YVGBP
ZWJDQ
SXKFT
EYLGV
AZMJW
USOKX
REPLY BYCOU RIER
CAQMZ
HUTOS
IRVPE
NCWQA
BHXTU
DIYVR
```

```
p: s e a u r c h i n b d f g j k l m o p q t v w x y z
c: H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
```

Plaintext: REPLY BY COURIER

Figure 4-3. Completing the plain component.

4-12. Probable Word Method

The probable word method of solution depends on your being able to correctly identify a portion of the plaintext. When you can do this, you can begin to reconstruct the keys. The partial key recoveries lead to more plaintext recoveries, and by working back and forth between keys and plaintext, you can complete the solution. There are many ways in which you can identify plaintext. The more you know about the senders of enciphered traffic and the situation in which it was sent, the more likely you are to be able to assume plaintext correctly.

a. **Stereotypes.** Military organizations tend to do things in standard ways. Rules for message formats are likely to be used. Standard forms are likely to be used for recurring needs. When you learn enough about the sender's standard ways of doing things, you can use those standards. Standard formats are most likely to be found in message beginnings and endings. Messages are likely to begin with addressees, message subjects, security classifications, and references to other messages. Messages are likely to end with signatures or unit identifications. These stereotypes are bad security practices, but difficult to avoid.

(1) Consider the following example of a message where stereotypes can be used to achieve a quick solution. The previous message from the same sender, already recovered, began, *TWO PART MESSAGE PART ONE.* The text gave the itinerary of a visiting team of officers from an allied country, but was incomplete. A mixed alphabet was used with the previous message, but it has changed with the new message.

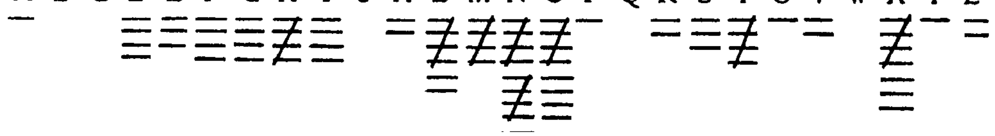
```
ZZZZZ NSHIX LNFOM MXKOI XLNNS  HNOXF STDDR OIXLN XNMTU NOOGN

ETLNV EHPLM YVEOD TZHIN OLLDA  HGOMZ HFFXG RTGKX ZZZZZ
```

(2) The first and last groups (ZZZZZ) are obviously not part of the text of the message. They are probably indicators of some kind.

(3) We begin by preparing the following worksheet with a frequency count and underlined repeats. The indicator groups are not included in the frequency count.

```
NSHIX   LNFOM   MXKOI   XLNNS   HNOXF
STDDR   OIXLN   XNMTU   NOOGN   ETLNV
EHPLM   YVEOD   TZHIN   OLLDA   HGOMZ
HFFXG   RTGKX
```

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:

c: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```



(4) If this is a follow-on to the message that began, *TWO PART MESSAGE PART ONE*, we would assume that it would begin *TWO PART MESSAGE PART TWO*. The underlined repeats are positioned perfectly for the repeated words *TWO* and *PART*, so the assumption seems well borne out.

(5) Next, we enter the assumed text in the message and the alphabet. Using those recovered values throughout the message produces the text shown below.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F
----- ---------                 --------- -------

w           e p a r t   a t s       t e e   t         r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V
              -------

  o   r s         e         o p t   e r r       o   e s
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a             g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X       O   K           F   H I   L M N     S
```

(6) From the recovered ciphertext letters, it appears that the cipher sequence is keyword mixed. On that basis, ciphertext G and J are placed in alphabetical order.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F
----- ---------                 --------- -------

w           e p a r t   a t s       t e e n t         r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V
              -------

  o   r s         e         o p t   e r r       o n e s
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n       n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X       O   K           F G H I J L M N     S
```

(7) Several possibilities for additional plaintext appear in the message with these additions. You may see other possibilities but for illustration, we will add the letters for the word *COMMANDING* appearing at the end of the message.

```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w i     d   e p a r t   a t s i     t e e n t     i r t
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

  o   r s         e     i c o p t   e r r       o n e s c
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n   d i n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X   Z R O   K   T       F G H I J L M N     S
```

(8) Additional placements are possible. Ciphertext Y belongs between X and Z. P and Q fit between N and S. U, V, and W fit between Sand X. The first word on the second line appears to be WILL. The phrase SIXTEEN THIRTY HOURS appears.

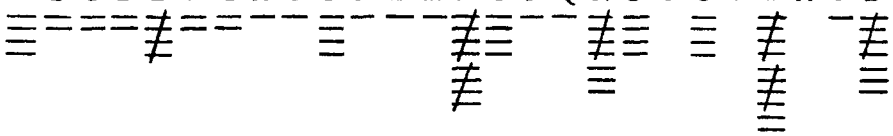
```
t w o p a   r t m e s   s a g e p   a r t t w   o t e a m
N S H I X   L N F O M   M X K O I   X L N N S   H N O X F

w i l l d   e p a r t   a t s i x   t e e n t   h i r t y
S T D D R   O I X L N   X N M T U   N O O G N   E T L N V

h o u r s   b y h e l   i c o p t   e r r l     o n e s c
E H P L M   Y V E O D   T Z H I N   O L L D A   H G O M Z

o m m a n   d i n g a
H F F X G   R T G K X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X Y Z R O   K E T     D F G H I J L M N P Q S U V W
```

Only the ciphertext letters A, B, and C remain to be placed. Of those, only A is used in the text, and it appears to be part of the commander's name. If C is placed as part of the keyword ROCKET and A and B placed in alphabetical order, the commander's name becomes *R L JONES.* The plaintext is *TWO PART MESSAGE PART TWO TEAM WILL DEPART AT SIXTEEN THIRTY HOURS BY HELICOPTER R L JONES COMMANDING.* The complete alphabet is shown below.

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X Y Z R O C K E T A B D F G H I J L M N P Q S U V W
```

b. **Exploitation of Numbers.** Not all cryptograms will include such stereotyped beginnings and endings. Without these stereotypes, repeated words in the text offer another possible point of entry. Spelled out numbers are often easy to recognize when they repeat in messages, as shown in the next example.

```
H W B N F  W A Z A O  U R R W L  W W Z M U  O J R N E

J Y I S J  R J O Q W  E U D R C  W R S Z N  N P W A Z

R C W E N  B N O K F  G N Z W E  U D R S Z  N N G N Z

W S W A Z  E X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:

c: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```



(1) The pattern of consecutive short three- to five-letter repeats is characteristic of numbers. Numbers tend to occur with each other in such things as grid coordinates, times, and quantities. In the above example, the repeated RSZNN must be *THREE,* the only five letter number to end in a double letter. We begin by placing *THREE* in the alphabet and entering other occurrences of the same letters.

```
      e        r        t t          r          t e
H W B N F  W A Z A O  U R R W L  W W Z M U  O J R N E

      h    t                t      t h r e  e       r
J Y I S J  R J O Q W  E U D R C  W R S Z N  N P W A Z

t       e    e          e r          t h r  e e   e r
R C W E N  B N O K F  G N Z W E  U D R S Z  N N G N Z

  h     r
W S W A Z  E X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:          N     S                   Z   R
```

(2) The recovered letters suggest additional numbers. RCW, which begins with plaintext T must be *TWO.* GNZW, which includes ER as the middle two letters must be *ZERO.* EUD, which has no letters in common with THREE, TWO, or ZERO, can only be *SIX*.

```
  o   e    o   r      i t t o    o o r   i      t e s
H W B N F  W A Z A O  U R R W L  W W Z M U  O J R N E
           -----

      h    t       o  s i x t w  o t h r e  e   o   r
J Y I S J  R J O Q W  E U D R C  W R S Z N  N P W A Z
                      ----- ---  ---------      -----

t w o s e    e        z e r o s  i x t h r  e e z e r
R C W E N  B N O K F  G N Z W E  U D R S Z  N N G N Z
-----                 ------- ----- -------- --- -----

o h o   r  s
W S W A Z  E X X X X
-   -----

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:         N     S U           W     Z E R     C D   G
```

(3) Several more possibilities can be placed at this point. Ciphertext F can be placed between D and G in the cipher sequence as the alphabetical structure begins to appear. The last word of the message is apparently *HOURS*, needing only the U to complete it. The partially repeated *FOUR* can be seen at the end of line two, and *SEVEN* follows *TWO* on the third line.

```
  o v e y  o u r u n  i t t o    o o r   i  n   t e s
H W B N F  W A Z A O  U R R W L  W W Z M U  O J R N E
           -----

      h    t   n   o  s i x t w  o t h r e  e f o u r
J Y I S J  R J O Q W  E U D R C  W R S Z N  N P W A Z
                      ----- ---  ---------

t w o s e  v e n   y  z e r o s  i x t h r  e e z e r
R C W E N  B N O K F  G N Z W E  U D R S Z  N N G N Z
-----                 ------- ----- -------- --- -----

o h o u r  s
W S W A Z  E X X X X
-   -----

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:         N P   S U         O W     Z E R A B C D F G
```

(4) The first word is *MOVE.* Q can be placed between P and S in the cipher sequence. The word *BY* completes the third line. With ciphertext K placed from the word *BY,* ciphertext L and M can also be placed.

```
m o v e y   o u r u n   i t t o c   o o r d i   n   t e s
H W B N F   W A Z A O   U R R W L   W W Z M U   O J R N E
            -----

      h     t   n g o   s i x t w   o t h r e   e f o u r
J Y I S J   R J O Q W   E U D R C   W R S Z N   N P W A Z
                        ----- ------- -----------   -----

t w o s e   v e n b y   z e r o s   i x t h r   e e z e r
R C W E N   B N O K F   G N Z W E   U D R S Z   N N G N Z
-----                   -------     --- ----------- -----

o h o u r   s
W S W A Z   E X X X X
-   -----

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:   K L M N P Q S U       H O W     Z E R A B C D F G
```

(5) *COORDINATES* online one provides the plaintext letter A as ciphertext J. With J placed in the alphabet, the letter I must be in the keyword, along with T, which will not fit in the alphabetic progression. The keyword is therefore *HOWITZER.* The complete plaintext is *MOVE YOUR UNIT TO COORDINATES ALPHA TANGO SIX TWO THREE FOUR TWO SEVEN BY ZERO SIX THREE ZERO HOURS.*

c. **Word Patterns.** When neither stereotypical beginnings and endings nor repeated numbers provide a point of entry, repeated words can often be recognized by their patterns of repeated letters.

(1) Such words as ENEMY, ATTACK, and DIVISION have repeated letter patterns that make them easy to recognize. They are even easier to recognize when the words are repeated in the text. Underlining the repeats gives an indication of where the words begin and end. For example, ATTACK and BATTALION have the same pattern of repeated letters. If the ciphertext OGGORF is repeated in the text, it is much more likely to be ATTACK than a portion of the word BATTALION. It could also be EFFECT, ATTAIN, or a number of other possibilities.

(2) In the case where two or more words have identical patterns, such as ATTACK and EFFECT, letter frequencies can help to decide between the possibilities. If the letters O and F of OGGORF are high frequency letters and the rest are fairly low, it is more likely to be EFFECT than ATTACK. If all the letters are high in frequency, ATTAIN is likely.

(3) Tables have been compiled of common pattern words for various languages to assist in analysis. Table D-3 in Appendix D of this manual provides an English

language word pattern table. Word patterns are also called *idiomorphs.* There is a formal procedure for recording word patterns, which is followed in the table. When you find a pattern word repeated in a cryptogram, you can follow the same procedure to record the pattern and then look it up in the table. The procedure is this—

- Find the first repeated letter in the pattern, and designate all occurrences of that character with the letter A.

```
G R F L Y M F P A R P Z
  A               A
```

- Continue lettering alphabetically from left to right, making sure that each new character gets the next letter of the alphabet and each repeated character gets the same letter.

```
G R F L Y M F P A R P Z
  A B C D   B     A
```

- Stop lettering when the **last** occurrence of the last repeated character is reached. In the example, P is the last occurrence of the last repeated character. The final character Z is not lettered.

```
G R F L Y M F P A R P Z
  A B C D E B F G A F
```

- Designate any characters before and after the pattern characters with dashes to show the length of the word.

```
G R F L Y M F P A R P Z
- A B C D E B F G A F -
```

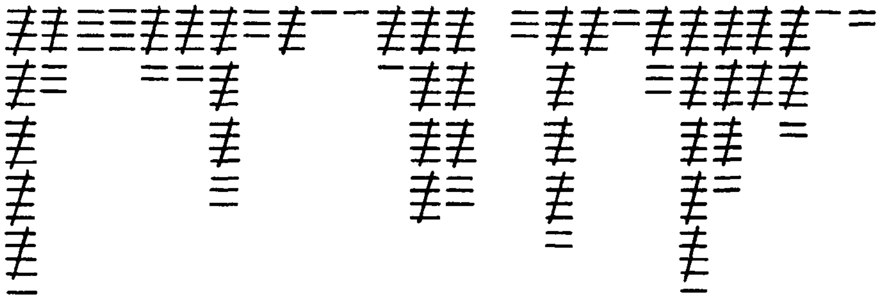
(4) To use the pattern, refer to Appendix D, Table D-3. The patterns are in alphabetical order beginning on page D-19. The pattern ABCDEBFGAF is located on page D-34. The only word listed for this pattern is *H EADQUARTER* S. The extra letters at the beginning and end of the pattern, designated by the dashes, fit HEADQUARTERS perfectly.

(5) The use of word patterns to solve a cryptogram is shown in the next example.

```
XGGXF SEALL KQIAV XGJQM UNAHD
PVWMQ WGUTU MMUET UMVAV IAVBA
FAVAG ZURFM UNNMU XWNGD MQQNA
HGEUN GUCZU PMMQI ATQVG EALLN
CQXMD QXWXG GXFSN GUCWA BANAU
VFUTT XVWEA LLTUB QRUME XMWRM
UTFMU NNMUX WNGEU RABQV AVQGU
MUXWY PVFGA UVQAI DGNQB QVNAH
NGUCU VQRAB QMQIA TQVGA NWABA
NAUVM QNQMB QXXXX
```

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:
```

```
c: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```



(6) The cryptogram shows all repeats longer than three letters. There are a number of shorter repeats, too, which will be used if necessary. We begin the analysis by deriving the word patterns for the longer repeats. The pattern and possible words from Appendix D for each repeat are shown below.

XGGXFS	FMUNNMUXWNG	MQIATQVG	WABANAUV
ABBA--	-ABCCABDEC-	-ABCDA--	-ABACA--
AFFAIR	CROSSROADS?	SABOTAGE	CEMETERY
ATTACH		EASTWARD	VICINITY
ATTACK		REGIMENT	DIMINISH
ATTAIN		INTERNAL	CIVILIAN
EFFECT		INTRENCH	DIVISION
OPPOSE			MONOPOLY

(7) *CROSSROADS* is the only choice for the second patten. There is an extra letter at the end of the repeat, but that may have been caused accidentally by a repeated first letter of the next word in each case. Using *CROSSROADS* as a trial starting point, we compare common letters with the other repeats. From *CROSSROADS*, we see that cipher M equates to plaintext R, for example. Examining the possible choices for the MQIATQVG repeat, only REGIMENT is consistent with the Rp-Mc pair. Similarly, the Op-Uc and Dp-Wc pairs of *CROSSROADS* are consistent with *DIVISION* for the WABANAUV repeat and no others. The common plaintext N and I between REGIMENT and DIVISION also equate to the same cipher letters (V and A) giving further evidence that we are on the right track. Using the common letters between *CROSSROADS*, REGIMENT, and DIVISION with the XGGXFS possibilities shows that either ATTACH or ATTACK is consistent with the first three. We now place the letters of *CROSSROADS*, *REGIMENT*, and *DIVISION* in the alphabet and cryptogram.

```
a t t a c     i           e g i n   a t   e r   o s i
X G G X F   S E A L L   K Q I A V   X G J Q M   U N A H D

  n d r e   d t o m o   r r o   m   o r n i n   g i n v i
P V W M Q   W G U T U   M M U E T   U M V A V   I A V B A

c i n i t     o   c r   o s s r o   a d s t     r e e s i
F A V A G   Z U R F M   U N N M U   X W N G D   M Q Q N A

  t   o s   t o     o     r r e q   i m e n t     i     s
H G E U N   G U C Z U   P M M Q I   A T Q V G   E A L L N

  e a r     e a d a t   t a c   s   t o   d i   v i s i o
C Q X M D   Q X W X G   G X F S N   G U C W A   B A N A U

n c o m m   a n d   i       m o v   e   o r     a r d   r
V F U T T   X V W E A   L L T U B   Q R U M E   X M W R M

o m c r o   s s r o a   d s t   o     i v e n   i n e t o
U T F M U   N N M U X   W N G E U   R A B Q V   A V Q G U

r o a d       n c t i   o n e i g     t s e v   e n s i
M U X W Y   P V F G A   U V Q A I   D G N Q B   Q V N A H

s t o   o   n e   i v   e r e g i   m e n t i   s d i v i
N G U C U   V Q R A B   Q M Q I A   T Q V G A   N W A B A

s i o n r   e s e r v   e
N A U V M   Q N Q M B   Q X X X X

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: X   F W Q   I   A       T V U     M N G   B
```

(8) With this start, you should be able to see many more possible plaintext words in the text. *TOMORROW*, *VICINITY*, and *ROAD JUNCTION* all appear with

only one or two letters missing. Many spelled out numbers also appear. The repeated NGUC is *STOP*, a common stereotype used in telegraphic text in place of a period. EALL is *WILL*. XGGXFS must be *ATTACK*. The completed plaintext is—

"ATTACK WILL BEGIN AT ZERO SIX HUNDRED TOMORROW MORNING IN VICINITY OF CROSSROADS THREE SIX TWO STOP YOUR REGIMENT WILL SPEARHEAD ATTACK STOP DIVISION COMMAND WILL MOVE FORWARD FROM CROSSROADS TWO FIVE NINE TO ROAD JUNCTION EIGHT SEVEN SIX STOP ONE FIVE REGIMENT IS DIVISION RESERVE.“

(9) Use of word patterns is a powerful tool to gain entry into a cryptogram. It will not always work out as easily as the example shown here. Repeated letters do not always represent repeated words. Many words that are used in messages will not be found in the word pattern tables, particularly proper names. Be alert to the patterns of repeated letters in names you would expect to find in message traffic. If you can recognize the pattern of a word, it does not have to be in the tables to use it.

4-13. Vowel-Consonant Relationships

When you can successfully discover plaintext words in a cryptogram, the solution usually comes quickly. Sometimes you will encounter a cryptogram in which you can find no basis to assume plaintext. You can find no stereotypes, no usable numbers, and no repeated pattern words. In these cases, you can use the characteristics of the language itself to determine individual letters.

a. **Language Characteristics.** Languages which use an alphabet to spell out words phonetically produce exploitable letter relationships. To make words pronounceable, vowels and consonants tend to alternate. We do not expect to find many consonants or many vowels consecutively. In cases where they do, the possibilities are limited to pronounceable combinations. Exploitation of these letter relationships begins by determining which letters are consonants and which are vowels.

(1) Vowels tend to occur next to consonants. Consonants tend to occur next to vowels. Each contacts the other more readily than it contacts its own type.

(2) Since there are more consonants than vowels in English, vowels tend to contact more different letters than consonants do. A vowel will commonly contact a lot of different consonants, whereas a consonant will tend to contact the smaller number of vowels. By studying which letters contact each other and how many different contacts each letter has, we can sort ciphertext letters into vowels and consonants fairly reliably.

(3) To make use of these vowel-consonant relationships, we use a special kind of frequency count which charts contacts as well as frequencies.

b. **Trilateral Frequency Count.** The trilateral frequency count is used to record, for each letter in a cryptogram, the letter that precedes it and the letter that follows it. Figure 4-4 shows a cryptogram and its trilateral frequency count. The pairs of letters appearing in the column below each letter of the alphabet are the preceding and following letters for each occurrence. For example, the YG that appears below the letter A shows that the first A in the cryptogram occurred as part of the segment YAG. Refer to the cryptogram itself, and you will see that the segment YAG occurs in the second group of the message. Two numbers appear above each letter of the alphabet. The top figure is the frequency of that letter, which is the same as the number of pairs of letters in the column below it. The second number is the number of different letters the basic letter contacts. This type of frequency distribution and its supporting contact information take some time to prepare by hand, but they can lead to the solution when other methods fail.

```
LBWYR YAGGB GIOYF BATGT BUUBV
GKBSK TEEAT HBUYA YWYUF QVTWY
VJVBA ATUDR TEECY DTUIG XYYBS
TWYKN UQVYQ FQFVY FIVIG BVPST
VYART EEAGB FIGXY VBSBN VSTWY
UTUYX

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:
```

Frequency:	8	13	1	2	6	6	9	1	5	1	3	1	-	2	1	1	4	3	5	13	9	12	5	3	16	-
Contacts:	7	12	2	4	4	6	8	2	5	1	6	1	-	4	2	2	4	4	5	12	9	11	3	2	12	-
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	YG	LW	EY	UR	TE	YB	AG	TB	GO	VV	GB	-B		KU	IY	VS	FV	YY	BK	AG	BU	BG	BY	GY	WR	
	BT	GG		YT	EA	UQ	GB		UG		ST			BV			UV	DT	BT	GB	UB	QT	YY	GY	RA	
	ET	FA			TE	QQ	BI		FV		YN						YF	AT	PT	KE	BY	YJ	TY	Y-	OF	
	YY	TU			EC	QV	TT		VG								FF		BB	AH	YF	JB	TY		UA	
	BA	UV			TE	YI	VK		FG										VT	VW	TD	YB	TY		AW	
	AT	KS			EA	BI	IX													AU	TI	QY			WU	
	YR	HU					IB													RE	NQ	FY			WV	
	EG	VA					AB													DU	YT	II			CD	
		VS					IX													SW	TY	BP			XV	
		GV																		SV		TY			WK	
		GF																		RE		YB			VQ	
		VS																		SW		NS			VF	
		SN																		UU					VA	
																									XV	
																									WU	
																									UX	

Figure 4-4. Triliteral frequency distribution.

(1) The contact information is used to determine which ciphertext letters are vowels and which are consonants. More often than not, the highest frequency plaintext letter is a vowel, even when E is not the highest frequency letter. An even more reliable indicator is the number of contacts. The letter that contacts the most different letters will usually be a vowel. In the example in Figure 4-4, ciphertext Y is likely to be a vowel for both reasons. The letters that Y contacts most frequently are likely to be consonants.

(2) In cases where there are several letters all about the same frequency and no letter stands out as a likely vowel, we can begin our approach through likely consonants instead. All or most of the lowest frequency letters should be consonants. The letters they contact most frequently are likely to be vowels.

(3) We can use either a likely vowel or the set of likely low frequency consonants as our starting point. Whichever we start with, we will use both as the problem develops. The object is to separate the consonants and vowels by plotting the contacts of each in separate vowel and consonant line charts.

(4) For our example, we will pick the low frequency consonants as the starting point. The process begins by charting the contacts of the lowest frequency letters. We will begin with the letters that only occurred once in Figure 4-4–C, H, J, L, O, and P. Draw a horizontal line two to three inches long and write the selected letters above it. Draw a vertical line several inches from the center of the horizontal line producing a T-shaped figure. This is the consonant line. The contacts are charted on the line with the first letters of each pair to the left and the second to the right. Each new contact letter is charted on a new row. With the contacts for C, H, J, L, O, and P charted, the consonant line appears below.

C H J	L O P
E	
	YY
T	
	BB
VV	V
I	
	S

(5) Continue adding the lowest frequency letters one frequency group at a time. We first placed those with a frequency of one. Next add those with a frequency of two. Continue with those with a frequency of three and so on. Stop when the next frequency would represent more than 20 percent of the total. Going any further raises the chance too high of including a vowel that would bias the chart. If a vowel occurs only once or twice and is included, its influence will be small. If it occurs five or six times and we include it, it could lead to wrong follow-on

decisions on vowels and consonants. In our example, there are 130 letters. We want to keep our sample below 20 percent, or not more than 26 letters altogether. On this basis, we can add the frequencies of 2, 3, and 4, but not 5.

D N K C H J	R X Q L O P
E	
YYYYY	YYYYY
T	TTTT
B	BBB
VV	VVVV
I	
S	S
UU	U
	R
K	
GGG	
	N
D	
A	
FF	FF

(6) The consonant line now shows that the low frequency consonants contact the ciphertext letter Y more than any other letter. The probability is very high that this is a vowel. It is tempting to select the letter V as a vowel, but it is better to proceed one letter at a time at this point.

(7) Using the letter Y and its contacts, we next begin construction of a vowel line. It is charted exactly the same as the consonant line chart. The vowel line including just the letter Y's contacts is shown below.

Y	
WWWWW	W
R	R
A	AAA
O	
	FF
UU	UU
VVV	VVV
C	
	D
XX	X
	K
	Q

(8) The vowel line shows us we were correct in not initially accepting the letter V as a vowel. It contacts the low frequency consonants quite readily, but it also contacts a vowel readily. It may be a consonant such as R, L, or N which easily

combines with other consonants. We will not try to place V in either line at this point.

(9) The letter W contacts Y six times and is a likely consonant. We will continue by going back to the consonant line and adding W.

W

C H J L O P	D N K R X G
E	
YYYYYY	YYYYYYYYYY
TTTT	TTTT
BB	BBB
VV	VVVV
I	
S	S
UU	U
	R
K	
GGG	
	N
D	
A	
FF	FF

Y

WWWWW	W
R	R
A	AAA
O	
	FF
UU	UU
VVV	VVV
C	
	D
XX	X
	K
	Q

(10) The letter T now appears as a strong candidate for a vowel. It is second only to Y in consonant contacts so far, and just as importantly, it does not contact the already selected vowel at all. We add T and its contacts to the vowel line.

W

C H J L O P	D N K R X G
E	
YYYYYY	YYYYYYYYYY
TTTT	TTTT
BB	BBB
VV	VVVV
I	
S	S
UU	U
	R
K	
GGG	
	N
D	
A	
FF	FF

YT

WWWWW	WWWW
RRR	R
AAAA	AAA
O	
	FF
UUU	UUUUU
VVVV	VVVV
C	
D	D
XX	X
K	K
	Q
G	G
	B
	EEE
	H
SSS	

(11) The vowel line shows A and U as likely consonants. Adding these letters to the consonant line produces the next diagram.

A U W
C H J L O P D N K R X G

EEE	
YYYYYYYYYYY	YYYYYYYYYYYYY
TTTTTTT	TTTTTTTT
BBBBBB	BBBB
VV	VVVV
I	I
S	S
UUU	UU
	RR
K	
GGG	GG
N	N
D	D
AA	A
FF	FFF
	Q

YT

WWWWW	WWWW
RRR	R
AAAA	AAA
O	
	FF
UUU	UUUUU
VVVV	VVVV
C	
D	D
XX	X
K	K
	Q
G	G
	B
	EEE
	H
SSS	

(12) B appears to be a vowel. This is reinforced by the letters BUUB in the first line of the text. If U was correctly selected as a consonant, B is probably a vowel on the basis of this letter pattern. It is a good idea at this point to return to the text and underline all the recovered vowels.

```
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V
  -   -     -       -         -     -   -   -   -     -
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y
    -       -       -     -   -     -   -           -   -
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S
      -       -         -       -     -           -   -
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T
-   -             -             -               -       -
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y
  -     -           -           -     -   -         -   -
U T U Y X
  -   -
```

p: a b c d e f g h i j k l m n o p q r s t u v w x y
c:

A U W
C H J L O P D N K R X G

EEE	
YYYYYYYYYYY	YYYYYYYYYYYYY
TTTTTTT	TTTTTTTT
BBBBBB	BBBB
VV	VVVV
I	I
S	S
UUU	UU
	RR
K	
GGG	GG
N	N
D	D
AA	A
FF	FFF
	Q

BYT

WWWWW	WWWWW
RRR	R
AAAA	AAAAA
O	
F	FF
UUUU	UUUUUUU
VVVVVVV	VVVVVV
C	
D	D
XX	X
KK	K
	Q
GGGG	GG
	B
	EEE
H	H
SSSS	SSS
L	
	N
T	

(13) Examination of the vowel-consonant patterns in the text confirms additional consonants. Double letters preceding or following the vowel are very unlikely to be vowels. We can then assign ciphertext E and Gas consonants. The GGBG segment on the first line could not all be vowels. EE occurs three times in the text following a vowel.

(14) V appears to be a consonant from the number of contacts in the vowel line, and its appearance between vowels in the segments YVB and TVY confirm it as a consonant. Placing G, E, and V in the consonant line produces this diagram.

A U W G E V
C H J L O P D N K R X Q

EEEEEE	EEE
YYYYYYYYYYYYYY	YYYYYYYYYYYYYYYY
TTTTTTTTTTTT	TTTTTTTTTT
BBBBBBBBB	BBBBBBBBBB
VVV	VVVV
I I I I I	I I I
S	SS
UUU	UU
	RR
K	K
GGGG	GGGG
NN	N
D	D
AAAA	AAA
FFF	FFF
QQ	Q
J	J
	P
	C
	XX

BYT

WWWWW	WWWWW
RRR	R
AAAA	AAAAA
O	
F	FF
UUUU	UUUUUUU
VVVVVVV	VVVVVV
C	
D	D
XX	X
KK	K
	Q
GGGG	GG
	B
	EEE
H	H
SSSS	SSS
L	
	N
T	

(15) The letters F, I, and S remain unidentified. At least one of these is likely to be a vowel, since four of the letters are expected to be vowels and we have only identified three so far. Comparing the appearance of F, I, and S in the vowel and consonant lines, we see that the letter I is the best candidate for a vowel. The letter I does not appear on the vowel line at all, whereas, F and S directly contact a number of the recovered vowels. We now underline I in the text and add it to the vowel line.

```
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V
  -   -     -       -     -   -     -   -   -   -     -
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y
    -       -       -     -   -     -   -           -   -
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S
      -       -         -       -     -   -       -   -
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T
-   -             -             -     -   -     -       -
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y
  -     -           -     -     -     -   -         -   -
U T U Y X
  -   -
```

```
p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c:
```

A U W C H J L O P	G E V D N K R X Q
EEEEEE	EEE
YYYYYYYYYYYYYY	YYYYYYYYYYYYYYYY
TTTTTTTTTTTT	TTTTTTTTTT
BBBBBBBBB	BBBBBBBBBB
VVV	VVVV
IIIII	III
S	SS
UUU	UU
	RR
K	K
GGGG	GGGG
NN	N
D	D
AAAA	AAA
FFF	FFF
QQ	Q
J	J
	P
	C
	XX

BYT I	
WWWWW	WWWWW
RRR	R
AAAA	AAAAA
O	O
FFF	FFF
UUUUU	UUUUUUU
VVVVVVVV	VVVVVVV
C	
D	D
XX	X
KK	K
	Q
GGGGG	GGGGG
	B
	EEE
H	H
SSSS	SSS
L	
	N
T	

(16) There are a number of directions you can take at this point. No single example can demonstrate them all. Some of the approaches that can be tried are—

- To analyze vowel combinations to determine individual vowels.

- To search for the plaintext consonants N and H. These two letters have typical patterns of contact with consonants and vowels. N tends to follow vowels and precede consonants. H tends to follow consonants and precede vowels. In some cryptograms these features will be very evident in the vowel and consonant line diagrams. In others, they will not stand out at all.
- To recover double letters by frequency analysis. Plaintext LL is the most frequent double consonant. EE and OO are the most frequent double vowels.
- To recover common word endings such as -ING and -TION, which often appear as repeats even when complete words do not repeat.

(17) We will use several of these approaches to complete the solution of the sample problem. First, one vowel combination appears in the cryptogram, the ciphertext TB as part of the segment TGTBU. Referring to the two-letter frequency data in Appendix A, page A-2, the most frequent vowel combinations are EE, IO, OU, and EA. TB is not EE, because it is not a double letter. It is likely to be one of the other three. IO is particularly significant, because it is usually part of a -TION combination when it appears. The letters G and U, which precede and follow BT in the text, are high frequency consonants and support the -TION possibility. The letter T occurs again before G, which would produce -ITION, a very good letter combination.

(18) If TGTBU is -ITION, the letter U may appear with the typical pattern of plaintext N. Examining the occurrence of U in the vowel and consonant lines, we see that U follows vowels more often than it precedes them. It also precedes consonants more often than it follows. The differences are slight, but they help to confirm the initial assumption.

(19) Ciphertext EE occurs three times. This is likely to be plaintext LL. Each time it is preceded by ciphertext T, which we have tentatively identified as the plaintext I. ILL is another good combination that appears as part of many common words such as HILL and WILL.

(20) Y is the most common letter, and it is a vowel. While we would not usually begin analysis by assuming the most common vowel is E, our tentative identification of I and O make this much more likely. If Yc is Ep, then the remaining high frequency vowel, Ic, is probably Ap.

(21) Placing all the tentative recoveries in the cryptogram produces the next example.

```
  o   e     e   t t o   t a   e     o   i t i   o n n o
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V
  -   -     -       -     -   -     -   -   -   -     -

t   o       i l l   i     o n e     e   e n         i   e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y
    -       -       -     -   -     -   -           -   -

      o       i n       i l l   e     i n a t     e   o
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S
      -       -         -       -     -   -       -   -

i   e       n     e             e     a   a t   o       i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T
-   -             -             -     -   -     -       -

  e     i   l l   t o     a t   e     o   o         i   e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y
  -     -           -     -     -     -   -         -   -

n i n e
U T U Y X
  -   -

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I       Y       T     E   U B         G
```

(22) With the assumed letters filled in, two numbers stand out. *ONE* appears in the second line, and *NINE* appears in the last line. Since numbers tend to occur with each other, our next objective is to try to place additional numbers adjacent to these two. If we try *SEVEN* after *ONE* because of the -E-EN pattern, it leads to the recovery of *SIX* before *ONE* and *FIVE* before *NINE.*

(23) All of the high frequency plaintext letters except R are now recovered. Vc is the obvious candidate for Rp due to its high frequency and appearance in the text.

(24) Placing plaintext S, V, X, F, and R reveals this text.

```
  o v e     e s t t o   t a   e     o s i t i   o n n o r
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V
  -   -     -       -     -   -     -   -   -   -     -

t   o f     i l l s i   x o n e s   e v e n       r i v e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y
    -       -       -     -   -     -   -           -   -

r   r o s   s i n       i l l   e     i n a t     e r o f
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S
      -       -         -       -     -   -       -   -

i v e       n   r e           r e     a r a t   o r   f i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T
-   -             -             -     -   -     -       -

r e s   i   l l s t o     a t   e   r o f o     r f i v e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y
  -     -           -     -     -     -   -         -   -

n i n e
U T U Y X
  -   -

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I       Y S     T     E   U B     V A G   W   H
```

(25) Many possibilities for plaintext appear now. *ZERO*, *POSITION*, *RIVER CROSSING*, *PREPARATORY*, and *FOUR* can all be seen upon close examination.

```
m o v e w   e s t t o   t a k e p   o s i t i   o n n o r
L B W Y R   Y A G G B   G I O Y F   B A T G T   B U U B V
  -   -     -       -     -   -     -   -   -   -     -

t h o f h   i l l s i   x o n e s   e v e n p   d r i v e
G K B S K   T E E A T   H B U Y A   Y W Y U F   Q V T W Y
    -       -       -     -   -     -   -           -   -

r c r o s   s i n g w   i l l b e   g i n a t   z e r o f
V J V B A   A T U D R   T E E C Y   D T U I G   X Y V B S
      -       -         -       -     -   -       -   -

i v e h u   n d r e d   p d p r e   p a r a t   o r y f i
T W Y K N   U Q V Y Q   F Q F V Y   F I V I G   B V P S T
-   -             -             -     -   -     -       -

r e s w i   l l s t o   p a t z e   r o f o u   r f i v e
V Y A R T   E E A G B   F I G X Y   V B S B N   V S T W Y
  -     -           -     -     -     -   -         -   -

n i n e
U T U Y X
  -   -

p: a b c d e f g h i j k l m n o p q r s t u v w x y z
c: I C J Q Y S D K T ? O E L U B F ? V A G N W R H P X
```

(26) Analysis of the cipher sequence shows it to be a simply transposed keyword mixed sequence, which identifies Jp as Zc and Qp as Mc.

I	S	O	B	A	R
C	D	E	F	G	H
J	K	L	M	N	P
Q	T	U	V	W	X
Y	Z				

CHAPTER 5

MONOALPHABETIC MULTILITERAL SUBSTITUTION SYSTEMS

Section I

Characteristics and Types

5-1. Characteristics of Multilateral Systems

As explained in Chapter 3, monoalphabetic unilateral systems are those in which the ciphertext unit is always one character long. Multilateral systems are those in which the ciphertext unit is more than one character in length. The ciphertext characters may be letters, numbers, or special characters.

a. **Security of Multilateral Systems.** By using more than one character of ciphertext for each character of plaintext, encipherment is no longer limited to the same number of different cipher units as there are plaintext units. Although there is still only one alphabet used in multilateral systems, the alphabet can have more than one ciphertext value for each plaintext value. These variant ciphertext values provide increased security. Additionally, the plaintext component of alphabets can be expanded easily to include numbers, punctuation, and common syllables as well as the basic 26 letters. When used, the variation in encipherment and the reduced spelling of numbers, punctuation, and common syllables minimize the exact weaknesses that we used in Chapter 4 to break into unilateral systems.

b. **Advantages and Disadvantages.** The increased security possible with variant multilateral systems is the major advantage. The major disadvantage is that by substituting more than one character of ciphertext for each plaintext value, the length of messages and resulting transmission times are increased. A second disadvantage is that more training and discipline are required to take advantage of the increased security. If training and discipline are inadequate, the security advantages are lost easily.

5-2. Types of Multilateral Systems

Multiliteral systems are further categorized by the type of substitution used. The major types are—

- Biliteral systems, which replace each plaintext value with two letters of ciphertext.
- Dinomic systems, which replace each plaintext value with two numbers of ciphertext.
- Trilateral and trinomic systems, which replace each plaintext value with three letters or numbers of ciphertext.
- Monome-dinome systems, which replace plaintext values with one number for some values and two numbers for other values.
- Biliteral with variants and dinomic with variants systems, which provide more than one ciphertext value for each plaintext value.
- Syllabary squares, which may be biliteral or dinomic, and which include syllables as well as single characters as plaintext values.

5-3. Cryptography of Multilateral Systems

The cryptography of each type of multilateral system, including some of the odd variations is illustrated in the following paragraphs. Most of these systems are coordinate matrix systems in which the plaintext values are found inside a rectangular matrix and the ciphertext values consist of the row and column coordinates of the matrix.

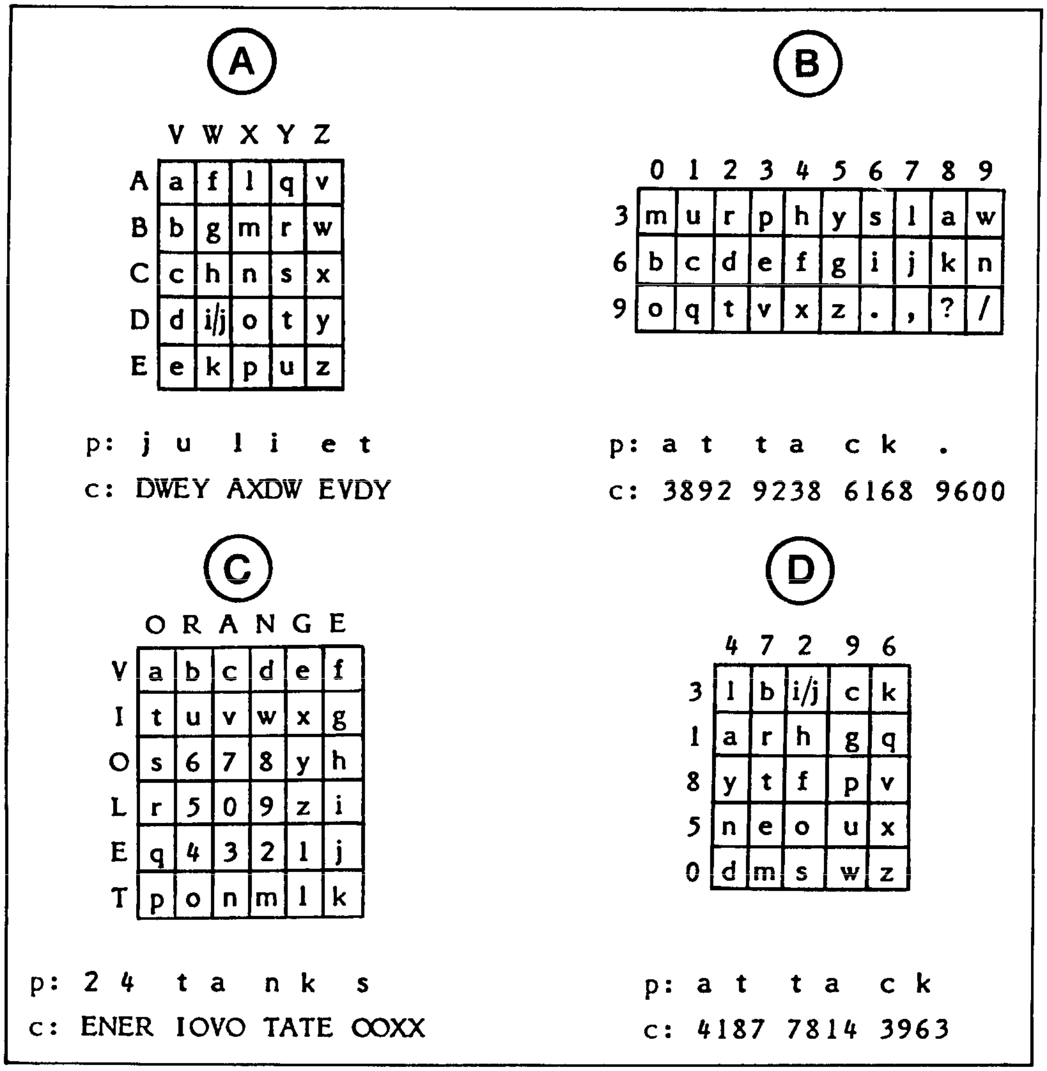
a. **Simple Biliterals and Dinomics.** The simplest multilateral systems use no variation. They typically use a small rectangular matrix large enough to contain the letters of the alphabet and any other characters the system designer wants to use as plaintext values.

(1) The plaintext values are the internals of the matrix. They may be entered alphabetically, follow a systematic sequence, or they may be random. They may be entered in rows, in columns, or by any other route.

(2) The row and column coordinates are the externals. Conventionally, the row coordinates are placed at the left outside the matrix, and the column coordinates are placed at the top. As with the internals, the coordinates may be selected randomly or produced systematically.

(3) A ciphertext value is created by finding the plaintext value inside the matrix and then combining the coordinate of the row with the coordinate of the column for that plaintext value. Either can be placed first, although placing the row coordinate before the column coordinate is more common.

(4) Five by five is a common size for a simple system (Figure 5-1). The 26 letters are fitted into the 25 positions in the matrix by combining two letters. The usual combinations are I and J or U and V. It is up to the deciphering cryptographer to determine which of the two is the correct value. There are few, if any, words in common usage in which good words can be formed using either letter of the I/J or U/V combinations. Other common sizes are 6 by 6 (which gives room for the 10 digits), 4 by 7, and 3 by 10. Many other sizes are possible.



A

	V	W	X	Y	Z
A	a	f	l	q	v
B	b	g	m	r	w
C	c	h	n	s	x
D	d	i/j	o	t	y
E	e	k	p	u	z

p: j u l i e t

c: DWEY AXDW EVDY

B

	0	1	2	3	4	5	6	7	8	9
3	m	u	r	p	h	y	s	l	a	w
6	b	c	d	e	f	g	i	j	k	n
9	o	q	t	v	x	z	.	,	?	/

p: a t t a c k .

c: 3892 9238 6168 9600

C

	O	R	A	N	G	E
V	a	b	c	d	e	f
I	t	u	v	w	x	g
O	s	6	7	8	y	h
L	r	5	0	9	z	i
E	q	4	3	2	1	j
T	p	o	n	m	l	k

p: 2 4 t a n k s

c: ENER IOVO TATE OOXX

D

	4	7	2	9	6
3	l	b	i/j	c	k
1	a	r	h	g	q
8	y	t	f	p	v
5	n	e	o	u	x
0	d	m	s	w	z

p: a t t a c k

c: 4187 7814 3963

Figure 5-1. Biliteral and dinomic matrices.

(5) Example A in Figure 5-1 is a simple 5 by 5 matrix with I and J in the same plain-text cell of the square. The coordinates and the sequence within are in alphabetic order.

(6) Example B is a simple 3 by 10 matrix with orderly coordinates and a keyword mixed sequence inscribed within. The four extra cells are used for punctuation marks.

(7) Example C is a 6 by 6 matrix with a spiral alphabetic sequence followed in the spiral with the 10 digits. The coordinates in this case are related words.

(8) Example D is a 5 by 5 matrix with numeric coordinates. The plaintext sequence is keyword mixed entered diagonally. In this case, there is deliberately no repetition between the row and column coordinates. This allows the coordinates to be read either in row-column order or in column-row order without any ambiguity, as in the sample enciphered text. This is unusual, but you should be alert to such possibilities.

b. **Triliterals and Trinomics.** Trilateral and trinomic systems are essentially the same as biliteral and dinomic systems. The difference is that either the row coordinates or the column coordinates consist of two characters instead of one, creating a three-for-one substitution. Such systems offer no real advantage except to provide a slightly different challenge to the cryptanalyst, and have the distinct disadvantage of tripling the length of messages. They are easily recognized, and offer no increase in security.

	L	M	N	O	P
	V	W	X	Y	Z
A	a	f	l	q	v
B	b	g	m	r	w
C	c	h	n	s	x
D	d	i/j	o	t	y
E	e	k	p	u	z

	0	1	2	3	4	5	6	7	8	9
13	m	u	r	p	h	y	s	l	a	w
26	b	c	d	e	f	g	i	j	k	n
39	o	q	t	v	x	z	.	,	?	/

p:	j	u	l	i	e	t
c:	DMW	EOY	ANX	DMW	ELV	DOY

p:	a	t	t	a	c	k
c:	138	392	392	138	261	268

c. **Monome-Dinomes.** Monome-dinomes are coordinate matrix systems constructed so that one row has no coordinate. The values from that row are enciphered with the column coordinate only. This means that some ciphertext values are two characters in length (dinomes) and others are only one (monomes). If the values used as row coordinates are also used as column coordinates, no plaintext values are placed in the monome row under those repeated column coordinates. The blanking of cells in the monome row is shown in the example below.

	1	2	3	4	5	6	7	8	9	0
-	h	e	x	a	-	-	d	c	i	m
5	l	b	f	g	j	k	n	o	p	q
6	r	s	t	u	v	w	y	z	.	,

p:	e	n	e	m	y	a	t	t	a	c	k	i	n	g
c:	2	57	2	0	67	4	63	63	4	8	56	9	57	54

Resulting message:

25720 67463 63485 69575 40000

(1) If the cells corresponding to the row coordinates in the monome row are not blanked, the deciphering cryptographer will have difficulty. Decipherment proceeds left to right, and when a 5 or a 6 is encountered in the matrix shown, it will always be a row coordinate or combine with a preceding row coordinate. It will never stand alone as a monome. If the 5 and 6 cells were not blanked, the deciphering cryptographer could not tell if a 5 or 6 were a monome or the beginning of a dinome. The cryptographer would have to rely on context to figure out which was intended, and that could lead to errors.

(2) The additional examples of monome-dinomes shown below demonstrate the various ways they can be constructed. The last example (top of page 5-5) is a monome-dinome-trinome.

	7	0	4	8	5	1	3	9	2	6
-	w	i	l	d	-	c	a	t	-	-
6	b	e	f	g	h	j	k	m	n	o
2	p	q	r	s	u	v	x	y	z	.
5	0	1	2	3	4	5	6	7	8	9

	2	4	6	8	0
-	t	e	n	o	r
1	c	b	x	a	s
3	d	f	g	h	i
5	p	m	l	k	j
7	q	u	v	w	y
9	z	.	,	;	:

	1	2	3	4	5	6	7	8	9	0
-	-	-	r	a	m	c	h	i	p	s
1	b	d	e	f	g	j	k	l	n	o
23	q	t	u	v	w	x	y	z	.	0

p: r e q u e s t h e l p

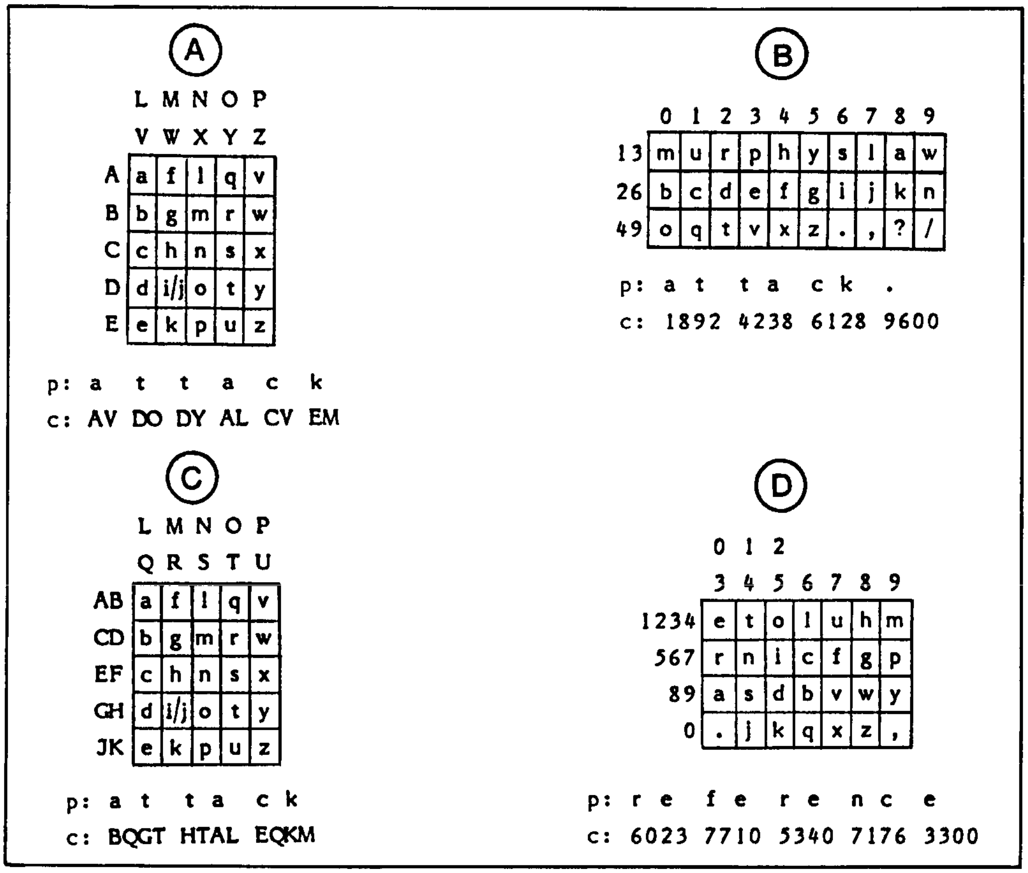
c: 3 13 231 233 13 0 232 7 13 18 9

Resulting message:

31323 12331 3023271318 90000

d. **Variant Systems.** Variants in a multiliteral system allow plaintext characters to be enciphered in more than one way. Variants can be external or internal.

(1) External variant systems have a choice of coordinates. Either row coordinates or column coordinates or both can have variants. Examples A and B in Figure 5-2 provide two ways to encipher every letter.



Ⓐ

	L	M	N	O	P
	V	W	X	Y	Z
A	a	f	l	q	v
B	b	g	m	r	w
C	c	h	n	s	x
D	d	i/j	o	t	y
E	e	k	p	u	z

p: a t t a c k

c: AV DO DY AL CV EM

Ⓑ

	0	1	2	3	4	5	6	7	8	9
13	m	u	r	p	h	y	s	l	a	w
26	b	c	d	e	f	g	i	j	k	n
49	o	q	t	v	x	z	.	,	?	/

p: a t t a c k .

c: 1892 4238 6128 9600

Ⓒ

	L	M	N	O	P
	Q	R	S	T	U
AB	a	f	l	q	v
CD	b	g	m	r	w
EF	c	h	n	s	x
GH	d	i/j	o	t	y
JK	e	k	p	u	z

p: a t t a c k

c: BQGT HTAL EQKM

Ⓓ

	0	1	2				
	3	4	5	6	7	8	9
1234	e	t	o	l	u	h	m
567	r	n	i	c	f	g	p
89	a	s	d	b	v	w	y
0	.	j	k	q	x	z	,

p: r e f e r e n c e

c: 6023 7710 5340 7176 3300

Figure 5-2. External variant systems.

Example C provides four ways to encipher every letter. Example D was constructed to provide the most variants for the most common letters. The letters E, T, and O can all be enciphered in eight different ways. R, N, and I can be enciphered in six different ways. A, S, D, L, U, H, and M can be enciphered in four different ways. Q, X, Z, and the comma can only be enciphered one way. When any of the systems are conscientiously used, repeated words in the text will not produce repeated ciphertext segments.

(2) Internal variant systems use larger matrices to provide variants inside the matrix. Each common plaintext letter appears more than once. Here are two examples of internal variant systems.

	3	0	2	8	6	5	1	4	7	9
7	e	e	e	e	t	t	o	n	i	s
3	e	e	e	t	t	o	r	i	a	d
9	e	e	t	t	o	r	i	a	d	u
1	e	e	t	o	r	n	a	d	u	f
6	e	t	o	r	n	a	d	u	c	m
4	t	o	r	n	a	s	u	c	m	p
8	o	r	n	a	s	l	c	y	g	w
2	r	n	i	s	l	h	y	g	v	k
5	n	i	s	l	h	f	b	v	j	x
0	i	s	l	h	f	b	p	w	q	z

	K	L	M	N	O	P	Q	R	S	T
A	l	u	c	k	y	c	h	a	r	m
B	o	b	j	e	c	t	i	o	n	s
C	g	o	l	d	r	e	c	o	r	d
D	a	f	f	e	c	t	i	o	n	s
E	r	a	p	s	e	s	s	i	o	n
F	i	n	c	e	n	d	i	a	r	y
G	t	r	i	v	i	a	q	u	i	z
H	h	e	a	v	y	m	e	t	a	l
I	m	a	s	t	e	r	w	o	r	k
J	s	i	x	t	y	s	e	v	e	n

The first example above places the letters in the matrix according to their expected frequency in plaintext. If their use is well balanced, all letters in the square will be used with about the same frequency. The second square achieves the same effect by using 10 words or phrases in the rows, which use all the letters. The first letters of the column spell out an eleventh word—logarithms.

e. **Syllabary Squares.** Another type of internal variant system is the syllabary square. This type includes common syllables as well as single letters. When these are used, the same square may be used for a period, changing the coordinates more frequently than the square itself.

	6	0	4	3	8	1	7	5	9	2
8	a	1	ad	al	an	and	as	at	b	2
4	c	3	ce	co	d	4	da	de	di	e
3	5	ea	ec	ed	ee	ei	el	en	ent	er
7	es	et	f	6	fi	fo	g	7	h	8
2	hi	ht	i	9	in	ing	io	ir	is	it
0	j	0	00	k	l	la	le	ll	m	ma
5	n	nd	ne	ng	ni	nt	o	on	or	ou
9	p	q	r	ra	re	ri	ro	rs	rt	s
1	se	si	st	t	ta	te	th	ti	tion	to
6	tw	ty	u	ur	v	ve	w	x	y	z

p:	r	ei	n	fo	r	ce	m	en	t	s
c:	94	31	56	71	94	44	09	35	13	92

p:	re	in	f	or	ce	m	ent	s
c:	98	28	74	59	44	09	39	92

The two sample encipherments of *REINFORCEMENTS* show that a syllabary square suppresses repeats in ciphertext just as single letter variant systems do. It also has the advantage of producing shorter text than single letter multilateral systems.

f. **Sum Checks.** It is very easy for errors to occur when messages are transmitted and received, whatever means of transmission are used. Because of this, some users introduce an error detection feature into traffic known as sum checking.

(1) In its simplest form, a sum-check digit is added to every pair of digits in numeric messages. The digit is produced by adding the pair of digits to produce the

third. If the result is larger than 9, only the second digit is used, dropping the 10's digit, for example 8 plus 9 equals 7 instead of 17. This is also known as modulo 10 arithmetic.

Ciphertext: 42 63 55 47 22 89

Ciphertext with sum check: 426 639 550 471 224 897

(2) Whenever the first two digits do not add up to the third, the receiving cryptographer is alerted that an error has occurred. The cryptographer then tries to figure out the correct digit from context or by assuming that two of the digits are correct and determining what the third should be.

(3) There are many variations on the simple system of sum checking described here. Sometimes the sum-check digit will be placed first or second in each resulting group of three. Sometimes a sum check will be applied to a larger group than two numbers. Sometimes a different rule of arithmetic will be used, such as adding the sum-check digit so that the resulting three always add to the same total. Sometimes a more complex system will be used that provides enough information to resolve many errors as well as detect them, particularly when computers are used in data and text transmissions.

(4) Computer produced sum checks can be used with any characters, not just numbers. Computer produced sum checks will normally be invisible to the user, as they are automatically stripped out when a message is received. They may or may not be invisible to the cryptanalyst. Recovery of computer produced sum checks is well beyond the scope of this text, but you should be alert to their existence.

Section II
Analysis of Simple Multilateral Systems

5-4. Techniques of Analysis

The first steps in solving any multilateral system are to identify the system and establish the coordinates. It makes little difference whether the system uses numbers or letters for coordinates. The techniques are the same in either case. Once the system is identified and the coordinates set up, a solution of the simpler systems is the same as with unilateral systems. Variant systems require additional steps. Each type is considered in the following paragraphs.

5-5. Identification of Simple Biliteral and Dinomic Systems

Simple biliteral and dinomic systems are very easy to recognize and solve.

a. First, the two-for-one nature of the system will usually be apparent. The message will be even in length. The majority of repeated segments will be even in length, although when an adjacent row or column coordinate is the same, a repeat may appear odd in length. The distance between repeats, counted from the first letter of one to the first letter of the next, will be even in length.

b. Second, unless the identical letters or numbers are used for row and column coordinates, there will be limitation by position. One set will appear in the row coordinate position, and the other set will appear in the column coordinate position. Even in the case where all coordinates are different and either the row or column coordinate character may be placed first, each pair will be limited to one from one set and one from the other. If you do not recognize it right away, charting contacts will make it obvious.

c. For systems with letters as coordinates, not more than half the alphabet will be used as coordinates. This severe limitation in letters used is the most obvious characteristic, since only very short unilateral messages are ever that limited. A phi index of coincidence will reflect that limitation, always appearing much higher than expected for a unilateral system.

d. Dinomic systems, since they are limited to the 10 digits anyway, are not quite as obvious. Simple systems should still show positional limitation, however.

5-6. Sample Solution of a Dinomic System

The next problem shows the steps in solution of a sample dinomic system. These steps apply equally to biliteral systems.

```
2023 2029 6224 6322 2144  4420 6362 4924 6529 2769
2043 2123 2227 4627 6521  2221 2723 6527 2349 2144
4481 8287 2423 4349 2144  4485 8089 6522 2746 2421
6365 2263 2142 2027 2324  6322 2144 4420 6362 4627
6521 2221 2723 6560 2144  4441 2047 2123 2422 6680

6666 6522 2746 4263 2069  2122 6425 2729 2924 2343
2123 4700
```

a. The most obvious thing about this cryptogram is that every pair of numbers begins with 2, 4, 6, or 8. The final pair begins with 0, but since it appears nowhere else, it is probably a filler. This suggests that we are dealing with a matrix with four rows.

b. Scanning the second digit of every pair, we see that there is some limitation in the column position, also. All digits are used except 8. The matrix appears to have nine columns, although it is possible that a column for 8 exists, but no values from it were used. Four by nine is a reasonable size for a matrix.

c. Next, we check for repeats and underline them. We also prepare a dinomic frequency count by setting up a 4 by 9 matrix and checking off each dinome that appears.

```
2023 2029 6224 6322 2144  4420 6362 4924 6529 2769
2043 2123 2227 4627 6521  2221 2723 6527 2349 2144
4481 8287 2423 4349 2144  4485 8089 6522 2746 2421
6365 2263 2142 2027 2324  6322 2144 4420 6362 4627
6521 2221 2723 6560 2144  4441 2047 2123 2422 6680

6666 6522 2746 4263 2069  2122 6425 2729 2924 2343
2123 4700
```

	1	2	3	4	5	6	7	9	0
2	15	10	10	7	1		11	4	8
4	1	2	3	10		4	2	3	

d. The two longer repeats both include patterns of repeated values. Word patterns can be constructed on repeated dinomes just as they were for repeated single letters. The word patterns for the two longer repeats are shown below.

```
-  A  B  C  D  D  E  A  -
24 63 22 21 44 44 20 63 62
A  R  T  I  L  L  E  R  Y

-  A  B  C  D  C  A  E  B
46 27 65 21 22 21 27 23 65
P  O  S  I  T  I  O  N  S
```

e. The word pattern lists in Appendix D show only one possibility for each pattern as shown. The two are consistent with each other. Using these recoveries, we can set up a matrix and place the values in it and the cryptogram.

```
e n  e    y a  r t  i l  l e  r y    a  s    o
2023 2029 6224 6322 2144 4420 6362 4924 6529 2769

e    i n  t o  p o  s i  t i  o n  s o  n    i l
2043 2123 2227 4627 6521 2221 2723 6527 2349 2144

l         a n       i l  l         s t  o p  a i
4481 8287 2423 4349 2144 4485 8089 6522 2746 2421

r s  t r  i    e o  n a  r t  i l  l e  r y  p o
6365 2263 2142 2027 2324 6322 2144 4420 6362 4627

s i  t i  o n  s    i l  l    e    i n  a t
6521 2221 2723 6560 2144 4441 2047 2123 2422 6680

     s t  o p    r  e    i t       o      a  n
6666 6522 2746 4263 2069 2122 6425 2729 2924 2343

i n
2123 4700
```

	1	2	3	4	5	6	7	9	0
2	i	t	n	a			o		e
4				l		p			
6		y	r		s				
8									

f. The plaintext words *ENEMY* and *AIRSTRIKE* are now obvious. Placing the M from ENEMY shows *COMMANDING* at the end of the message. Most of the remaining plaintext letters are easily recovered.

```
e n  e m  y a  r t  i l   l e  r y  h a  s m  o v
2023 2029 6224 6322 2144  4420 6362 4924 6529 2769

e d  i n  t o  p o  s i   t i  o n  s o  n h  i l
2043 2123 2227 4627 6521  2221 2723 6527 2349 2144

l         a n  d h  i l   l         s t  o p  a i
4481 8287 2423 4349 2144  4485 8089 6522 2746 2421

r s  t r  i k  e o  n a   r t  i l  l e  r y  p o
6365 2263 2142 2027 2324  6322 2144 4420 6362 4627

s i  t i  o n  s w  i l   l b  e g  i n  a t
6521 2221 2723 6560 2144  4441 2047 2123 2422 6680

     s t  o p  k r  e v   i t    c  o m  m a  n d
6666 6522 2746 4263 2069  2122 6425 2729 2924 2343

i n  g
2123 4700
```

	1	2	3	4	5	6	7	9	0
2	i	t	n	a	c		o	m	e
4	b	k	d	l		p	g	h	
6		y	r		s			v	w
8									

g. The letters in the second row precede all the letters in the third row alphabetically. This suggests an alphabetic structure, although the columns are clearly not in the correct order. The first row probably contains a keyword. If we rearrange the columns so the letters in the second and third rows fall in alphabetical order, we see the next structure.

	1	3	5	7	9	0	2	4	6
2	i	n	c	o	m	e	t	a	
4	b	d		g	h		k	l	p
6		r	s		v	w	y		
8									

h. The plaintext letters area keyword mixed sequence based on INCOME TAX. After placing the remaining letters, there are still 10 blank cells in the matrix. Seven of them are used in the cryptogram, and they cluster together in segments of three or four dinomes. They show the typical pattern of numbers. In particular, the four plaintext values of groups 50 and 51 of the message indicate time, and 66 is probably a 0. More likely than not, the remaining numbers fill the bottom row of the matrix in numerical order, but these recoveries cannot be confirmed without more information. If hill numbers could be compared to known numbers from an enemy map sheet, we could accept the values with more confidence. At this point, we are reasonably confident of the letter arrangement and the number 0, but the remaining numbers are only a possibility. However, if this were a current real life situation and the enemy referred to by the text is our own forces, we would certainly consider reporting the likelihood of air strikes on our artillery positions.

5-7. Analysis of Monome-Dinome Systems

The characteristics of biliteral and dinomic systems that stand out most are the divisibility by two and the positional limitation that makes it easy to determine matrix coordinates. By changing the length of the plaintext unit from character to character, monome-dinome systems avoid both of these characteristics. In their place, however, the frequency of the numbers (or occasionally, letters) used as row coordinates tends to be higher than the other coordinates. Choosing the highest frequency numbers as row coordinates gives a starting point to reconstruct a monome-dinome system. Consider the next example.

```
8 0 7 9 6   7 8 0 0 9   6 0 7 2 0   5 1 1 8 7   3 3 8 1 2
0 7 9 6 0   7 6 0 5 9   6 9 7 3 0   7 1 0 7 0   9 9 0 8 9
6 0 9 0 5   9 6 0 7 0   6 2 0 5 0   0 9 1 0 9   1 3 8 6 6
9 6 0 5 8   2 4 7 1 0   8 1 0 5 9   6 9 7 4 0   7 9 6 1 0
9 0 5 9 1   1 9 7 8 7   1 6 8 3 3   0 7 3 8 9   7 0 8 0 5
0 0 0 1 9   6 0 5 0 9   0 7 0 5 5   0 5 4 5 8   5 7 9 5 0
1 9 1 9 6   9 7 4 0 7   9 6 9 6 0   7 2 0 5 1   1 8 7 3 3
8 1 2 0 7   0 6 9 1 0   7 0 3 9 0   5 6 5 4 5   3 5 3 9 9
9 5 2 0 5   0 0 0 3 0   0 8 2 0 4
```

Numbers:	1	2	3	4	5	6	7	8	9	0
Frequency:	19	8	13	6	22	20	25	16	33	53

a. Repeats are underlined and the number frequencies are shown in the example. A dinomic system can be ruled out, because the repeats are an odd interval apart. The distance between the repeats is 153 characters, counting from the first character of one to the first character of the next. A three-for-one substitution is possible from the position of the repeats, but no patterns or positional limitations appear when divided into threes. The very high frequency of the numbers 0 and 9 in relation to the other numbers suggests that the system is monome-dinome. The most likely row coordinates are 0 and 9. Other row coordinates are possible, but at this point it is best to start with the most likely candidates only.

b. Begin by breaking the message into monomes and dinomes using only the 0 and 9 as row coordinates. Mark off the divisions in pencil, keeping in mind that some changes may be required later. Start with the first character of the message and work through in order to the end, marking off the monomes and dinomes. Whenever the first character after a division is a 0 or 9, include it with the next character. If it is any other character, leave it as a monome.

```
8/0 7/9 6/   7/8/0 0/9   6/0 7/2/0   5/1/1/8/7/   3/3/8/1/2/
0 7/9 6/0    7/6/0 5/9   6/9 7/3/0   7/1/0 7/0    9/9 0/8/9
6/0 9/0 5/   9 6/0 7/0   6/2/0 5/0   0/9 1/0 9/   1/3/8/6/6/
9 6/0 5/8/   2/4/7/1/0   8/1/0 5/9   6/9 7/4/0    7/9 6/1/0
9/0 5/9 1/   1/9 7/8/7/  1/6/8/3/3/  0 7/3/8/9    7/0 8/0 5/
0 0/0 1/9    6/0 5/0 9/  0 7/0 5/5/  0 5/4/5/8/   5/7/9 5/0
1/9 1/9 6/   9 7/4/0 7/  9 6/9 6/0   7/2/0 5/1/   1/8/7/3/3/
8/1/2/0 7/   0 6/9 1/0   7/0 3/9 0/  5/6/5/4/5/   3/5/3/9 9/
9 5/2/0 5/   0 0/0 3/0   0/8/2/0 4
```

c. With the divisions in place, we can try a word pattern on the long repeat.

```
96 07 2 05 1 1 8 7 3 3 8 1 2 07
-  A  B C  D D E F G G E D B A
R  E  C O  N N A I S S A N C E
```

d. We next set up a monome-dinome matrix with row coordinates 0 and 9 and include the recovered letters. Shown below is the partially recovered matrix and the cryptogram with all letters from *RECONNAISSANCE* placed in the plaintext and the matrix.

```
a   e   r    i a       r     e c   o   n n a i    s s a n c
8/0 7/9 6/   7/8/0 0/9   6/0 7/2/0   5/1/1/8/7/   3/3/8/1/2/

 e   r    e       o   r       s   e   n   e           a  r
0 7/9 6/0   7/6/0 5/9   6/9 7/3/0   7/1/0 7/0   9/9 0/8/9

       o      r    e       c   o                  n s a
6/0 9/0 5/   9 6/0 7/0   6/2/0 5/0   0/9 1/0 9/   1/3/8/6/6/

 r   o  a    c   i n       n  o    r          e    r   n
9 6/0 5/8/   2/4/7/1/0   8/1/0 5/9   6/9 7/4/0   7/9 6/1/0

   o         n     a i    n   a s s     e  s a            o
9/0 5/9 1/   1/9 7/8/7/   1/6/8/3/3/   0 7/3/8/9   7/0 8/0 5/

          r    o          e   o        o      a      i
0 0/0 1/9   6/0 5/0 9/   0 7/0 5/5/   0 5/4/5/8/   5/7/9 5/0

       r            e      r   r    e   c   o n    n a i s s
1/9 1/9 6/   9 7/4/0 7/   9 6/9 6/0   7/2/0 5/1/   1/8/7/3/3/

a n c   e              e                           s   s
8/1/2/0 7/   0 6/9 1/0   7/0 3/9 0/   5/6/5/4/5/   3/5/3/9 9/

    c  o                   a c
9 5/2/0 5/   0 0/0 3/0   0/8/2/0 4
```

	1	2	3	4	5	6	7	8	9	0
-	n	c	s				i	a		
0					o		e			
9						r				

e. These recoveries suggest additional plaintext, particularly the message beginning *AERIAL RECONNAISSANCE REPORTS ENEMY.* Placing these new values leads to additional recoveries.

```
a   e   r    i a l      r    e c o     n n a i     s s a n c
8/0 7/9 6/   7/8/0 0/9   6/0 7/2/0   5/1/1/8/7/   3/3/8/1/2/

 e  r   e    p  o    r    t  s  e    n  e  m     y  a  r
0 7/9 6/0   7/6/0 5/9   6/9 7/3/0   7/1/0 7/0   9/9 0/8/9

  m   o        r   e    d  c  o  l     u    m     n s a p p
6/0 9/0 5/   9 6/0 7/0   6/2/0 5/0   0/9 1/0 9/   1/3/8/6/6/

 r  o  a     c h i n    g  n  o  r     t  h  e    r  n   m
9 6/0 5/8/   2/4/7/1/0   8/1/0 5/9   6/9 7/4/0   7/9 6/1/0

  o   u      n  t  a i    n p a s s     e  s a  t      g   o
9/0 5/9 1/   1/9 7/8/7/   1/6/8/3/3/   0 7/3/8/9   7/0 8/0 5/

 l  f   r     o   m        e  o       o      a       i     f
0 0/0 1/9   6/0 5/0 9/   0 7/0 5/5/   0 5/4/5/8/   5/7/9 5/0

  u   r        t  h  e    r   r  e     c  o  n      n a i s s
1/9 1/9 6/   9 7/4/0 7/   9 6/9 6/0   7/2/0 5/1/   1/8/7/3/3/

a n c  e       d  u  e     b  y                    s   s
8/1/2/0 7/   0 6/9 1/0   7/0 3/9 0/   5/6/5/4/5/   3/5/3/9 9/

   c  o       l  b   l     a c  k
9 5/2/0 5/   0 0/0 3/0   0/8/2/0 4
```

	1	2	3	4	5	6	7	8	9	0
-	n	c	s	h		p	i	a	-	-
0	f		b	k	o	d	e	g	m	l
9	u					r	t			y

f. Several things remain to be done to complete the solution. The columns can be rearranged to recover a keyword in the top row and alphabetical progression in the next two rows. Additionally, there are two unrecovered segments of text. Both of them include a number of 5s, and the preceding text in each case suggests numbers. The solution is that there is another row in the matrix with the 5 as its coordinate. It was not used enough to select from frequency alone, but once enough text was recovered, the structure can be seen. The added row includes the numbers. The complete solution appears in the next example, with the recovery of specific numbers only tentative.

```
a   e   r    i a   l    r     e  c    o   n n  a i   s s a n c
8/0 7/9 6/   7/8/0 0/9    6/0 7/2/0     5/1/1/8/7/   3/3/8/1/2/

  e   r    e    p  o    r     t  s    e   n  e    m     y   a  r
0 7/9 6/0    7/6/0 5/9    6/9 7/3/0     7/1/0 7/0    9/9 0/8/9

    m   o     r    e     d   c  o    l     u    m    n s a p p
6/0 9/0 5/   9 6/0 7/0    6/2/0 5/0     0/9 1/0 9/   1/3/8/6/6/

 r    o  a    c h i n    g   n  o    r     t  h   e     r   n  m
9 6/0 5/8/   2/4/7/1/0    8/1/0 5/9     6/9 7/4/0    7/9 6/1/0

    o   u     n  t  a i    n p a s s     e  s a  t      g    o
9/0 5/9 1/   1/9 7/8/7/   1/6/8/3/3/    0 7/3/8/9    7/0 8/0 5/

 l    f    r     o    m     e   o    7     6   4      2   .    f
0 0/0 1/9    6/0 5/0 9/   0 7/0 5/5     0/5 4/5 8/   5 7/9 5/0

    u   r      t  h   e     r   r     e   c   o  n    n a i s s
1/9 1/9 6/   9 7/4/0 7/   9 6/9 6/0     7/2/0 5/1/   1/8/7/3/3/

a n  c  e       d   u    e     b   y      1   6    0     0    z
8/1/2/0 7/   0 6/9 1/0    7/0 3/9 0/    5 6/5 4/5    3/5 3/9 9

 .   c  o     l    b    l    a  c  k
9 5/2/0 5/   0 0/0 3/0    0/8/2/0 4
```

	3	6	7	1	8	2	4	0	9	5
-	s	p	i	n	a	c	h	-	-	-
0	b	d	e	f	g	j	k	l	m	o
9	q	r	t	u	v	w	x	y	z	.
5	0	1	2	3	4	5	6	7	8	9

5-8. Application of Vowel-Consonant Relationships to Multiliterals

Vowel-consonant relationship solutions can be applied to multiliterals, too. As long as you can determine the coordinates of the matrix, you can set up a dummy matrix with any sequence of characters inside as a pseudoplain component. You then reduce the cryptogram to unilateral terms by deciphering with the dummy matrix. Next, solve the resulting unilateral cryptogram using any of the techniques learned with unilateral systems, including the use of trilateral frequency counts and the vowel and consonant lines.

5-9. Solution of Trilateral and Trinomic Systems

Trilateral and trinomic systems are solved in exactly the same way as biliterals and dinomics. The systems are identified by the tendency of messages to break into groups of three instead of groups of two. With simple triliterals and trinomics, positional limitation is even more evident than it is for biliterals and dinomics. Look for a limited set of pairs of characters as either the first pair of characters or the last pair of characters in every three, Once these are found, set up your coordinates and solve as before.

Section III

Analysis of Variant Multilateral Systems

5-10. Identification of Variant Systems

As with any coordinate system, analysis of variant multilateral systems begins with determination of the coordinates. If the product of the row and column coordinates is 50 or more, the system is almost certainly a variant system of some kind.

5-10. Analysis of External Variant Systems - Frequency Matching

External variant systems are generally easier to solve than internal variant systems. Frequency counts can usually be used to determine which coordinates combine with each other on the same row or column, whenever the text is long enough to give a good representative sample, as shown in the next problem.

```
IIUC RAPC OIPU IANU NMDR   NIRI ISIU AIII PSPR AUUN
AMDG ANPG URDU IMMA PRAU   MROU RIIM NAMO ICDN UUUA
UIOM ARAA AIII DSMI RRNO   MMPU RGUR UNDS NIIA RMMA
PSUC UONM IOAR RADU PUPG   OCIA PUMO RCMM MCDR ROIA
SORI ACNM UNRI IMII SMRA   ANNA SRNM ROMI NONR RAUC

RIPN SADG AUPR IONA DUUU   MRIA OGNR RAIR MAIA RGNI
MOPO RAMM MUII DRPS MIAR   MOAC DGUA URAC NISR NOIG
DSSI RORM MINO MURU MMAI   DOUA PGRR USXX
```

	A	C	G	I	M	N	O	R	S	U
A	1	3		3	1	2		3		3
D			3			1	1	3	3	3
I	6	1	1	5	3		2	1	1	1
M	3	1		4	4		4	2		2
N	3			4	4		4	2		1
O		1	1	1	1					1
P		1	3			1	1	3	3	4
R	6	1	2	5	2		3	2		1
S	1			1	1		1	2		
U	3	3		1		3	1	3	1	2

a. The cryptogram used 10 different letters as row coordinates and 10 different letters as column coordinates. Using these coordinates, a digraphic frequency count has been completed as shown. For example, the letter I is paired with itself five times, so the number 5 appears in the matrix at the point where the row and column of I intersect.

b. Examining the frequency count, we can see that there are good frequency pattern matches between certain rows and certain columns. For example, the I row and the R row are nearly identical. Similarly, the A column and the I column are nearly identical. Carrying this process further, we can match the row pairs, AU, DP, IR, MN, and OS. The column pairs are AI, CN, GS, MO, and RU. At this point, we have no idea in what order the coordinate pairs belong or which letter in each pair comes first or if it even matters which letter comes first. We have enough information, however, to reduce the cryptogram to unilateral terms.

c. To reduce the cryptogram to unilateral terms, we set up a matrix with the combined coordinates and write any sequence of letters within it, for example, A through Y.

	A	C	G	M	R
	I	N	S	O	U
AU	A	B	C	D	E
DP	F	G	H	I	J
IR	K	L	M	N	O
MN	P	Q	R	S	T
OS	U	V	W	X	Y

```
K B   K G   U J   K T   S J     P K   M O   A K   H J   E B
IIUC  RAPC  OIPU  IANU  NMDR    NIRI  ISIU  AIII  PSPR  AUUN

D H   B H   E J   N P   J E     T Y   K N   P S   L G   E A
AMDG  ANPG  URDU  IMMA  PRAU    MROU  RIIM  NAMO  ICDN  UUUA

A X   E A   A K   H P   O S     S J   M E   B H   P K   N P
UIOM  ARAA  AIII  DSMI  RRNO    MMPU  RGUR  UNDS  NIIA  RMMA

H B   D S   N E   K J   J H     V K   J S   L S   Q J   N K
PSUC  UONM  IOAR  RADU  PUPG    OCIA  PUMO  RCMM  MCDR  ROIA

X K   B S   B K   N K   X K     B P   Y S   N P   S T   K B
SORI  ACNM  UNRI  IMII  SMRA    ANNA  SRNM  ROMI  NONR  RAUC


K G   U H   E J   N P   J E     T K   W T   K O   P K   M P
RIPN  SADG  AUPR  IONA  DUUU    MRIA  OGNR  RAIR  MAIA  RGNI

S I   K S   T K   J H   P E     S B   H A   E B   P Y   S M
MOPO  RAMM  MUII  DRPS  MIAR    MOAC  DGUA  URAC  NISR  NOIG

H U   N N   P S   T O   S A     I A   H O   C
DSSI  RORM  MINO  MURU  MMAI    DOUA  PGRR  USXX
```

d. We see that repeats appear in the pseudotext that results from our trial decipherment. The repeats that were suppressed by the variants are now visible with the variants combined. The recovery of the plaintext is like any of the previous problems. When we recover the plaintext and enter the recovered values in the matrix in place of the trial sequence, we reach the solution shown below.

	A	C	G	M	R
	I	N	S	O	U
AU	l	n	k	g	i
DP	-	m	a	b	r
IR	e	f	d	s	c
MN	t	u	-	o	p
OS	y	z	x	v	w

```
e n  e m  y r  e p  o r    t e  d c  l e  a r  i n
K B  K G  U J  K T  S J    P K  M O  A K  H J  E B
IIUC RAPC OIPU IANU NMDR   NIRI ISIU AIII PSPR AUUN

g a  n a  i r  s t  r i    p w  e s  t o  f m  i l
D H  B H  E J  N P  J E    T Y  K N  P S  L G  E A
AMDG ANPG URDU IMMA PRAU   MROU RIIM NAMO ICDN UUUA

l v  i l  l e  a t  c o    o r  d i  n a  t e  s t
A X  E A  A K  H P  O S    S J  M E  B H  P K  N P
UIOM ARAA AIII DSMI RRNO   MMPU RGUR UNDS NIIA RMMA

a n  g o  s i  e r  r a    z e  r o  f o  u r  s e
H B  D S  N E  K J  J H    V K  J S  L S  Q J  N K
PSUC UONM IOAR RADU PUPG   OCIA PUMO RCMM MCDR ROIA

v e  n o  n e  s e  v e    n t  w o  s t  o p  e n
X K  B S  B K  N K  X K    B P  Y S  N P  S T  K B
SORI ACNM UNRI IMII SMRA   ANNA SRNM ROMI NONR RAUC


e m  y a  i r  s t  r i    p e  x p  e c  t e  d t
K G  U H  E J  N P  J E    T K  W T  K O  P K  M P
RIPN SADG AUPR IONA DUUU   MRIA OGNR RAIR MAIA RGNI

o b  e o  p e  r a  t i    o n  a l  i n  t w  o d
S I  K S  T K  J H  P E    S B  H A  E B  P Y  S M
MOPO RAMM MUII DRPS MIAR   MOAC DGUA URAC NISR NOIG

a y  s s  t o  p c  o l    b l  a c  k
H U  N N  P S  T O  S A    I A  H O  C
DSSI RORM MINO MURU MMAI   DOUA PGRR USXX
```

e. With the plaintext values filled into the matrix, we can see in what order the rows and columns belong. Starting with the last row of the internals, we rearrange the columns of the matrix in alphabetic order.

	M	R	G	A	C
	O	U	S	I	N
AU	g	i	k	l	n
DP	b	r	a	-	m
IR	s	c	d	e	f
MN	o	p	-	t	u
OS	v	w	x	y	z

The first row of the internals should follow alphabetically after the third row—scdef, gikln.

	M	R	G	A	C
	O	U	S	I	N
DP	b	r	a	-	m
IR	s	c	d	e	f
AU	g	i	k	l	n
MN	o	p	-	t	u
OS	v	w	x	y	z

f. All that remains is to fill in the missing letters H, J, and Q in the plaintext sequence, and to try to recognize how the coordinates were constructed. As mentioned earlier, it is common practice to couple I with J or U with V when using a 5 by 5 matrix. Since J did not appear in the plaintext, we may assume it occupies an alphabetical position within the I block. The Q clearly belongs between the P and T, leaving the H in the top row. The plaintext keyword is BRAHMS (the classical composer). With that as a clue, the letters in the coordinates are shifted to their correct positions, revealing the keywords PIANO, DRUMS, MUSIC, and ORGAN.

	M	U	S	I	C
	O	R	G	A	N
PD	b	r	a	h	m
IR	s	c	d	e	f
AU	g	i/j	k	l	n
NM	o	p	q	t	u
OS	v	w	x	y	z

5-12. Analysis of Variants - Isologs

Two or more encrypted messages with different encrypted text, but the same underlying plaintext are called isologs. When isologs are encountered, your job is much easier. Isologs are particularly useful in solving variant multilateral systems, either external or internal.

a. Isologs can be recognized by one or more of these characteristics—

- Identical message lengths.
- Similar characteristics in the text, such as repeated segments or characters occurring in the same position in each message.

- External indications, such as identical times of file or identical message numbers included in the header for each message. Normally, no two different messages from the same sender receive the same file time or message number. When you see the same time of file on the same date originating from the same unit, the messages are likely to be isologs.

b. Two messages that showed the same time of file in the message header appear in Figure 5-3.

```
Message 1:

XLNH GVDV NZRH DKXH AMNV  RPGZ XMNK DZGP XVDH QHNB
QCFH DVRP GLFP DSAZ RHFB  GKNZ DBFL DLGH RSFH QKRB
TSDP QVNK DZFP DKQP QMAC  NBRL RPRK NSRV NBFL FBNP
DBLM FZGV ACRK TCTH XPTM  AHNL NMRM DBFS FHRH NCRZ
XCFV NBRL FPTS DHGK NKDZ  FHNV

Message 2:

GYQB EDAD QTOW ATZM OPFT  GSAY OTFD ZDKW KYZY VSQD
EWOS ATGW KTGS FMKP OWFS  LTQT ZDEM ARVS ERGW LDFW
OYZB LTFT ZTOS FDVW EWOH  QDLR GSZS AMQS QTLM FWQY
ZDGH AWET GPZW GTQM ZRGD  EPFM EYKM QTLM GSGW LBAS
OTQW ZTER GWGB QBED ADZD  OSAT
```

Figure 5-3. Isolog example.

c. Each message shows positional limitations. Message 1 has the letters ADFGLNQRTX in the row coordinate position and BCHKLMPSVZ in the column coordinate position. Message 2 has AEFGKLOQVZ in the row coordinate position and BDHMPRSTWY in the column coordinate position. The two messages are not encrypted in the same system, but they appear to be isologs.

d. The initial step in solving these isologs is to see what values equate to each other in the two messages. Pick one of the most frequent digraphs in either message as a starting point. For example, FH occurs four times in the first message. A frequency count, while not strictly necessary, may be helpful in spotting the most common values. The digraphs that occur in the same positions in message 2 as FH in message 1 are OS, GW, GS, and another OS.

e. The next step is to find each of the digraphs in message 2 that equated to FH from message 1. The letters OS, GW, and GS in message 2 and the digraphs in the same position in message 1 are underlined in Figure 5-3.

f. We now see that RH, RP, FP, and FH in message 1 equate to GS, GW, and OS in message 2. A check of the new values in message 1 adds the additional digraph OW in message 2, completing the equations for that set. It appears that R and F are variant row coordinates and P and H are variant column coordinates in message 1. Similarly, the message 2 variants are G and O on the rows and W and S on the columns.

g. Continue the process by picking additional repeated values. Complete the equations for each, working back and forth between the two messages, just as we did for the initial digraph FH. Continue until all coordinates have been combined, or you run out of digraphs to compare. You can set up a plot to keep track of the equations as shown in the next example.

Row	Column	Message 1	Message 2	Row	Column
FR	HP	RH RP FP FH	GS GW OS OW	GO	SW
DN	BZ	DZ NZ DB NB	QD QT ZT ZD	QZ	DT
	KV	NV DV DK NK	FD FT AD AT	AF	
GQ		QK QV GK GV	ED ET LT LD	EL	
AL	CM	AM LM AC	OH GP GH OP		HP
TX	LS	XL TS	GB OY GY		BY
		GP GH QP QH	VS VW KW	KV	
		DS DL NS NL	FM AM AR		MR

h. Other combinations could have been selected than the ones shown, but these are sufficient to show all the variants in both matrices. From this point, either message can be reduced to unilateral terms and solved. Then the recovered plaintext can be applied to the other message to complete the recovery of the second matrix. Note that if the same matrix was used in both messages, the similarity should be quickly recognized and the solution accomplished more easily. The next paragraph shows the simpler technique when the same matrix is used.

5-13. Solution Using Isologous Segments

Segments of ciphertext which have the same underlying plaintext are known as isologous segments. A technique similar to the one used in isolog solution can be used any time repeated plaintext can be identified. This is likely to occur with repeated beginnings and endings to messages or with long repeated words and phrases.

a. Recognizing repeated plaintext in variant systems requires painstaking inspection of the ciphertext. Computer indexes of repeated plaintext, which show repeated text on consecutive lines along with the preceding and following text makes repeats easier to recognize. In any long plaintext repeat, some of the ciphertext digraphs or dinomes are likely to repeat. Other ciphertext digraphs or dinomes are likely to show common row or column coordinates. Pairs with neither row nor column coordinates in common will generally be in the minority. Therefore, although a lot of trial and error may be involved, the longer repeated plaintext segments can often be identified. Consider the two message beginnings shown below.

Message 1:

```
3469 8489 2469 1420 8957  7238 2311 8840 9626 6269
- -    ------  -    -  -----------   - ---- ---
1429 1622 8924 ...
       -   - -
```

Message 2:

```
3368 6389 2468 1335 8807  7238 2316 6890 9636 6788
- -    ------  -    -  -----------   - ---- ---
7338 7127 6934 ...
       -   - -
```

b. The similarities of the text make it quite clear that the underlying plaintext is the same in both cases, and the same matrix is used for both. Proceeding on the assumption that the plaintext and matrix are the same, it is easy to match the remaining values to determine the variants. For example, from the first dinome in each message, 3 and 4 are column variants. From the second dinome in each message, 8 and 9 are column variants. All the variants can be combined from this short example, and the remainder of the solution is routine.

5-14. Analysis of Internal Variant Systems

Internal variant systems are generally more difficult to solve than external variant systems. With no coordinates to combine, frequency counts do not provide immediate clues to variants. Similarly, isologous segments are harder to recognize. Some characters are likely to repeat in isologous segments with internal variant systems, but the partial repeats caused by common row or column coordinates are much less likely to occur. Still, given enough messages from a single system to produce repeats; given operator carelessness in encryption; or given stereotyped traffic, these systems can readily be solved, too. Once a plaintext entry is found, the remainder of a solution is not difficult. When you find isologs or isologous segments, you can equate ciphertext values just as was demonstrated in the internal variant examples. The only difference is that you do not combine coordinates through this process, but instead find all cells in the matrix that have the same plaintext value.

5-15. Analysis of Syllabary Squares

Syllabary squares are closely related to small code charts, and the solution of both types of systems is similar. The analysis of syllabary squares produces some distinct differences.

a. Isologs or isologous segments are not necessarily the same length in each case. The encipherment examples below are repeated from paragraph 5-3e.

	6	0	4	3	8	1	7	5	9	2
8	a	1	ad	al	an	and	as	at	b	2
4	c	3	ce	co	d	4	da	de	di	e
3	5	ea	ec	ed	ee	ei	el	en	ent	er
7	es	et	f	6	fi	fo	g	7	h	8
2	hi	ht	i	9	in	ing	io	ir	is	it
0	h	0	00	k	l	la	le	ll	m	ma
5	n	nd	ne	ng	ni	nt	o	on	or	ou
9	p	q	r	ra	re	ri	ro	rs	rt	s
1	se	si	st	t	ta	te	th	ti	tion	to
6	tw	ty	u	ur	v	ve	w	x	y	z

```
p:  r  ei n  fo r  ce m  en t  s
c:  94 31 56 71 94 44 09 35 13 92
```

```
p:  re in f  or ce m  ent s
c:  98 28 74 59 44 09 39  92
```

b. Isologous segments can often still be recognized by the plaintext values which have no variation. In the example, there is only one way to encipher the letters M and S. When *REINFORCEMENTS* is enciphered, the ciphertext equivalents of M and S will always be the same. Other values are likely to begin with the same row coordinate, since syllables beginning with the same letter are likely to be on the same row, such as the R and the RE. Still others will have a possible variation, but the variation will not be used. The repeated CE syllable in both segments is an example of this. As a result of all these considerations, isologous segments are often recognizable and provide a point of entry to the system.

c. Solution of syllabary spelling will be further explained in Part Six, Analysis of Code Systems.

PART THREE

PoIygraphlc Substitution Systems

CHAPTER 6

CHARACTERISTICS OF POLYGRAPHIC SUBSTITUTION SYSTEMS

Section I

Characteristics of Polygraphic Encipherment

6-1. Types of Polygraphic Systems

As first explained in Part One, polygraphic cipher systems are those in which the plaintext units are consistently more than one letter long. The most common type is digraphic substitution, which replaces two letters of plaintext with two letters of ciphertext. There are also such systems as trigraphic and tetragraphic substitution. The larger types are rare, and awkward to use in military applications, so they are not included in this manual.

6-2. Digraphic System Characteristics

The simplest type of digraphic substitution, if not the simplest type to construct, uses a 26 by 26 matrix with plaintext values as coordinates to two-letter ciphertext values within the table. A sample of a digraphic substitution matrix is shown in Table 6-1.

Table 6-1. Digraphic substitution matrix.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	WZ	IY	NX	CW	HV	EU	SR	TQ	RP	AO	BN	DM	FL	GK	JJ	KI	LH	MF	OD	PC	QB	UT	VG	XA	YE	ZS
b	IZ	NY	CX	HW	EV	SU	TR	RQ	AP	BO	DN	FM	GL	JK	KJ	LI	MH	OF	PD	QC	UB	VT	XG	YA	ZE	WS
c	NZ	CY	HX	EW	SV	TU	RR	AQ	BP	DO	FN	GM	JL	KK	LJ	MI	OH	PF	QD	UC	VB	XT	YG	ZA	WE	IS
d	CZ	HY	EX	SW	TV	RU	AR	BQ	DP	FO	GN	JM	KL	LK	MJ	OI	PH	QF	UD	VC	XB	YT	ZG	WA	IE	NS
e	HZ	EY	SX	TW	RV	AU	BR	DQ	FP	GO	JN	KM	LL	MK	OJ	PI	QH	UF	VD	XC	YB	ZT	WG	IA	NE	CS
f	EZ	SY	TX	RW	AV	BU	DR	FQ	GP	JO	KN	LM	ML	OK	PJ	QI	UH	VF	XD	YC	ZB	WT	IG	NA	CE	HS
g	SZ	TY	RX	AW	BV	DU	FR	GQ	JP	KO	LN	MM	OL	PK	QJ	UI	VH	XF	YD	ZC	WB	IT	NG	CA	HE	ES
h	TZ	RY	AX	BW	DV	FU	GR	JQ	KP	LO	MN	OM	PL	QK	UJ	VI	XH	YF	ZD	WC	IB	NT	CG	HA	EE	SS
i	RZ	AY	BX	DW	FV	GU	JR	KQ	LP	MO	ON	PM	QL	UK	VJ	XI	YH	ZF	WD	IC	NB	CT	HG	EA	SE	TS
j	AZ	BY	DX	FW	GV	JU	KR	LQ	MP	OO	PN	QM	UL	VK	XJ	YI	ZH	WF	ID	NC	CB	HT	EG	SA	TE	RS
k	BZ	DY	FX	GW	JV	KU	LR	MQ	OP	PO	QN	UM	VL	XK	YJ	ZI	WH	IF	ND	CC	HB	ET	SG	TA	RE	AS
l	DZ	FY	GX	JW	KV	LU	MR	OQ	PP	QO	UN	VM	XL	YK	ZJ	WI	IH	NF	CD	HC	EB	ST	TG	RA	AE	BS
m	FZ	GY	JX	KW	LV	MU	OR	PQ	QP	UO	VN	XM	YL	ZK	WJ	II	NH	CF	HD	EC	SB	TT	RG	AA	BE	DS
n	GZ	JY	KX	LW	MV	OU	PR	QQ	UP	VO	XN	YM	ZL	WK	IJ	NI	CH	HF	ED	SC	TB	RT	AG	BA	DE	FS
o	JZ	KY	LX	MW	OV	PU	QR	UQ	VP	XO	YN	ZM	WL	IK	NJ	CI	HH	EF	SD	TC	RB	AT	BG	DA	FE	GS
p	KZ	LY	MX	OW	PV	QU	UR	VQ	XP	YO	ZN	WM	IL	NK	CJ	HI	EH	SF	TD	RC	AB	BT	DG	FA	GE	JS
q	LZ	MY	OX	PW	QV	UU	VR	XQ	YP	ZO	WN	IM	NL	CK	HJ	EI	SH	TF	RD	AC	BB	DT	FG	GA	JE	KS
r	MZ	OY	PX	QW	UV	VU	XR	YQ	ZP	WO	IN	NM	CL	HK	EJ	SI	TH	RF	AD	BC	DB	FT	GG	JA	KE	LS
s	OZ	PY	QX	UW	VV	XU	YR	ZQ	WP	IO	NN	CM	HL	EK	SJ	TI	RH	AF	BD	DC	FB	GT	JG	KA	LE	MS
t	PZ	QY	UX	VW	XV	YU	ZR	WQ	IP	NO	CN	HM	EL	SK	TJ	RI	AH	BF	DD	FC	GB	JT	KG	LA	ME	OS
u	QZ	UY	VX	XW	YV	ZU	WR	IQ	NP	CO	HN	EM	SL	TK	RJ	AI	BH	DF	FD	GC	JB	KT	LG	MA	DE	PS
v	UZ	VY	XX	YW	ZV	WU	IR	NQ	CP	HO	EN	SM	TL	RK	AJ	BI	DH	FF	GD	JC	KB	LT	MG	OA	PE	QS
w	VZ	XY	YX	ZW	WV	IU	NR	CQ	HP	EO	SN	TM	RL	AK	BJ	DI	FH	GF	JD	KC	LB	MT	OG	PA	QE	US
x	XZ	YY	ZX	WW	IV	NU	CR	HQ	EP	SO	TN	RM	AL	BK	DJ	FI	GH	JF	KD	LC	MB	OT	PG	QA	UE	VS
y	YZ	ZY	WX	IW	NV	CU	HR	EQ	SP	TO	RN	AM	BL	DK	FJ	GI	JH	KF	LD	MC	OB	PT	QG	UA	VE	XS
z	ZZ	WY	IX	NW	CV	HU	ER	SQ	TP	RO	AN	BM	DL	FK	GJ	JI	KH	LF	MD	OC	PB	QT	UG	VA	XE	YS

p: at ta ck at da wn

c: PC PZ FN PC CZ AK

a. As the example shows, with any digraphic system, repeated plaintext digraphs can cause a ciphertext repeat. Repeated single letters do not cause ciphertext repeats. Digraphic systems suppress individual letter frequencies, but show normal frequency patterns for pairs of letters. Since there are 676 possible digraphs in the English language, many more groups of text are needed for digraphic frequencies to be very useful as a direct aid to analysis.

b. Repeated plaintext words and phrases cause ciphertext repeats only when they begin in the same odd or even position. If both occurrences of a plaintext repeat begin in the odd position or both begin in the even position, the ciphertext repeats. If one occurrence is in an odd position and one is in an even position, they will produce different ciphertext. As a result, nearly half of all plaintext repeats are suppressed. This is shown in these three alternate examples, all enciphered from Table 6-1.

```
   at ze ro fo ur ze ro ze ro st op
   PC CV EJ PJ DF CV EJ CV EJ DC CI

-a tz er of ou rz er oz er os to p-
-- OS UF PU RB LS UF GS UF SD TJ --

-a tz er ot hr ee ze ro ze ro st op
-- OS UF TC YF RV CV EJ CV EJ DC CI
```

c. In the first example, all three *ZEROs* produce a repeat when they all begin in the even position. In the second example, they all begin in the odd position, and only the portions of the three *ZEROS* that appear as complete digraphs (the ERs) produce a repeat. In the third example, the two *ZEROs* that begin in the even position produce repeats, but the first *ZERO,* which begins in the odd position, does not.

d. The suppression of individual letter frequencies and a significant portion of plaintext repeats means that digraphic systems are considerably more secure than unilateral systems and most multiliterals.

6-3. Four-Square System

Large table digraphics are awkward systems for military usage. In their place, there are several much more convenient small matrix digraphic systems available with about the same degree of security. The first of these is the four-square.

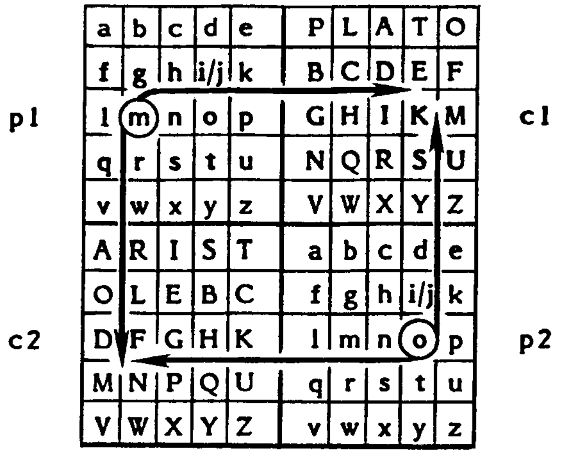
a. The four-square consists of four 5 by 5 matrices in a square. The two plaintext letters and the two ciphertext letters of each encipherment each use a different square. The squares marked p1 and p2 usually, but not always, contain standard sequences. The two squares marked c 1 and c2 can include any mixed sequence.

	a	b	c	d	e	P	L	A	T	O	
	f	g	h	i/j	k	B	C	D	E	F	
pl	l	m	n	o	p	G	H	I	K	M	cl
	q	r	s	t	u	N	Q	R	S	U	
	v	w	x	y	z	V	W	X	Y	Z	
	A	R	I	S	T	a	b	c	d	e	
	O	L	E	B	C	f	g	h	i/j	k	
c2	D	F	G	H	K	l	m	n	o	p	p2
	M	N	P	Q	U	q	r	s	t	u	
	V	W	X	Y	Z	v	w	x	y	z	

p: mo rt ar fi re

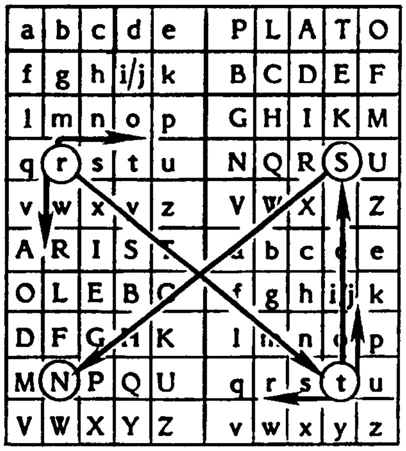
c: KF SN LM EO UR

b. Encipherment or decipherment follows a rectangular pattern. Whether enciphering or deciphering, the letters of the digraphs are located in the appropriately labeled squares. These letters form diagonally opposite corners of a rectangle. The equivalents, plaintext or ciphertext, are the remaining corners of the same rectangle. For example, plaintext MO determines the rectangle outlined in the square below. Plaintext M determines the upper row and the left column of the rectangle. Plaintext O determines the bottom row and the right column of the rectangle. The ciphertext equivalent, KF, is then found in the remaining corners in the appropriately labeled squares.



	a	b	c	d	e	P	L	A	T	O	
	f	g	h	i/j	k	B	C	D	E	F	
pl	l	m	n	o	p	G	H	I	K	M	cl
	q	r	s	t	u	N	Q	R	S	U	
	v	w	x	y	z	V	W	X	Y	Z	
	A	R	I	S	T	a	b	c	d	e	
	O	L	E	B	C	f	g	h	i/j	k	
c2	D	F	G	H	K	l	m	n	o	p	p2
	M	N	P	Q	U	q	r	s	t	u	
	V	W	X	Y	Z	v	w	x	y	z	

c. For a second example, to encipher RT, R is located in the pl square, and T is located in the p2 square. The ciphertext equivalent of RT is found in the remaining corners of the rectangle prescribed by RT. The first ciphertext letter, S, is found in the cl square in the plaintext T column and the plaintext R row. The second ciphertext letter, N, is found in the c2 square at the intersection of the plaintext R column and the T row. Tracing the letters from pl to p2 to cl to c2 is shown below.



	a	b	c	d	e	P	L	A	T	O	
	f	g	h	i/j	k	B	C	D	E	F	
p1	l	m	n	o	p	G	H	I	K	M	c1
	q	r	s	t	u	N	Q	R	S	U	
	v	w	x	y	z	V	W	X	Y	Z	
	A	R	I	S	T	a	b	c	d	e	
	O	L	E	B	C	f	g	h	i/j	k	
c2	D	F	G	H	K	l	m	n	o	p	p2
	M	N	P	Q	U	q	r	s	t	u	
	V	W	X	Y	Z	v	w	x	y	z	

d. Decipherment is handled in exactly the same way, except that the ciphertext letters in the cl and c2 squares determine the rectangle by which the plaintext letters are found.

6-4. Vertical Two-Square

The two types of two-squares are simpler than the four-square system. The first is the vertical two-square, which uses two 5 by 5 matrices one on top of the other. Normally both squares contain mixed sequences.

	D	U	N	G	E	
	O	S	A	B	C	
p1	F	H	I/J	K	L	c1
	M	P	Q	R	T	
	V	W	X	Y	Z	
	D	R	A	G	O	
	N	S	B	C	E	
c2	F	H	I/J	K	L	p2
	M	P	Q	T	U	
	V	W	X	Y	Z	

p: al lq ui et on th ew es te rn fr on tx

c: CJ IU NH GU ON PL UZ UE TE MC HD ON QZ

a. The rectangular rule used with the four-square is used with the two-square, also. Whenever the letters to be enciphered are in the same column, however, the letters become their own equivalents. The encipherment of ON and TE in the example illustrates this.

b. The case where the plaintext letters remain unchanged in the ciphertext is called a transparency. A weakness of this system is that in the long run, about 20 percent of the digraphs in a cryptogram will be transparencies. This is enough to give away more plaintext in many cases and enable a speedy solution.

6-5. Horizontal Two-Square

The second kind of two-square is the horizontal two-square, like the vertical, it uses two 5 by 5 matrices.

	C	A	S	T	O	P	O	L	U	X	
	R	B	D	E	F	A	B	C	D	E	
p1	G	H	IJ	K	L	F	G	H	IJ	K	c1
c2	M	N	P	Q	U	M	N	Q	R	S	p2
	V	W	X	Y	Z	T	V	W	Y	Z	

p:	we	ha	ve	no	ty	et	be	gu	nt	of	ig	ht
c:	ZB	FB	ZR	NA	UY	AY	EB	JC	MW	PL	GI	FW

a. The rectangular rule again applies. In the horizontal two-square, values on the same row are replaced with the same letters in the reverse order. This is illustrated by the encipherment of the plaintext letters *be* and *ig* in the example.

b. Digraphs in ciphertext which are the same as the plaintext in reverse, are called reverse transparencies. Like the direct transparencies of the vertical two-square, they occur in the long run in about 20 percent of the digraphs. They severely weaken the security of the system.

6-6. Playfair Cipher

The Playfair cipher is the most common digraphic system. *Playfair* is always capitalized, because it was named for a Lord Playfair of England. It is the simplest of systems to construct, using only a 5 by 5 matrix, yet it is more secure than uniliterals and most multiliterals. The rules of encipherment and decipherment are a little more complex than the previous digraphic systems. Sizes other than 5 by 5 are occasionally used.

D	I/J	G	R	A
P	H	C	B	E
F	K	L	M	N
O	Q	S	T	U
V	W	X	Y	Z

p: th es ho th ea rd ro un dt he wo rl dx
c: QB CU PQ QB NE AJ DT ZU RO CP VQ GM GV

a. The first rule of encipherment and decipherment is the familiar rectangular rule. This applies any time the two letters to be enciphered or deciphered are not in the same row or column. The first four digraphs in the example follow this rule. One additional step must be remembered. In tracing the encipherment or decipherment in the matrix, always move vertically from the second letter to the third letter. For example, to encipher TH, locate the T and the H and move vertically from the H to the letter that is in the same column as the H and the same row as the T. Following this rule, TH is enciphered as QB, not BQ. Similarly, to decipher CU, locate the C and the U, move vertically from the U to find the first plaintext letter E and then the second plaintext letter S.

b. When the two letters to be enciphered or deciphered are in the same row, follow the rule, *encipher right, decipher left.* To encipher or decipher, pick the letter to the right or left of each letter of the given digraph, as appropriate. In the example, the plaintext letters R and D are in the same row. They are enciphered with the letters immediately to the right of each letter, producing ciphertext AJ (or AI). If a letter to be enciphered is at the right edge, as in the encipherment of HE, the next letter to the right of the right edge is considered to be the letter in the same row at the far left. The letter to the right of E is P. Similarly, if deciphering, the letter to the left of the left edge is the letter at the far right in the same row. The letter to the left of F is N. Each row is treated as if it were written in a circle with the first letter of a row immediately following the last letter.

c. When the two letters to be enciphered or deciphered are in the same column, use the rule *encipher below, decipher above.* To encipher EA in the example, the letters below E and A are N and E respectively. To decipher ZU, the letters above Z and U are U and N respectively. As with the rows, columns are treated as if they were written in a circle. The letter after the bottom letter in a column is the top letter; the letter before the top letter is the bottom letter.

d. The rules *encipher right, decipher left* and *encipher below, decipher above* produce the acronyms ERDL and EBDA. For many analysts, it is convenient to memorize these pronounceable acronyms to remember the rules.

e. The rectangular rule and the row and column rules take care of all possible cases except double letters. In the Playfair system, there is no rule for enciphering or deciphering a double letter in the same digraph. When double letters are encountered in plaintext in the same digraph, the cryptographer must break up the double letters with a null letter, such as inserting an X between them. As a result, double letters will never be encountered in the ciphertext, except in error. This is only true of the Playfair system. Four-squares and two-squares can handle double letters without any problem.

Section II
Identification of Polygraphic Substitution

6-7. General Digraphic Characteristics

Certain identifying characteristics are common to all digraphic systems. Other characteristics appear only with specific systems.

a. Message lengths, repeats, and distances between repeats are likely to be even in length in all digraphic systems because the basic unit is two-letters. Furthermore, the systems which use 5 by 5 matrices will often only use 25 letters, omitting either the I or the J in ciphertext. In some cases, these values will be used alternately just to ensure use of all letters.

b. Digraphic systems are most often mistaken for biliteral with variant systems, because both exhibit ciphertext which breaks into units of two and both can use most letters. The key distinction to look for between biliterals and digraphics is the complete absence of any positional limitation (paragraph 5-5b) in digraphic systems.

c. Two-square systems stand out because of the director reverse transparencies. Scan the text for the presence of good plaintext digraphs, either direct or reversed, to identify two-square systems. Direct transparencies indicate vertical two-squares; reversed transparencies indicate horizontal two-squares.

d. If no double letters are present in a digraphic, it is probably a Playfair system.

e. Monographic frequency counts for digraphic systems are not as flat as random text and not as rough as plaintext or unilateral systems. They generally fall in between the two. The monographic phi test can be used to confirm this, if necessary.

6-8. Digraphic Frequency Counts

There are several types of frequency counts you can take for working with digraphic systems.

a. The most common way to take a digraphic count is to break the text into digraphs and count those digraphs. For example, given text ABCDE FGHIJ . . . , you would normally break it as AB, CD, EF, GH, IJ, ... There are two other ways to take a digraphic count, however. If you are unsure whether there may be indicator groups or null letters at the beginning, you may not know where to begin breaking the text into digraphs. As a comparison, you can skip the first character and begin separating the text into digraphs beginning with the second character. This will produce a completely different set of digraphs than the usual method: A, BC, DE, FG, HI, J . . . . The third way to produce a digraphic count is to combine the two methods to count all possible digraphs. In this case, you would count AB, BC, CD, DE, EF, FG, GH, HI, IJ, ... Unless you have a reason to want an alternate method, stick to the first method.

b. There are two ways to record your count on paper. One is to make a 26 by 26 square on graph paper, and mark the digraphs in the appropriate cells. The other way, useful with short cryptograms, is to write the letters A through Z horizontally, and mark the digraphs by putting the second letter of each digraph under the first letter of the digraph in the A through Z sequence. Then by scanning the columns under each letter for repeated letters, you can readily spot repeated digraphs. This method takes much less space than a 26 by 26 square and gives you the same information.

6-9. Digraphic Coincidence Tests

The phi test and phi index of coincidence can be calculated for digraphic frequency counts as well as monographic.

a. The digraphic phi test is calculated in essentially the same way as the monographic test. In the monographic phi test, 1 out of 26 comparisons in random text was expected to be a coincidence for a probability of 0.0385. In the digraphic phi test, 1 out of 676 comparisons is expected to be a coincidence for a probability of 0.0015. The probability of a coincidence in plaintext is 0.0069 instead of 0.0667. Thus, the formulas for the digraphic phi test are—

$$2\ \phi p = 0.0069\ N\ (N - 1).$$

$$2\ \phi r = 0.0015\ N\ (N - 1).$$

$$2\ \phi o = \Sigma f\ (f - 1).$$

$$2\ \Delta IC = \frac{676\ \Sigma f\ (f - 1)}{N\ (N - 1)} = \frac{2\ \phi o}{2\ \phi r}.$$

N is the total number of digraphs counted.
The frequency of each repeated digraph is f.

b. As discussed in the first part of this chapter, digraphic ciphertext frequencies will occur with the same numbers as plaintext frequencies when digraphic systems are used. If the digraphic ϕo is close to ϕp but the monographic ϕo is low, the system is likely to be a digraphic system. If you are using the index of coincidence form of the test, the expected 2 ΔIC is 4.6. The results are much more variable than the monographic test, because of the large number of different elements counted, but it can still be used as a guide. As with any statistical test, the results should not be used by themselves, but used along with all other available information.

6-10. Examples of System Identification

Three messages in unknown systems follow to show the process that leads to system identification. Repeats are underlined, monographic and digraphic frequency counts are shown, and monographic and digraphic ICs are calculated for each. The three messages were all sent by the same headquarters to subordinate elements, and all contained a common message serial number in their header.

a. Message texts and data.

Message 1:

```
TVCX XSWM WZWV JEVH HCJS  IUZZ TVKP VYUY JWTZ CUIK
XCEI SVJC XIUT IDDI ETWM  IWHH ISWC TIXP ZTVK RIKU
IKCU ISDV UHVM IRPC WUTU  CJZK VUTV JTNI XMIB VYUZ
JVTW EIZT VKEC JEIX CCXX  XICM IZEV HHCK CZZI ZEVH
HCCJ SYJJ IEIZ ZCUP HISW  ECXK UVEI SYUI ZZTV KKIJ

AUII J
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	19	3	11	0	0	10	28	13	11	0	5	1	0	4	0	2	8	13	15	18	10	11	5	16

Total letters = 205

Monographic IC = 1.74

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C	0	0	1	0	0	0	0	0	0	2	1	0	1	0	0	0	0	0	0	0	2	0	0	1	0	1
D	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
E	0	0	2	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
H	0	0	2	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I	0	1	0	1	1	0	0	0	1	1	2	0	0	0	0	0	0	1	2	0	1	0	1	1	0	2
J	0	0	1	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0
K	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
L	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Q	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	2	0
T	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	4	1	0	0	1
U	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	1	1
V	0	0	0	0	0	0	0	2	0	0	2	0	1	0	0	0	0	0	0	0	1	0	0	0	2	0
W	0	0	1	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	1	1	0	0	0	1
X	0	0	1	0	0	0	0	0	2	0	1	0	1	0	0	1	0	0	1	0	0	0	1	0	0	0
Y	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Z	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2

Total digraphs = 102

Digraphic IC = 3.41

Message 2:

```
NPEG MISY DQQR PATH GFTS  LYUV DNPR RWIP SPDR AGYL
RKBE FIPO EGLY RFCZ AFFP  SYLE KZLF SDFN LRVI NPOC
CRYL NCYL FMPT HTYA IWES  TNNE VARP TNPO OZLR YAOW
IPAV PNUE AINP XKGV EFGE  EGKY RLGS AIBP KZGF NCUV
IAUA THGF GVSI PVRA EFUV  AGYI LFSD EBKR TPEF SIYL

UVDN PRLA VNYL ARXX
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
15	3	5	6	13	14	12	3	12	0	6	14	2	13	5	18	2	15	10	8	6	11	3	3	13	4

Total letters = 216

Monographic IC = 1.26

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	0	0	0	0	1	2	0	2	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
B	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
D	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	1	1	0	0	0	0	0	0	0	0
E	0	1	0	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2	0	0	0	0
H	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
I	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	2
L	1	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	2	0
M	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
N	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0
O	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
P	1	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	2	0	1	0	1	0	0	0	0
Q	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
R	1	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0
S	0	0	0	2	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	2	0
T	0	0	0	0	0	0	0	2	0	0	0	0	0	2	0	1	0	0	1	0	0	0	0	0	0	0
U	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0
V	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
X	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Y	2	0	0	0	0	0	0	0	1	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Z	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Total digraphs = 108

Digraphic IC = 5.38

Message 3:

```
GMGH NGMO RWOG GOEG HWMM  HOHR GLNM GEGG HDND HADD
OONL MFRM GFER MLEE GEYO  NANW GAGW GFRF YDYL DOMA
MRYG YFOW ODGR HLNG RWDW  YAGM OOOL OAOW NFHM GOAD
DOGW GDHG DWDG HOYD GMOO  OWAR MMHM GERL NEOO RANL
DWRL NDNA DOOG DLHR YLHG  HEED OWYR ERNG HWYA HFYL

YGGL RFML GRYA HFHE GAGM  EOOW RWAG DOOM GRNW NLMF
HLEH GFGO YMOW RMHF GERA  NMYD HAYF OORW NGYD MWRO
MODW NDEG DOMM YMHR GGHD  YDMA NGMF RMDW MMNF HEHD
GHND YGGL ODYW GAHL OONF  OWRF MMYG YAAE HDDO DDHW
YMNG MORL YLGE YFDW DGNO  NAOO MFRM HMGR RAOE DOGL

DRNL OWDO HAXX
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	0	0	40	20	19	54	32	0	0	0	22	40	26	50	0	0	31	0	0	0	0	27	2	26	0

Total letters = 412

Monographic IC = 2.16

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	2	0	0	2	0	0	0	0	1	0	0	8	0	0	1	0	0	0	0	6	0	0	0
E	0	0	0	1	1	0	2	1	0	0	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G	3	0	0	1	5	3	2	2	0	0	0	4	4	0	3	0	0	4	0	0	0	0	2	0	0	0
H	3	0	0	4	3	3	2	0	0	0	0	3	3	0	2	0	0	3	0	0	0	0	3	0	0	0
I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
M	2	0	0	0	0	4	0	0	0	0	0	2	5	0	3	0	0	1	0	0	0	0	1	0	0	0
N	3	0	0	4	1	3	6	0	0	0	0	4	2	0	1	0	0	0	0	0	0	0	2	0	0	0
O	1	0	0	2	1	0	2	0	0	0	0	1	1	0	7	0	0	0	0	0	0	0	8	0	0	0
P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Q	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
R	3	0	0	0	0	3	0	0	0	0	0	3	4	0	1	0	0	0	0	0	0	0	4	0	0	0
S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
U	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Y	4	0	0	5	0	3	4	0	0	0	0	4	3	0	1	0	0	1	0	0	0	0	1	0	0	0
Z	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Total digraphs = 206

Digraphic IC = 8.90

b. Different analysts might approach the identification of the systems used in these messages in different ways, but here is one example of how the systems can be identified.

(1) Although the messages all carry the same message serial number, which is usually a sign of isologs, the messages are all different lengths. If they are isologs, they are not enciphered in the same system.

(2) A comparison of monographic frequency counts confirms that they are in different systems. The highs and lows in each frequency count are too different for any possibility of repeated use of the identical system.

(3) The ICs give a different picture in each. Message 1 has monographic and digraphic ICs consistent with plaintext or a unilateral system. The digraphic IC of 3.41 is slightly below the expected 4.6, but it is within acceptable limits. Message 2 shows a low monographic IC of 1.26, but the digraphic IC of 5.38 is also well within plaintext limits. This is typical of digraphic systems. Message 3 is quite high in both monographic and digraphic ICs.

(4) Messages 1 and 2 use nearly all letters. Message 3, which is twice as long as message 1, uses only 14 different letters. The high ICs and the limited letter usage are consistent with a biliteral with variants system. A close inspection of the digraphic frequency count will show rows and columns with very similar patterns, suggesting external variants that can be combined. Different letters are used in the row position than those used in the column position. This positional limitation confirms the identification of a biliteral with variants system.

(5) Message 1 has the most repeated text, which is consistent with a unilateral system. Message 2 has only a few repeats and message 3 has only short and fragmentary repeats. In message 3, the fragmented repeat on lines 7 and 10 are in the identical relative position in message 2 as the ZTVK repeat in lines 2 and 5 of message 1. This similarity strongly confirms that the two messages are isologs.

(6) The identifications of the systems in messages 1 and 3 are clear at this point, but message 2 still needs to be•clarified. The underlined repeats in message 2 are in the same relative position as in message 1, if you adjust for the slightly increased length of the message. Only some of the repeats from message 1 appear in message 2, however. This is consistent with a digraphic system, which will only show repeats that begin in the same even or odd position.

(7) In message 2, a check of the long diagonal from the AA position to the ZZ position of the digraphic frequency count shows that the only double letter that appeared was the filler XX at the end of the message. The Playfair is the only

digraphic system which will not show double letters. Finally, because the Playfair cannot encipher double letters, all double letters that occur in digraphs must be broken up by the insertion of null letters. This characteristic explains how it can be an isolog, but appear slightly longer. The three messages are all clearly isologs, and the systems are confidently identified, lacking only the final solution for full confirmation. Solution techniques for each of the major digraphic system types are explained in the next chapter.

CHAPTER 7

SOLUTION OF POLYGRAPHIC SUBSTITUTION SYSTEMS

Section I
Analysis of Four-Square and Two-Square Ciphers

7-1. Identification of Plaintext

Recovery of any digraphic system is largely dependent on the ability to correctly identify or assume plaintext. As with any system, isologs and stereotyped messages can help a great deal. Pattern words can also be of assistance. With unilateral systems, patterns of repeated letters provided an assist. With digraphic systems, patterns of repeated digraphs can do the same thing. Appendix D, beginning on page D-38, includes several types of word pattern tables. The first type, listed on pages D-38 and D-39 shows patterns applicable to any digraphic system. The means of representing digraphic patterns are simpler than those for unilateral patterns. The patterns identify the repeated digraph in a word or phrase by the letters AB in each case, and non-repeating digraphs are just represented by dashes. Here are a few examples that show how the patterns are formed.

```
DE CO DE
AB -- AB

PO ST PO NE
AB -- AB --

MA IN TA IN IN G-
-- AB -- AB AB --

-M AI NT AI N-
-- AB -- AB --
```

7-2. Solution of Regular Four-Squares

Regular four-square ciphers, in which the plaintext squares are in A through Z order, are slightly easier to solve than the type with all mixed squares.

a. With the known plaintext squares, an additional type of word pattern can be used. Since the plaintext locations are fixed, certain words will always produce single letter ciphertext repeats. The word MI LI TA RY, for example, will always produce a repeated ciphertext letter in the first and third cipher position. When MI LI TA RY is enciphered by the matrix shown in paragraph 6-3, it produces KL KO NS SW. Four-square word patterns are shown on pages D-43 through D-47. The patterns are represented by the repeated letters only, placing A, C, E, and soon in the first letter positions of digraphs, and B, D, F, and so on in the second letter positions. Repeats between different positions are ignored. Following these rules, a few examples of four-square word patterns appear below.

```
re qu es te d-
UR UM AU US OY
A- A- -- A- --

el em en ts
PK LK AK RQ
-B -B -B --

qu ar te rm as te r-
UM LM US QF AM US RW
AB -B AD -- -B AD --
```

b. Identifying the four-square from other digraphic systems is largely a matter of elimination. It will include double letters, unlike the Playfair. It will not include a high proportion of good plaintext digraphs or reversed plaintext digraphs like the two-squares. There is no ready clue to tell whether a four-square is a regular one or not, but it is often easiest to assume the simplest case for a start and only consider more complicated construction when the simple case fails to produce a solution.

c. To demonstrate the use of four-square word patterns and recovery of the system, consider the cryptogram shown below.

```
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

d. The underlined repeats give a chance to try a four-square word pattern as an entry to the cryptogram.

```
DM FI PK RO FM
-B A- -- -- AB
```

The only word with this pattern in Appendix D is INFORMATION. Placing *INFORMATION* in the text, and beginning reconstruction of a regular matrix produces the next example.

```
            in form atio  n
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

                                               in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio n
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F		
p1	l	m	n	o	p						HI c1
	q	r	s	t	u		P				
	v	w	x	y	z						
						a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K		M		l	m	n	o	p	p2
	O					q	r	s	t	u	
						v	w	x	y	z	
			R								
			Q								

e. The recovered values have been placed in the matrix, and the alphabetic construction is apparent. Additionally, four values have been placed outside the matrix for the moment as suggested by the plaintext Ns at the end of *INFORMATION.* H and I must be in the same row as plaintext N. R and Q must be in the same column. Several additions can now be made from the alphabetic construction. L and N fit in the third row of the c2 matrix. Further, if H and I are in the third row of the cl matrix, then they must be the first two letters on that row and G is the last letter of the second row. Placing all of these in the matrix and using the partially recovered matrix to decipher as much plaintext as possible produces the next example.

```
          llin form atio n                    at
TATO UTOD HIDM FIPK ROFM HRVH BMAH NHKM UNAN ZMRO

     c                                    at   in
SKHH RQBX FSYF KQNS QFAT KQUY SMQP SMNT MYRO RYDM

form atio n                     h
FIPK ROFM IQLT TYSQ RYRV FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P				
	v	w	x	y	z						
						a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O					q	r	s	t	u	
						v	w	x	y	z	
			R								
			Q								

f. Next, suppose that Q in the c1 matrix is in the keyword. If so, the U would normally be with it. There are not enough letters left in the alphabet after the P in the cl matrix to put both Q and U at the beginning, so Q is almost certainly right after the P.

g. We can be fairly confident of the recoveries up to this point. A number of possibilities present themselves, but as they are only possibilities, the work should be done lightly in pencil. We can next try placing the Q and R in the c2 matrix. The Q is more likely to be in the sequence than the keyword, so we will tentatively place it in the fourth row and R in the first row. We can place P in the fourth row, also, before Q. Another possibility is to place plaintext A on line one of the message, forming the word *ALL* before *INFORMATION.*

```
        a llin form atio  na                    at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

     ct                          rs        at   in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio nr                     he           rs
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

						O					
	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P	Q			
	v	w	x	y	z						
			R			a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q			q	r	s	t	u	
						v	w	x	y	z	

h. Next consider the plaintext RS on line two. It must certainly be preceded by a vowel, therefore, the ciphertext digraph SM must produce a vowel in the p2 position. The only vowel in the same row in the p2 matrix as the ciphertext M in the c2 matrix is plaintext O. S must be in the fourth column of the c1 matrix above the plaintext O. The only logical place for the S is on the fourth row. Adding the S and entering the values increases our solution as shown in the next example.

```
        a llin form atio  na                    at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

     ct                        tors to     at   in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio nr     st              he           rs
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

						O					
	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P	Q	S		
	v	w	x	y	z						
			R			a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q			q	r	s	t	u	
						v	w	x	y	z	

i. These additions suggest several possibilities. *STOP* may appear in the middle of line 2. *REQUEST* may be the word after *INFORMATION* on line 3. Placing these values produces good alphabetical progression in the matrix and many more plaintext possibilities.

```
 qu     a llin form atio  na          on        at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

ro   ct   it   nsou       ns   tors topu pdat edin
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio nreq uest edby         he   qu    e rs
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e	L			R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I	K	M	N	c1
	q	r	s	t	u	O	P	Q	S	T	
	v	w	x	y	z						
			R		Y	a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q	S	T	q	r	s	t	u	
	U	V	W	X	Z	v	w	x	y	z	

j. From here, the solution is routine. *REQUEST* is the first word. *HEADQUARTERS* is the last word. These values in turn fill in enough blanks in the matrix to recognize the keywords and complete the solution. The keywords are LAUREL and HARDY.

7-3. Solution of Mixed Four-Squares

Slightly different techniques must be used when standard sequences are not used in the p1 and p2 squares. The specific four-square word patterns of Appendix D, pages D-43 through D-47 no longer apply, although the general digraphic patterns that precede them on pages D-38 and D-39 are still applicable. Generally, because the matrix construction is less orderly, more text must be known or assumed to successfully complete the solution. The problem that follows shows how the solution can be approached with mixed squares.

```
FMFE FMPX ZPYX IYYP GGME  TXGS YGGB YLFI HAGB YLMK
MRGH YRFM BYYP MMBQ YMHD  MHLN MNOS YPVI DMXH RPGL
MNSO QLMP GBYL VGQI QLYX  KTZG HEEM GBKM FLYK PHMA
SREE GDMK DEBG TTEB IXCN  VINI SOSC HHIG THHM OQPO
TGKI VGQI PMXR CPGH YRSE  PLMN LNMN ACVC OCCO KPWC

PKIP PCSU GHYR FKSC YGXX
```

a. The above cryptogram has been identified as a four-square. Previous messages from the same headquarters have been signed by ADAMS or MILLER. The repeated segments in the text suggest several possibilities for plaintext.

(1) The AB -- AB pattern at the beginning fits the common stereotype *REFERENCE.*

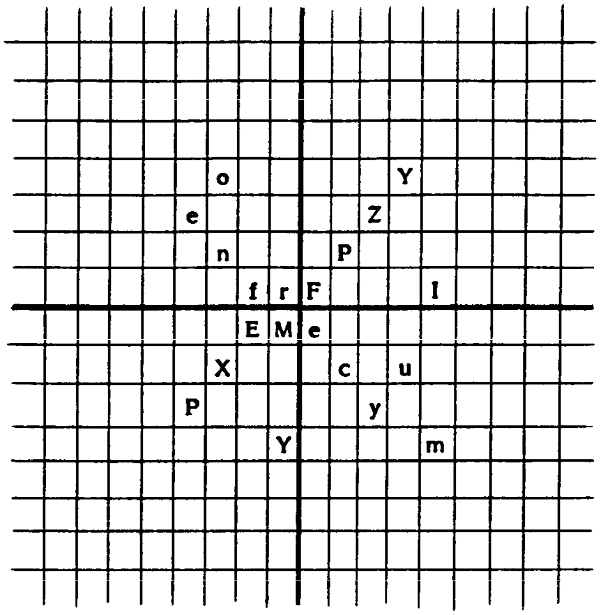
(2) The repeated GBYL segments appear to be numbers, and the number of characters is exactly right to fit in the expanded stereotype *REFERENCE YOUR MESSAGE NUMBER,* before the numbers. To add to this, recent messages from the addressee have been numbered in the mid 4500s. *FOUR FIVE FOUR* is probably the text of the first three numbers.

(3) GHYR occurs at good sentence length intervals and is probably *STOP.*

(4) These possibilities give enough values to begin reconstructing the matrix.

b. If you assume that standard p1 and p2 squares were used, entering the values in the matrix produces conflicts. The squares must be mixed. To recover a mixed four-square, divide a sheet of cross-section paper into four areas, representing the four squares. The areas cannot initially be limited to 5 by 5 squares, although eventually the recovered values will condense into that size. Proceed by entering each plaintext and ciphertext pair of digraphs into the appropriate areas, maintaining the rectangular relationship. Start new rows and columns for each pair entered unless there are one or more values in common with previous entries. The entries for the first seven pairs are shown in the next diagram.

```
refe renc eyou rmes sage  numb erfo urfi vefo ur
FMFE FMPX ZPYX IYYP GGME  TXGS YGGB YLFI HAGB YLMK

  st  op
MRGH YRFM BYYP MMBQ YMHD  MHLN MNOS YPVI DMXH RPGL

          four
MNSO QLMP GBYL VGQI QLYX  KTZG HEEM GBKM FLYK PHMA

SREE GDMK DEBG TTEB IXCN  VINI SOSC HHIG THHM OQPO

                 st  op
TGKI VGQI PMXR CPGH YRSE  PLMN LNMN ACVC OCOO KPWC

          stop
PKIP PCSU GHYR FKSC YGXX
```



c. The first digraph pair entered was plaintext re equalling ciphertext FM, appearing in the inner corners of the four areas. We will use the notation re=FM to represent such pairs from here on with the plaintext in lower case. The next pair, fe=FE was placed on the same row as the first pair because of the common letters with the first pair. The entries continue, placing the letters on new rows and columns except when previously used values occur. The eighth pair, es=YP, presents a new situation. Plaintext e and ciphertext Y are already on different rows. The new pair shows that these two rows should be combined. The diagram below shows the entry before combining the rows. The rows are combined by writing the plaintext o of the first row in the same position on the second row.

					o						Y				
				e						Z	Y				
					n				P						
						f	r	F				I			
						E	M	e							
					X				c		u				
				P						y	s				
							Y					m			

d. When all entries have been made and all rows and columns combined wherever possible, the diagram appears as shown below. All plaintext that can be deciphered from the partially recovered matrix is also filled in.

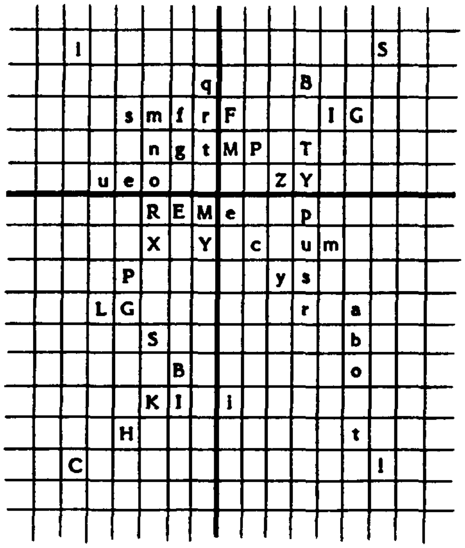
```
refe renc eyou rmes sage  numb erfo urfi vefo ur
FMFE FMPX ZPYX IYYP GGME  TXGS YGGB YLFI HAGB YLMK

 st  opre  es  e                    es         a
MRGH YRFM BYYP MMBQ YMHD  MHLN MNOS YPVI DMXH RPGL

          four        ou   e        fo
MNSO QLMP GBYL VGQI QLYX  KTZG HEEM GBKM FLYK PHMA

SREE GDMK DEBG TTEB IXCN  VINI SOSC HHIG THHM OQPO

 r                st op
TGKI VGQI PMXR CPGH YRSE  PLMN LNMN ACVC OCOO KPWC

          stop      er
PKIP PCSU GHYR FKSC YGXX
```

						g		M							
	f	m		s									G	F	
			u	e	o					Z	Y				
					n				P		T				
						f	r	F				I			
						E	M	e							
					X				c		u				
				P						y	s				
							Y					m			
			L	G							r		a		
		S											b		
	B												o		
	I													i	
				H									t		
					R						p				

e. More plaintext can be added at this point. The four-letter number after *FOUR FIVE FOUR* must be *NINE,* because ZERO will not fit properly in the matrix. The word beginning at the end of the first line is probably *REQUEST*, and the sender is *MILLER*, not ADAMS. When these recoveries are added to the matrix, there are enough recoveries to see the basic structure of the four-square.

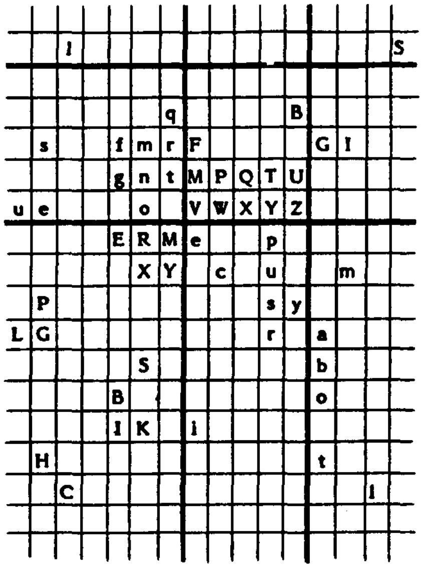
	l												S
						q				B			
		u	e	o					Z	Y			
				n	g	t	M	P		T			
			s	m	f	r	F				I	G	
				R	E	M	e			p			
				X		Y		c		u	m		
			P						y	s			
		L	G							r		a	
				S								b	
					B							o	
				K	I								
			H									t	
	C												l

f. Each area shows signs of alphabetic progression. The upper right area shows partial rows with the letters FGI, MPT, and YZ. The lower left has rows with IK and XY. The upper left has columns with fg, mno, and qrt. The lower right has a column with prsu in it. These patterns suggest that the plaintext squares (upper left and lower right) use sequences entered by columns and the ciphertext squares use sequences entered by rows. With this in mind, the rows and columns can be rearranged. The most obvious place to start is to rearrange the rows so that the partial sequences FGI, MPT, and YZ are the last three rows in the upper squares.



	l												S	
						q				B				
			s	m	f	r	F				I	G		
				n	g	t	M	P		T				
		u	e	o					Z	Y				
				R	E	M	e			p				
				X		Y		c		u	m			
			P						y	s				
		L	G							r		a		
				S								b		
					B							o		
				K	I		i							
			H									t		
	C												l	

g. Moving these three rows put the letters mno and fg in the correct order in the upper left area. The row before these. three rows also appears to be correctly placed. Now examine the column arrangement. In the upper right area, the Y and Z are probably in the last two columns in the original matrix. With the T placed directly above the Y, there are just enough spaces to fill in UVWX between the T and the YZ on the bottom two rows. Then, with the U appearing in the alphabetical progression, the Q is probably the missing letter on the fourth row. The complete fourth row can be placed in MPQTU order. Similarly, in the upper left area, the fg, mno, and qrt columns are probably the second, third, and fourth columns of that matrix. We can now rearrange the columns so the first five columns on each side of the center line reflect the original order.



		l													S
						q					B				
	s			f	m	r	F					G	I		
				g	n	t	M	P	Q	T	U				
u	e				o		V	W	X	Y	Z				
				E	R	M	e			p					
					X	Y		c		u			m		
	P									s	y				
L	G									r		a			
					S							b			
				B								o			
				I	K		i								
	H											t			
		C												l	

h. The rearranged matrix suggests many more possibilities. In the upper left area, uvwxyz can be filled in as was done with the upper right. In the upper right, the G can be moved next to the F, combining two columns. Rows can be rearranged in the lower areas. Examining the lower right area, the fourth column must include the q by the same logic as was used in the upper right area. The correct order is pqrsu.

		l													S
							v								
						q	w				B				
	s			f	m	r	x	F	G					I	
				g	n	t	y	M	P	Q	T	U			
	e				o	u	z	V	W	X	Y	Z			
				E	R	M		e			p				
											q				
	G					L			a		r				
	P										s	y			
					X	Y			c		u			m	
					S				b						
				B					o						
				I	K			i							
	H								t						
		C													l

i. All the rows and columns outside the 5 by 5 squares can be systematically placed in the squares by following the alphabetical order. Fully combined, the four-square appears below.

			p	v					
		l	q	w	S			B	
s	f	m	r	x	F	G	I	K	L
	g	n	t	y	M	P	Q	T	U
e		o	u	z	V	W	X	Y	Z
H	E	R	M		e	t		p	v
	B	C	D	F	l	o		q	w
G	I	K	L		i	a		r	x
P	Q	S	T	U		b		s	y
V	W	X	Y	Z		c	m	u	z

j. The remaining values are easily recovered by using this matrix to fill in more plaintext in the cryptogram. The additional plaintext will suggest still more plaintext, which can be used to complete the four-square.

7-4. Solution of Two-Square Ciphers

The solution of two-square ciphers, either horizontal or vertical, is similar to the solution of a mixed four-square, only much simpler. The worksheet is divided into two areas by a vertical or horizontal line, as appropriate, instead of four. Plaintext is much easier to recognize because of the transparencies that occur. Matrix reconstruction proceeds, like the four-square, by entering digraph pairs in their rectangular relationship, except for transparencies, which are plotted in the same row or column. New values are plotted in new rows and columns, unless one or more values are in common with previous plots, as with the four-square. As recovery proceeds, working back and forth between the matrix and the text, the two-squares can be combined and condensed to the original form, like the four-square.

Section II
Analysis of Playfair Ciphers

7-5. Security of Playfair Ciphers

Breaking into Playfair ciphers is similar to the solution of mixed four-squares in some respects and very different in others.

a. The Playfair shares the rectangular principle of encipherment with four-squares and two-squares, but it is complicated further by the EBDA and ERDL rules. When recoveries are plotted, every possible rule must be considered, not just the rectangular rule.

b. Recognition of plaintext is aided by another type of word pattern that occurs with Playfair only. Whenever a plaintext digraph is repeated in reverse order, the ciphertext appears in reverse order, too. This does not happen with four-squares and two-squares. It occurs whichever rule of decipherment is used. The word DEFENDED, for example, has a Playfair word pattern of AB -- -BA, the same as DEPARTED, RECEIVER, and a number of others. Playfair word patterns are listed in Appendix D, pages D-40 through D-42. The general digraphic word patterns of pages D-38 and D-39 can also be used.

7-6. Reconstruction of Playfair Ciphers

To illustrate the analysis of Playfair ciphers and the reconstruction of the Playfair matrix, consider the following message. This message was sent from a brigade headquarters to three subordinate battalions.

```
DT BV VF GO OG MV CQ IH NS MN VI FC IK FK NX KH UB GK AV LH
CA CF WC YC IA VM PB CI FK CA GV UH NC BX OV LY NU CQ ED GO
OG MV CQ VW OV UB QH CM CM QM UO BX OV YG DH HB KR CY OG MV
CQ IH NS NS QR EX IU GO OG OE GO XK AV DT CB XK AV XK AV YV
TQ RH OC NS NB GS LG FN RH GO CV MX VM SL FU CM GO XK AV KT
GH KT GH DT CB YV TQ
```

a. Initial plaintext recoveries are fairly easy with this message.

(1) The XK AV repeats on line four strongly suggest *ZE RO* with another four digit letter group in between them. The numbers are most likely to be a spelled out time.

(2) YV TQ, appearing after the time and at the end of the message, is probably *ST OP.*

(3) The series of four letter repeats beginning with *ZE RO* at the end of line five and continuing on line six before the final *ST OP* is probably another time.

(4) The repeat GO OG MV CQ has a number of possibilities in Appendix D, but in the context in which the message was sent, it is most likely to be *B AT TA LI ON.*

(5) If BATTALION is correct, then the partial repeat beginning at the end of line three represents the plaintext *TA LI ON.* This is again part of the word BATTALION, but the word started out as an even letter division with the digraph *BA.* TT, the next digraph, is impossible with the Playfair system, so a null must have been inserted, probably *TX.* With the addition of the null, the remainder of the word is divided into digraphs, as before, to produce the partial repeat.

(6) The ciphertext in the middle of line four, GO OG OE GO, which deciphers as *AT TA -- AT* using the common values from *B AT TA LI ON,* is probably *AT TA CK AT.*

b. These plaintext recoveries give more than enough information to reconstruct the original Playfair matrix. The trickiest step in matrix reconstruction is to pick the best starting point. As every possibility for the matrix is plotted, it can get very complicated. Careful selection of what values to place first can reduce the complexity a great deal. The cryptogram is repeated below with all recovered values filled in to assist in finding the best starting point.

```
       b at ta li on
DT BV VF GO OG MV CQ IH NS MN VI FC IK FK NX KH UB GK AV LH

               il                                  on  b at
CA CF WC YC IA VM PB CI FK CA GV UH NC BX OV LY NU CQ ED GO

ta li on                                        ba tx ta li
OG MV CQ VW OV UB QH CM CM QM UO BX OV YG DH HB KR CY OG MV

on                   at ta ck at ze ro       ze ro ze ro st
CQ IH NS NS QR EX IU GO OG OE GO XK AV DT CB XK AV XK AV YV

op                                  il          at ze ro
TQ RH OC NS NB GS LG FN RH GO CV MX VM SL FU CM GO XK AV KT

               st op
GH KT GH DT CB YV TQ
```

(1) Usually the best starting point, if available, is to select a digraph pair where there is a letter in common between the plaintext and ciphertext digraphs. These only occur when adjacent rows or columns are involved, using the ERDL or EBDA rules respectively. This problem does not have any recovered digraph pairs with a common letter, so another starting point must be found.

(2) The next best starting point is to find two digraph pairs with at least two letters in common between the two pairs. The ro=AV and at=GO pairs share the As and Os in common. Other pairs are also possible.

(3) The reconstruction begins by taking one of the selected pairs and plotting each possibility for it. All three rules must be considered. The three separate plots that follow show the result of plotting ro=AV for the rectangular rule, ERDL, and EBDA in turn.

```
Rectangular rule:          ERDL:               EBDA:

   R     A              R A     O V              R
                                                 A


   V     O                                       O
                                                 V
```

(4) The positioning of the letters is arbitrary. In the rectangular plot, we do not know that R is to the left of A or above V. We do not know how many rows and columns occur between the characters. We only know that the four letters form

a rectangle if that is the correct rule. In the ERDL plot, we do not know that RA is to the left of OV or if there is a column in between the pairs or not. Similarly, in the EBDA plot, we do not know that RA comes above OV or if there is a row in between. The spaces and placements are unknown until the reconstruction has proceeded further.

(5) The next step is to add our second pair to the first plots. Again, we have to consider all three rules as we add the second pair. With three possible rules for each pair, there could be as many as nine different possible plots after two pairs if we did not select some letters in common to limit the possibilities.

(6) Consider first, the addition of at=GO to the rectangular plot of the first pair.

```
R   A   G

V   O   T
```

(7) ERDL cannot be used with the second pair, since we have already placed A and O in separate rows. To use ERDL, they must be in the same row.

(8) When EBDA is applied to the at=GO pair and linked to the ro=AV rectangular plot, the plot looks like this.

```
R   A
    G

    T
V   O
```

(9) When we try to link at=GO to the ERDL plot for ro=AV, it cannot be done. With A and O in the same row, the rectangular plot and the EBDA plot cannot be applied properly. If we try to plot ERDL for at=GO, it results in six different letters on the same row, which is not possible in a normal Playfair. Therefore, we can cross out or erase the ERDL plot for ro=AV.

(10) We next plot all possible rules for at=GO with the EBDA plot for ro=AV. The rectangular rule is the only possibility. ERDL for at=GO is impossible, because we have already placed A and O in the same column. EBDA is impossible, because it would place six different letters in the same column.

```
R   A   G  |  R   A  |  R
           |      G  |  A   G
           |         |
V   O   T  |      T  |  O   T
           |  V   O  |  V
```

(11) The next step is to again pick a digraph pair with at least two letters in common with the letters already plotted. The most obvious possibility is the ba=KR on line three. Following the same approach as we did with the second pair, we find four possibilities this time.

R	A	G
V	O	T
B	K	

R	A
	G
	T
V	O
B	K

B	K	A	R	G
		O	V	T

B	K	A	R
		G	
		T	
		O	V

(12) Both st=YV and op=TQ have two letters in common with the recovered diagrams. Checking all possibilities for each of these produces the next four diagrams.

R	A	G
V	O	T
B	K	
S		Y
	Q	P

		A	G	R
S	Y	O	T	V
		K		B
		Q	P	

B	K	A	R	G
		O	V	T
			S	Y
		Q		P

R	A	G		
V	O	T	P	Q
B	K			
S		Y		

(13) Various approaches can be used to further build the possible diagrams. One approach is to try to recover more text. The repeated KT GH is certain to be a spelled out number. If we try to decipher KT using all of our trial diagrams, all

but the third one produce plaintext -O. The third diagram produces G-. From these results, we can rule out the third diagram, since no number has a G in the first position. The number *FO UR* is the only likely plaintext with O in the second position. We add fo=KT to the three remaining diagrams and then try to fit ur=GH. In each case, only the ERDL rule will apply. The last of the three remaining diagrams is also eliminated, since ur=GH cannot be plotted. We are left with these possibilities.

R	H	A	U	G
V		O		T
B		K		F
S				Y
		Q		P

		A	U	G	R	H
S	Y	O		T	V	
		K		F	B	
		Q		P		

(14) The second diagram above is impossible, since there is no way to fit the SY so that it aligns with the row above it. We are finally down to a single diagram, and with careful selection of digraph pairs to plot, we can keep it to a single diagram. Next we will plot on=CQ, tx=CY, and ze=XK.

R	H	A	U	G	
V		O		T	C
B		K		F	E
S		Z		Y	X
		Q		P	N

(15) The X, Y, and Z on the fourth line clearly belong in sequence.

R	H	U	G	A
V		C	T	O
B		E	F	K
S		X	Y	Z
		N	P	Q

(16) The partially reconstructed matrix can now be used to add substantially more plaintext in the message.

```
         b  at  ta  li  on       x          et      ef       a  re  af  ro
DT  BV  VF  GO  OG  MV  CQ  IH  NS  MN  VI  FC  IK  FK  NX  KH  UB  GK  AV  LH

ou  te      xt      il   f      ef  ou  rt  hr      es  to          on   b  at
CA  CF  WC  YC  IA  VM  PB  CI  FK  CA  GV  UH  NC  BX  OV  LY  NU  CQ  ED  GO

ta  li  on      to  re   a              ac  es  to           r  ba  tx  ta  li
OG  MV  CQ  VW  OV  UB  QH  CM  CM  QM  UO  BX  OV  YG  DH  HB  KR  CY  OG  MV

on       x   x   a          at  ta  ck  at  ze  ro      ve  ze  ro  ze  ro  st
CQ  IH  NS  NS  QR  EX  IU  GO  OG  OE  GO  XK  AV  DT  CB  XK  AV  XK  AV  YV

op  ar   t   x   e  ry      ep  ar  at   o      il      eg      at  ze  ro  fo
TQ  RH  OC  NS  NB  GS  LG  FN  RH  GO  CV  MX  VM  SL  FU  CM  GO  XK  AV  KT

ur  fo  ur      ve  st  op
GH  KT  GH  DT  CB  YV  TQ
```

(17) DT CB is clearly FIVE. The word on line five, after op=TQ is AR TI LX LE *RY*. The second row includes the numbers *-F IV EF OU RT HR EX E-*. These additions are placed in the matrix.

```
R H U G A

B D E F K
L   N P Q

S   X Y Z
V I C T O
```

(18) The missing M and W are easily placed alphabetically. The rows are placed in correct order by shifting the last row to the top and placing the remaining rows alphabetically. The keyword is VICTOR HUGO.

(19) To solve Playfair systems like this, it is important to remember to try all possibilities and to keep the work as simple as possible. It is very easy to overlook possible arrangements, so work very carefully. Always look for the digraph pairs with the least possibilities to plot to keep the work from getting very complex. If the square appears to be alphabetical in construction, use the alphabeticity to help you put rows and columns in the correct order whenever you can.

PART FOUR

Polyalphabetic Substitution Systems

CHAPTER 8

PERIODIC POLYALPHABETIC SUBSTITUTION SYSTEMS

Section I
Characteristics of Periodic Systems

8-1. Types of Polyalphabetic Systems

All the substitution systems explained up to this point are monoalphabetic systems. Whether they deal with one letter at a time or several, whether they have one cipher equivalent for each plaintext letter or more than one, they are still systems with only one alphabet. The constant feature that makes a system monoalphabetic is that a given ciphertext value always translates into the same plaintext value. In polyalphabetic systems, a given ciphertext value changes its plaintext meaning.

a. Most polyalphabetic systems are monographic; they encipher a single letter at a time. Polygraphic polyalphabetics are possible, but have little practical military value.

b. A typical polyalphabetic system will use from 2 to 26 different alphabets. Polyalphabetic systems which repeat the same set of alphabets over and over again in the same sequence are known as periodic systems. Polyalphabetic systems which do not keep repeating the same alphabets in the same order are known as aperiodic systems. Periodic systems, because of their regular repeating keys, are generally less secure than aperiodic systems. Aperiodic systems, on the other hand, are generally more difficult to use, unless the encipherment is done automatically by a cipher machine or computer.

c. The classic types of polyalphabetic systems use a set of alphabets, such as the 26 alphabets pictured in Figure 8-1. Figure 8-1, known as a Vigenere square, includes all possible alignments of a direct standard alphabet. Mixed alphabets can also be used in such a square. If all 26 alphabets are used, any letter can equal any other letter. There are necessarily three elements to the encryption process with polyalphabetic ciphers, which the square and the accompanying examples illustrate. The plaintext letters are listed across the top of the square. The cipher equivalents are found in the 26 sequences below. The final element is the key that designates which alphabet is used at any given time. The key letter is found on the left side of the square. The first example in Figure 8-1 shows the use of a repeating key based on a keyword. Since the same key is repeated over and over again, the resulting system is periodic. The second example uses a nonrepeating key based on a quotation. Since this key does not repeat, it is an aperiodic system. Note that the reuse of the same alphabets does not constitute a repeating key. For the system to be classified as periodic, the same alphabets must be reused over and over again in the same sequence.

Plaintext

Key

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

PERIODIC

Plain:	repor	tatze	rotwo	twoze	rotom	orrow
Key:	RIFLE	RIFLE	RIFLE	RIFLE	RIFLE	RIFLE
Cipher:	IMUZV	KIYKI	IWYHS	KETKI	IWYZQ	FZWZA

APERIODIC

Plain:	mount	ainpa	ssesb	locke	dbyhe	avysn	owfal	llast	night
Key:	FOURS	COREA	NDSEV	ENYEA	RSAGO	OURFO	REFAT	HERSB	ROUGH
Cipher:	RCOEL	CWETA	FVWWW	PBAOE	UTYNS	OPPXB	FAKAE	SPRKU	EWANA

Figure 8-1. Use of Vigenere square.

d. Another way to picture the same system as the first example in Figure 8-1 is shown below. In this case, instead of using the complete alphabet square, only the alphabets actually used are shown. These alphabets are used repeatedly to produce the same results. In this example, the key is expressed in terms of the number of the cipher sequence used, instead of by the repeating key letters.

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C1:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
C2:	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
C3:	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
C4:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
C5:	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Plaintext:	repor	tatze	rotwo	twoze	rotom	orrow
Key:	12345	12345	12345	12345	12345	12345
Ciphertext:	IMUZV	KIYKI	IWYHS	KETKI	IWYZQ	FZWZA

e. Another type of polyalphabetic system does not use multiple alphabets in the classic sense, but instead enciphersa message in a single alphabet. Then it applies either a repeating key or nonrepeating key to the first encipherment to create a polyalphabetic. One method of applying a polyalphabetic key to a monoalphabetic encipherment is to use a numeric system and arithmetically add a key to it. For example, here is a dinomic system, which has been further enciphered by a repeating numeric additive. The first encipherment is labeled I, for intermediate cipher, and the second encipherment is labeled C. The 8-digit repeating key is labeled K. Modulo 10 arithmetic is used (paragraph 5-3f(1)).

	0	1	2	3	4	5	6	7	8	9
3	m	u	r	p	h	y	s	l	a	w
6	b	c	d	e	f	g	i	j	k	n
9	o	q	t	v	x	z	.	,	?	/

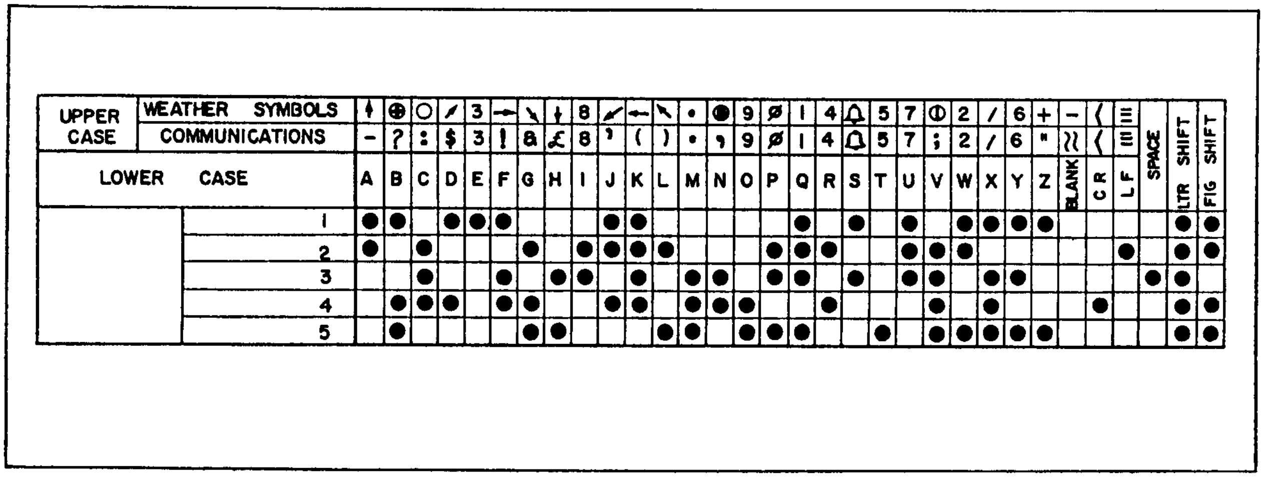
p:	a t	t a	c k	a t	z e	r o	n i	n e	h u	n d	r e	d .
I:	3892	9238	6168	3892	9563	3290	6966	6963	3431	6962	3263	6296
K:	4209	9336	4209	9336	4209	9336	4209	9336	4209	9336	4209	9336
C:	7091	8564	0367	2128	3762	2526	0165	5299	7630	5298	7462	5522

f. Another approach to applying a polyalphabetic key begins with the built-in encoding system used by teleprinters or computers. Paragraph 8-2 shows examples of these.

8-2. Machine Based Polyalphabetics

When text is sent electronically by radio or wire, some form of coding must be used. The earliest system of coding for electronic transmission was Morse code, which is still used widely today. When teleprinters took their place in communications, a new binary type of coding system was devised, which can be handled by machine more easily than Morse code can. Any binary coding system uses only two characters, which can be represented electronically as a signal pulse or no signal pulse, high voltage or low voltage, or one frequency or another frequency. Which of these approaches is used depends on the equipment in use and is not our concern here. We are concerned with how the two binary characters, whatever their electronic origin, are combined to represent alphabetic, numeric, and special characters, and how they may further be encrypted. Various notations have been used to represent the two binary characters—Xs and 0s, 1s and 0s, +s and -s, or Ms (for marks) and Ss (for spaces). We will use 1s and 0s in this text, but you should be aware that you may see other notations elsewhere, particularly in older literature.

a. **The Baudot Code.** Teleprinter systems generally use a 5-digit binary code known originally as the Baudot code. There are 32 possible combinations of 5 digits, which are not enough for the letters, numbers, and printer control characters needed for communications. The number of possible characters is approximately doubled by the use of upper and lower shift characters, similar to the shift key on a typewriter, giving all characters two alternate meanings except the shift characters themselves and the space character. There are still not enough characters for upper and lower case letters, so all traffic passed by such teleprinter systems use capital letters only. The standard international teleprinter code is shown in Figure 8-2. Each dot represents a 1 and each space represents a 0. Other codes are also used besides the one shown.



UPPER CASE	WEATHER SYMBOLS	↑	⊕	○	↗	3	→	↘	↓	8	↙	←	↖	•	⬤	9	Ø	1	4	🔔	5	7	⏀	2	/	6	+	−	⟨	≡	SPACE	LTR SHIFT	FIG SHIFT
	COMMUNICATIONS	−	?	:	$	3	!	&	£	8	'	(	)	.	,	9	Ø	1	4	🔔	5	7	;	2	/	6	"	≀	⟨	≡			
LOWER CASE		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	BLANK	CR	LF			
	1	●	●		●	●	●				●	●						●		●		●		●	●	●	●					●	●
	2	●		●				●		●	●	●	●				●	●	●			●	●	●						●		●	●
	3			●			●		●	●		●		●	●		●	●		●		●	●		●	●					●	●	
	4		●	●	●		●	●			●	●		●	●	●			●				●		●				●			●	●
	5		●					●	●				●	●		●	●	●			●		●	●	●	●	●					●	●

Figure 8-2. International teleprinter code.

The binary digits themselves are known as bauds—a term derived from the Baudot code. The terminology has carried over into modern computer. systems as well. Polyalphabetic keys, also in 5-digit binary form, are easily applied to coded text electronically by baud addition. An example of this process is shown below. Although other rules are also possible, the addition of key and plaintext bauds is usually accomplished by the rule, *Like values sum to 0; unlikes sum to 1.* (In computer logic, this would be called an exclusive OR, or XOR operation.)

Plaintext:	e	n	e	m	y
Bauded plain:	10000	00110	10000	00111	10101
Key:	**01010**	**11010**	**10100**	**01110**	**10110**
Bauded cipher:	11010	11100	00100	01001	00011
Ciphertext:	J	U	(space)	L	O

One advantage of this rule of addition is that adding the same key to the ciphertext produces the plaintext again.

b. **Computer Codes.** Communications between computers use more than 5 digits. Typical computer codes use either 7- or 8-binary digits (bits), giving a range of 128 characters or 256 characters. These permit upper and lower case letters, a full range of punctuation marks and special characters, and a number of codes to control printers and communications devices as well. With the 8-bit, 256 character set, graphics may also be enabled to permit transmitting pictures as well as text. The most common standard for the first 128 characters, whether 7-bit or 8-bit, is the American standard code for information interchange (ASCII) standard, which you can find in many computer manuals. Encipherment and decipherment can be accomplished in 7- and 8-bit operation just as was shown for 5-digit teleprinter operations. The more complex systems are far beyond the scope of this manual, but simple repeating key systems can be solved using the techniques discussed here. One problem that computer codes present is that less than half of the possible 7-bit characters are letters and numbers, and many of them stand for printer control codes that do not print out as characters normally. Working with binary numbers themselves is unwieldy, but any 7- or 8-bit value can be represented by two hexadecimal (base 16) arithmetic digits. Hexadecimal arithmetic is not explained here, but explanations are available in many computer manuals and texts, if needed. Hexadecimal and binary numbers are also explained in Army Correspondence Course Program Subcourse SA0709.

Section II
Identifying Periodic Systems

8-3. Analysis of Repeated Ciphertext

Polyalphabetic systems normally have very flat frequency counts. The phi IC is normally close to the random expectation of 1.00. Since other systems, including variant multiliterals and aperiodic systems, also can produce flat frequency counts, this is not enough to identify a system as periodic. The key to identifying a system as periodic is to recognize through repeated ciphertext that a repeating key is used.

a. Repeated ciphertext can occur in two ways. Whenever the same plaintext is enciphered by the same keys, the ciphertext will also repeat. Such repeats are called causal repeats. The second way that ciphertext can repeat is by pure chance. Different plaintext enciphered with different keys will sometimes produce short ciphertext repeats. Causal repeats are much more likely to occur than accidental repeats, particularly if they are longer than two or three characters. The example below, repeated from Section I, shows how causal repeats occur.

Plaintext:	repor	tatze	rotwo	twoze	rotom	orrow
Key:	12345	12345	12345	12345	12345	12345
Ciphertext:	IMUZV	KIYKI	IWYHS	KETKI	IWYZQ	FZWZA

The plaintext words *ZERO* and *TWO* both occur twice. The repeated *ZEROs* lined up with the same alphabets, producing a ciphertext repeat. The repeated *TWOs* lined up with different alphabets and did not produce a ciphertext repeat.

b. Whenever causal repeats occur, the distance between them must be a multiple of the period length. In the example above, the two *ZEROs* occurred 10 letters apart. Note that the distances are counted from the first letter of one repeat to, but not including, the first letter of the second repeat. If the distance was not a multiple of the period five, the ciphertext repeat would not have occurred.

c. The distance between causal repeats is a multiple of the period length. Given a cryptogram of unknown period that includes ciphertext repeats, the period can be determined, or at least narrowed down, by analyzing the distances between repeats. The period must be a factor of the distance. The factors of a number are all the numbers which divide evenly into that number. When there is more than one repeat, the period must be a common factor of all such distances. For example, if a cryptogram has repeats that are 28, 35, and 42 letters apart, the only number that evenly divides all the distances is 7. The period must be 7. Utility tables showing common factor numbers are in Appendix E.

d. Here is a more complex example. Suppose a cryptogram suspected of being periodic includes the following repeats.

Repeat	Distance
GXKLRYPDL	84
ZBHHNST	90
XTVTB	36
SRM	35

The next step after determining the distances is to list the factors for each repeat, as shown below.

Repeat	Distance	Factors
GXKLRYPDL	84	2, 3, 4, 6, 7, 8, 12
ZBHHNST	90	2, 3, 5, 6, 9, 10
XYVTN	36	2, 3, 4, 6, 9, 12
SRM	35	5, 7

No numbers evenly divide the distances between all the repeats. In such cases, either the system was not a periodic system, or one or more of the repeats is accidental. In this problem, the SRM repeat is probably accidental, because it is the shortest. Discarding the SRM repeat from consideration, the remaining repeats all have common factors of 2, 3, and 6. Where more than one factor is possible, it is generally safest to assume the largest. If the period is actually 3, for example, it will reveal itself by repeated alphabets as the cryptogram is solved.

8-4. Analysis by Frequency Counts

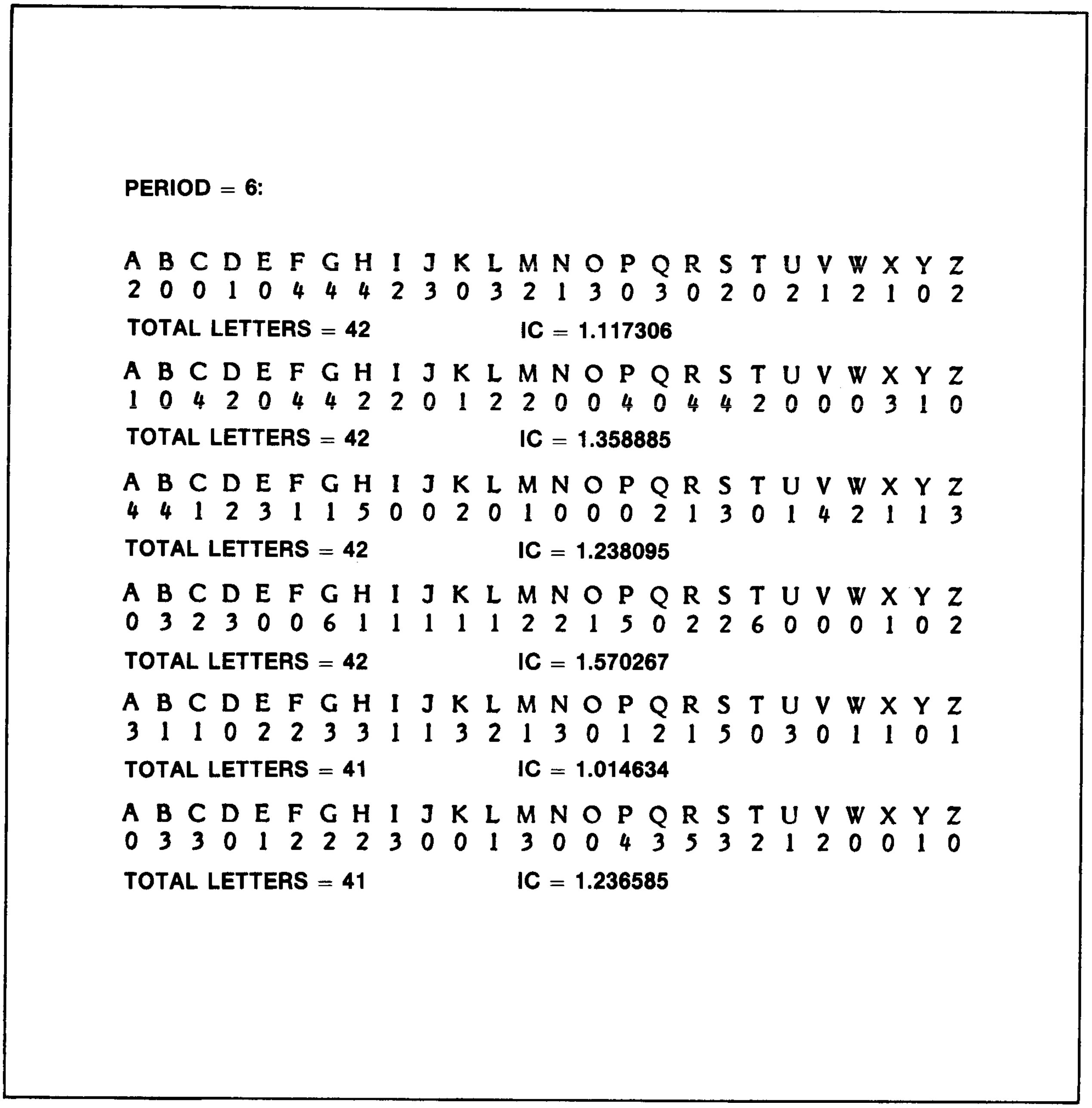
Periodic systems can be identified even when there are no repeated words in the text. Causal single-letter ciphertext repeats will still occur and significantly outnumber the accidental single-letter repeats.

a. To find the causal single-letter repeats, take frequency counts for each alphabet according to its position in the suspected repeating cycle. If the period is incorrect, the separate frequency counts will remain flat. If the period is correct, the separate frequency counts will be as rough as plaintext on the average. Recognizing when a count is rough or flat is difficult by eye, particularly with anything but very long cryptograms, but the phi test performed on each separate alphabet gives a reliable indication. Taking separate frequency counts by position for each suspected period and then calculating phi tests on each is a laborious and time-consuming process by hand. It can be done when necessary, but it is best performed by computer support. Figures 8-3, 8-4, and 8-5 show computer generated output for suspected periods of 6, 7, and 8 for the following cryptogram.

```
LPADW GUGHG ETZHV KSRQS ACNPJ  GHTHH QCKGS CHHRB HMDIH HMCJM
EXEVH LVPQS OCHPK MZYBZ SMMPF  TLBGF KRAEA FBMHQ IXSZC PGAQT
KPLPS GXIVX BGFRI TSTGF SPYNS  SNTAL SIOSC MJRMI ZSICF RQTUV
HLVPQ SOCHP KQFDW SFRAK MILRG  GECAU HFEGN YXXZO GLGMZ DUHUC
XGRIL SARZQ FDWBB PSRUD UGJGD  JNTWF BTABQ SVBGF WRDPP BFRGN


 A  B  C D E  F  G  H I J K L  M N O  P  Q  R  S  T U V W X Y Z
10 11 11 8 6 13 20 17 9 5 7 9 11 6 4 14 10 13 19 10 7 7 5 7 3 8

TOTAL LETTERS = 250                          MONOGRAPHIC IC = 1.098474
```

b. The average ICs for each period in Figure 8-3 and 8-4 are flat, The average IC for a period of 8 in Figure 8-5 is much higher than the other two. This clearly shows that the period of 8 is more likely correct than periods of 6 and 7.

c. The computer program used to generate these examples is listed in Appendix F. It is written in GW BASIC, and is readily adaptable to many different computers.



```
PERIOD = 6:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2 0 0 1 0 4 4 4 2 3 0 3 2 1 3 0 3 0 2 0 2 1 2 1 0 2
TOTAL LETTERS = 42          IC = 1.117306
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 0 4 2 0 4 4 2 2 0 1 2 2 0 0 4 0 4 4 2 0 0 0 3 1 0
TOTAL LETTERS = 42          IC = 1.358885
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
4 4 1 2 3 1 1 5 0 0 2 0 1 0 0 0 2 1 3 0 1 4 2 1 1 3
TOTAL LETTERS = 42          IC = 1.238095
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 3 2 3 0 0 6 1 1 1 1 1 2 2 1 5 0 2 2 6 0 0 0 1 0 2
TOTAL LETTERS = 42          IC = 1.570267
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 1 1 0 2 2 3 3 1 1 3 2 1 3 0 1 2 1 5 0 3 0 1 1 0 1
TOTAL LETTERS = 41          IC = 1.014634
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 3 3 0 1 2 2 2 3 0 0 1 3 0 0 4 3 5 3 2 1 2 0 0 1 0
TOTAL LETTERS = 41          IC = 1.236585
```

Figure 8-3. Frequencies, period 6.

PERIOD = 7:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	2	2	2	1	3	4	1	1	0	0	1	1	1	1	1	3	1	2	2	1	2	0	1	0	1

TOTAL LETTERS = 36 IC = .784127

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	0	1	1	2	4	3	4	1	1	3	1	1	1	0	2	0	1	4	2	2	0	0	1	0	0

TOTAL LETTERS = 36 IC = 1.155556

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	2	1	2	0	1	1	2	3	0	1	1	4	2	1	2	2	1	2	0	1	1	2	1	0	1

TOTAL LETTERS = 36 IC = .7428572

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	1	5	1	2	0	2	2	1	2	1	1	1	0	0	2	1	3	1	2	1	1	1	0	2	1

TOTAL LETTERS = 36 IC = .8666667

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	2	0	1	0	2	2	2	0	0	1	3	2	2	1	1	1	3	4	1	1	1	2	3	1	0

TOTAL LETTERS = 36 IC = .9079365

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	2	0	0	2	4	4	1	1	0	0	1	0	0	4	1	2	2	2	0	2	0	1	0	3

TOTAL LETTERS = 35 IC = 1.22353

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	2	0	1	1	1	4	2	2	1	1	2	1	0	1	2	2	2	4	1	1	0	0	0	0	2

TOTAL LETTERS = 35 IC = .9176471

Figure 8-4. Frequencies, period 7.

```
PERIOD = 8:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 0 0 1 1 2 3 3 0 3 4 1 1 1 0 0 0 0 4 0 0 2 1 1 0 1
TOTAL LETTERS = 32          IC = 1.362903

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 1 1 0 0 0 5 0 0 1 1 1 4 1 0 5 3 7 0 0 0 0 0 0 1 0
TOTAL LETTERS = 32          IC = 2.620968

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 0 0 2 2 3 0 1 2 0 0 0 2 1 0 0 6 1 2 0 1 0 0 2 1 2
TOTAL LETTERS = 31          IC = 1.565592

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 0 1 5 1 0 0 0 6 0 0 0 0 1 0 1 0 0 4 7 1 0 0 3 1 0
TOTAL LETTERS = 31          IC = 3.075269

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2 1 0 0 1 0 0 4 0 0 1 3 0 0 3 1 0 0 3 0 3 2 4 0 0 3
TOTAL LETTERS = 31          IC = 1.621505

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 4 3 0 0 3 2 5 0 0 0 0 0 0 1 1 0 1 5 1 0 2 0 1 0 2
TOTAL LETTERS = 31          IC = 1.956989

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 4 2 0 1 2 5 4 1 1 0 1 1 2 0 0 1 1 1 0 2 1 0 0 0 0
TOTAL LETTERS = 31          IC = 1.453764

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 4 0 0 3 5 0 0 0 1 3 3 0 0 6 0 3 0 2 0 0 0 0 0 0
TOTAL LETTERS = 31          IC = 2.460215
```

Figure 8-5. Frequencies, period 8.

CHAPTER 9

SOLUTION OF PERIODIC POLYALPHABETIC SYSTEMS

Section I
Systems Using Standard Cipher Alphabets

9-1. Approaches to Solution

When standard alphabets are used with monoalphabetic systems, three approaches are possible. The simplest occurs when text can be immediately identified. Identification of only two or three letters in a standard unilateral alphabet is sufficient to reconstruct and confirm the entire alphabet. The other two methods, where text is not readily identifiable, are to match frequency patterns to the normal A through Z pattern and to generate all possible solutions. All three of these methods also apply to standard alphabet periodic polyalphabetics.

9-2. Solution by Probable Word Method

When the alphabets in a periodic system are known or suspected to be standard, the identification of one plaintext word is usually enough to recover the whole system. The period must be identified first, as explained in the previous chapter, either by analysis of repeat intervals or by the phi test. Then when a word is recognized from repeats or stereotypes, the alphabets can be written and tried throughout the cryptogram. If they produce good plaintext throughout, the problem is solved.

```
EIYMB EKVWO YBTOE ILMFK CRRAK  WJWBZ ELUYO NZUZF ZNTIH YMZXT
IMSWG WRRPC HFGNV ZQALN QCNGJ  VBFSQ RVFPO ENISI CIMHJ SJDBT
ALSDI CSOGH ZYAWW JCEQE MRCFY  KIIXC SERRE RGZPB RMJDC IMRHZ
SFZXT TWQHW YHVAG UYDUS QPGJD  BTSGZ JYAGK KARXQ MJE
```

Repeats	Distance	Factors
ZXT	105	3, 5, 7
CIM	54	3, 6, 9
JBDT	77	7, 11

Factor analysis does not show us a clearcut period length, but if we select the four letter repeat as the most likely causal repeat, 7 appears to be the correct period. If we also try *STOP* as the four letter repeat, it gives us the following text and alphabets.

```
re    nais    cer e   t sen     smov    he av    idge    ing
EIYMB EKVWO YBTOE ILMFK CRRAK  WJWBZ ELUYO NZUZF ZNTIH YMZXT

e   p men    owar    ud dy     erso    ofb a   r svi    stop
IMSWG WRRPC HFGNV ZQALN QCNGJ  VBFSQ RVFPO ENISI CIMHJ SJDBT

   my po    ions    ngr i   h  ave    nhea    yr ei    rced
ALSDI CSOGH ZYAWW JCEQE MRCFY  KIIXC SERRE RGZPB RMJDC IMRHZ

  ing p   f our    htho    st  op    sonc    and i
SFZXT TWQHW YHVAG UYDUS QPGJD  BTSGZ JYAGK KARXQ MJE
```

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C1:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
C2:	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
C3:																										
C4:																										
C5:																										
C6:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
C7:	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

From the partial plaintext that this produces, *STOP* is clearly correct. Such words as *RECONNAISSANCE, HEAVY,* and *REINFORCED* are apparent, any one of which will complete the solution. For another type of probable word approach, applicable to periodics or aperiodic, see paragraph 10-3c on crib dragging.

9-3. Solution by Frequency Matching

With monoalphabetic systems using standard alphabets, the solution was very easy whenever a message was long enough to give a recognizable pattern. The characteristic pattern of highs and lows of a standard sequence cannot be easily concealed. The same technique applies to polyalphabetic systems, although messages necessarily must be longer to produce a recognizable pattern for each separate alphabet.

```
FNPDM GJRMF FTFFZ IQKTC LGHAS   EOSIM PVLZF LJEWU WTEAH EOZUA
NBHNJ SXFFT JNRGR KOEXP GZSEY   XHNFS EZAGU EORHZ XQMRH ZBLTF
BYQDT DAKEI LKSIP UYKSX BTERQ   QTWPI SAOSF TQKTS QLZVE EYVAE
JSNFB IFNEI OZJNR RFSPR TEHNJ   ROJSI UOCZB GQPLI STUAE KSSQT
EFXUJ NFGKO UHLZF HPRYV TUSCP   JDJSE BLSYU IXDSJ JAEVF KJNQF

FIFMP EHYQD
```

a. Factor analysisisshows common factors of three and six for all repeat intervals. Based, on this, a frequency count for six alphabets is produced, as listed in Figure 9-1. If the period were actually three, the first and fourth, the second and fifth, and the third and sixth frequency counts would be similar. This is clearly not the case, so the period is confirmed as six.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	2	0	0	3	5	0	0	0	10	0	0	0	0	2	4	4	0	4	3	6	0	0	1	0	0

TOTAL LETTERS = 44 IC = 2.638478

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	0	2	2	7	1	0	1	2	0	0	1	1	6	2	1	0	4	5	2	1	1	1	0	0	0

TOTAL LETTERS = 44 IC = 1.731501

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	1	0	6	2	0	1	0	0	0	5	2	2	3	4	2	2	0	3	0	0	1	3	4	1

TOTAL LETTERS = 43 IC = 1.468439

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	0	3	3	6	3	0	4	2	3	2	0	0	0	1	0	4	1	1	1	3	0	1	0	4

TOTAL LETTERS = 43 IC = 1.439646

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	3	0	1	0	7	1	7	1	0	1	0	1	0	2	0	3	1	8	1	0	0	1	1	0	1

TOTAL LETTERS = 43 IC = 2.303433

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	0	0	0	1	0	3	1	4	2	5	1	1	3	1	0	1	0	2	4	2	1	0	1	3	5

TOTAL LETTERS = 43 IC = 1.295681

Figure 9-1. Periodic frequencies.

b. The easiest patterns to match are generally those with the highest ICs. The first, second, and fifth alphabets have the highest ICs, and all can be matched fairly easily. In the first, plaintext A equals ciphertext B. In the second, plaintext A equals ciphertext A, and in the fifth, plaintext A equals ciphertext O. Other alphabets can be matched, too, but using these as an example, the partially reconstructed text is shown below.

```
en  y  ir   r ef   c sc   t r  e  u  ov  r  ie   i da   a ta
FNPDM GJRMF FTFFZ IQKTC LGHAS  EOSIM PVLZF LJEWU WTEAH EOZUA

  t i s  r  in  d  ne   s re    t es   m t e  t  wo  t  al
NBHNJ SXFFT JNRGR KOEXP GZSEY  XHNFS EZAGU EORHZ XOMRH ZBLTF

n pd   m di   e o u  e  at  c   sw   e ns   c ss   l d e  m
BYQDT DAKEI LKSIP UYKSX BTERQ  QTWPI SAOSF TQKTS QLZVE EYVAE

is  n  en   a in   r or   t i  r  e  to  n  pp   e ta   e pt
JSNFB IFNEI OZJNR RFSPR TEHNJ  ROJSI UOCZB GQPLI STUAE KSSQT

  j i n  w  th  r  or   f rc    p re   e t i  e  ia  r  in
EFXUJ NFGKO UHLZF HPRYV TUSCP  JDJSE BLSYU IXDSJ JAEVF KJNQF

r em   t pd
FIFMP EHYQD
```

c. The letter combinations produced by the three recovered alphabets are consistent with good plaintext. Expanded plaintext can be recognized in many places. The first word is *ENEMY* for example. Filling in added plaintext is a surer and quicker means of completing the solution at this point than trying to match more alphabets. Here is the complete solution.

```
enemy airbo rnefo rcesc aptur  edbug ovair field indaw natta
FNPDM GJRMF FTFFZ IQKTC LGHAS  EOSIM PVLZF LJEWU WTEAH EOZUA

ckthi smorn ingpd enemy stren  gthes timat edatt wobat talio
NBHNJ SXFFT JNRGR KOEXP GZSEY  XHNFS EZAGU EORHZ XOMRH ZBLTF

nspdi mmedi ateco unter attac  kswer eunsu ccess fulpd enemy
BYQDT DAKEI LKSIP UYKSX BTERQ  QTWPI SAOSF TQKTS QLZVE EYVAE

iscon centr ating armor inthi  rdsec torin appar entat tempt
JSNFB IFNEI OZJNR RFSPR TEHNJ  ROJSI UOCZB GQPLI STUAE KSSQT

tojoi nupwi thair borne force  spdre quest immed iater einfo
EFXUJ NFGKO UHLZF HPRYV TUSCP  JDJSE BLSYU IXDSJ JAEVF KJNQF

rceme ntspd
FIFMP EHYQD
```

p:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C1:	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C2:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C3:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
C4:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
C5:	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
C6:	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

9-4. Solution by the Generatrix Method

With standard alphabets or any known alphabets, the method of completing the plain component can be used. This method, when applied to periodic systems, is commonly called the generatrix method. The advantage of this method over frequency matching is that it will work even with fairly short cryptograms. Just as with a monoalphabetic system (see paragraph 4-11), the first step is a trial decryption at any alphabet alignment, followed by listing the plain component sequence vertically underneath each letter of the trial decryption. Whenever the plain and cipher sequences are identical and in the same direction, no trial decryption is necessary. The key difference with periodic systems is that the process must be applied to the letters of each alphabet separately. Plaintext will not be immediately obvious when you look at the generated lines of letters from only a single alphabet, so selection must be initially based on letter frequencies and probabilities rather than recognizable text. The process is illustrated with the following cryptogram enciphered with direct standard alphabets.

QNMZC TAAED FASRR TITYI UGPGW QVMAX TRMRM ZHMNZ KFQEI RIOUX

XAAGR UGPG

a. The cryptogram has a period of five, which can be confirmed either through periodic-phi tests or factor analysis of all the repeats, including two letter repeats, which are not underlined.

b. The most obvious step to try is to substitute *STOP* for the four letter repeat. It does not produce plaintext elsewhere, however. More powerful methods of solution are required.

c. The cryptogram can be readily solved by the generatrix method. The first step is to separate the letters produced by each alphabet. The letters from each of the five alphabets are listed separately below. Notice that if you read all the first letters, it produces the first group of the cryptogram. The second letters produce the second group and so on.

QTFTUQTZKRXU NAAIGVRHFIAG MASTPMMMQOAP ZERYGARNEUGG CDRIWXMZIXR

d. No trial decryption is required, because the same sequence is expected for both the plain and cipher components. Therefore, the next step is to complete the plain component sequence for each letter grouping. This is illustrated in Figure 9-2.

```
QTFTUQTZKRXU    NAAIGVRHFIAG    MASTPMMMQOAP    ZERYGARNEUGG    CIRIWXMZIXR
296962902836 62 888855876885 84 688966662886 79 098658889655 77 78885360838 64
RUGUVRUALSYV    OBBJHWSIGJBH    NBTUQNNNRPBQ    AFSZHBSOFVHH    DJSJXYNAJYS
865658687865 78 844175885147 62 849628888642 73 868074886577 74 71813688168 57
SVHVWSVBMTZW    PCCKIXTJHKCI    OCUVROOOSQCR    BGTAICTPGWII    EKTKYZOBKZT
857558546905 67 677283917278 67 876588888278 83 459887965588 82 92926084209 51
TWIWXTWCNUAX    QDDLJYUKILDJ    PDVWSPPPTRDS    CHUBJDUQHXJJ    FLULZAPCLAU
958539578683 76 277716628771 61 675586669878 81 776417627311 52 67670867786 68
UXJXYUXDOVBY    REEMKZVLJMEK    QEWXTQQQUSET    DIVCKEVRIYKK    GMVMABQDMBV
631366378546 58 899620571692 64 295392226899 66 785729588622 69 56568427645 58
VYKYZVYEPWCZ    SFFNLAWMKNFL    RFXYURRRVTFU    EJWDLFWSJZLL    HNWNBCRENCW
562605696570 57 866878562867 77 863668885966 79 915776581077 63 78584789875 76
WZLZAWZFQXDA    TGGOMBXNLOGM    SGYZVSSSWUGV    FKXEMGXTKAMM    IOXOCDSFODX
507085062378 51 955864387856 74 856058885655 69 623965392866 65 88387786873 73
XAMABXAGRYEB    UHHPNCYOMPHN    THZAWTTTXVHW    GLYFNHYULBNN    JPYPDETGPEY
386843858694 72 677687686678 82 970859993575 76 576687667488 78 16667995696 70
YBNBCYBHSZFC    VIIQODZPNQIO    UIABXUUUYWIX    HMZGOIZVMCOO    KQZQEFUHQFZ
648476478067 67 588287068288 70 688436666583 69 760588056788 68 22029667260 42
ZCOCDZCITAGD    WJJRPEAQORJP    VJBCYVVVZXJY    INAHPJAWNDPP    LRARFGVIRGA
078770789857 73 511869828816 63 514765550316 48 888761858766 78 78886558858 76
ADPDEÁDJUBHE    XKKSQFBRPSKQ    WKCDZWWWAYKZ    JOBIQKBXOEQQ    MSBSGHWJSHB
876798716479 79 322826486822 53 527705558620 52 184822438922 53 68485751874 63
BEQEFBEKVCIF    YLLTRGCSQTLR    XLDEAXXXBZLA    KPCJRLCYPFRR    NTCTHIXKTIC
492964925786 71 677985782978 83 377983334078 62 267187766688 72 89797832987 77
CFRFGCFLWDJG    ZMMUSHDTRUMS    YMEFBYYYCAMB    LQDKSMDZQGSS    OUDUIJYLUJD
768657675715 70 066687798668 77 669646667864 74 727286702588 62 86768167617 63
DGSGHDGMXEKH    ANNVTIEUSVNT    ZNFGCZZZDBNC    MRELTNEARHTT    PVEVJKZMVKE
758577563927 71 888598968589 91 086570007487 52 689798988799 97 65951206529 50
EHTHIEHNYFLI    BOOWUJFVTWOU    AOGHDAAAECOD    NSFMUOFBSIUU    QWFWKLANWLF
979789786678 91 488561659586 71 885778889787 90 886668648866 80 25652788576 61
FIUIJFIOZGMJ    CPPXVKGWUXPV    BPHIEBBBFDPE    OTGNVPGCTJVV    RXGXLMBOXMG
686816880561 63 766352556365 59 467894446769 74 895856579155 73 83537648365 58
GJVJKGJPAHNK    DQQYWLHXVYQW    CQIJFCCCGEQF    PUHOWQHDUKWW    SYHYMNCPYNH
515125168782 51 722657735625 57 728167775926 67 667852776255 66 86766876687 75
HKWKLHKQBIOL    ERRZXMIYWZRX    DRJKGDDDHFRG    QVIPXRIEVLXX    TZIZNODQZOI
725277224887 61 988036865083 64 781257777685 70 258638895733 67 90808872088 58
ILXLMILRCJPM    FSSAYNJZXASY    ESKLHEEEIGSH    RWJQYSJFWMYY    UAJAOPERAPJ
873768787166 74 688868102886 70 982779998587 88 851268165666 60 68188698861 69
JMYMNJMSDKQN    GTTBZOKAYBTZ    FTLMIFFFJHTI    SXKRZTKGXNZZ    VBKBPQFSBQK
166681687228 61 599408286490 64 697686661798 79 832809253800 48 54246268422 45
KNZNOKNTELRO    HUUCAPLBZCUA    GUMNJGGGKIUJ    TYLSAULHYOAA    WCLCQRGTCRL
280882899788 77 766786740768 72 566815552861 58 967886776888 88 57772859787 72
LOAOPLOUFMSP    IVVDBQMCADVB    HVNOKHHHLJVK    UZMTBVMIZPBB    XDMDRSHUDSM
788867866686 84 855742678754 68 758827777152 66 606945680644 58 37678876786 73
MPBPQMPVGNTQ    JWWECRNDBEWC    IWOPLIIIMKWL    VANUCWNJAQCC    YENESTIVETN
664626655892 65 155978874957 75 858678886257 78 588675818277 72 69898985998 88
NQCQRNQWHOUR    KXXFDSOECFXD    JXPQMJJJNLXM    WBOVDXOKBRDD    ZFOFTUJWFUO
827288257868 71 233678897637 69 136261118736 45 548573824877 68 06869615668 61
ORDRSORXIPVS    LYYGETPFDGYE    KYQRNKKKOMYN    XCPWEYPLCSEE    AGPGUVKXGVP
887888838658 85 766599667569 81 262882228668 60 376596677899 82 85656523556 56
PSESTPSYJQWT    MZZHFUQGEHZF    LZRSOLLLPNZO    YDQXFZQMDTFF    BHQHVWLYHWQ
689896861259 77 600766259706 54 708887776808 74 672360267966 60 47275576752 57
```

Figure 9-2. Generatrix method.

e. To aid in selection of the most likely generated letter sequences, numeric probability data has been added to each line of the listing. The numbers listed below each letter are assigned on the basis of logarithmic weights of the letter probabilities. To the right of each group of logarithmic weights is the sum of the weights for that group. Using this kind of weighting lets us determine the relative probabilities of each line by adding the weights for each letter. The weights in Figure 9-2 have been added according to the log weights shown in Table 9-1.

Table 9-1. Logarithmic weights of letter probabilities.

Letter:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Log weight:	8	4	7	7	9	6	5	7	8	1	2	7	6	8	8	6	2	8	8	9	6	5	5	3	6	0

f. The listing in Figure 9-2 was computer generated. When this work must be done manually, it is easier to generate the sequences without the probability data. Then scan the generated rows for each alphabet to visually select those with the most high frequency letters. Finally, if necessary, the probability data can be added only for the selected rows.

g. Only rarely will the correct rows consist entirely of those with the highest totals. Normally, you will have to try different combinations of the high probability rows until you find the correct match. The best place to start is with those rows that stand out the most from others in the same alphabet groups. In the illustrated problem shown below, alphabets four and five provide the most likely starting point. In each case, the sum of the log weights for one row are well above any others. These are listed below, superimposed above each other with room for the other three alphabets to be added.

1:

2:

3:

4: **MRELTNEARHTT 97**

5: **YENESTIVETN 88**

h. As the rows are superimposed, the plaintext will appear vertically. The next step is to see which high probability rows from other alphabets will fit well with the starting pair. Trying both of the two highest probability rows for alphabet three produces the next two possibilities.

1:				
2:				
3:	AOGHDAAAECOD	90	ESKLHEEEIGSH	88
4:	MRELTNEARHTT	97	MRELTNEARHTT	97
5:	YENESTIVETN	88	YENESTIVETN	88

i. Reading the plaintext vertically, the grouping on the right is better than the one on the left. The DTS sequence in the left grouping is unlikely, and all the letter combinations on the right are acceptable. Furthermore, the EMY combination at the beginning of the right grouping suggests *ENEMY*. The letter sequences for the first two alphabets which begin with E and N respectively are both high probability sequences. The complete solution is shown below.

1:	EHTHIEHNYFLI	91
2:	NAAIGVRHFIAG	84
3:	ESKLHEEEIGSH	88
4:	MRELTNEARHTT	97
5:	YENESTIVETN	88

"ENEMY HAS RETAKEN HILL EIGHT SEVEN THREE IN HEAVY FIREFIGHT LAST NIGHT"

Section II

Systems Using Mixed Alphabets With Known Sequences

9-5. Approaches to Solution

When mixed sequences are used in periodic systems, a variety of different techniques can be used to solve them. When the plain and cipher sequences are known, the same techniques used with standard alphabets can be used, adapted to the known sequences. When one or both of the sequences are unknown, new techniques must be used. Each situation is a little different. The major paragraphs of this section deal with each situation: both sequences are known, the ciphertext sequence is known, or the plaintext sequence is known. Techniques for solving periodics when neither sequence is known are covered in the next section.

9-6. Solving Periodics With Known Mixed Sequences

Exactly the same techniques that were used with standard alphabets can be used with any known mixed sequences.

a. Successful assumption of plaintext allows you to directly reconstruct the cipher alphabets, as before.

b. The generatrix method works, making sure that a trial decryption is first performed with the sequences set at any alignment. All possible letter combinations are then generated by completing the plain component sequence, as before. The key points to remember are to perform the trial decryption and to use the plain component as the generatrix sequence, not a standard sequence.

c. Frequency matching also works, but there are some differences in its application. Frequency counts must be arranged in the cipher sequence order, not in standard order. The pattern that the frequency counts are matched to must be adjusted to the order of the known plain component. Rearrange the patterns of peaks and troughs to fit the plain component. For example, shown below is the pattern for a standard plain sequence and the pattern that results if a keyword mixed sequence based on POLYALPHABETIC is used as the plain component.

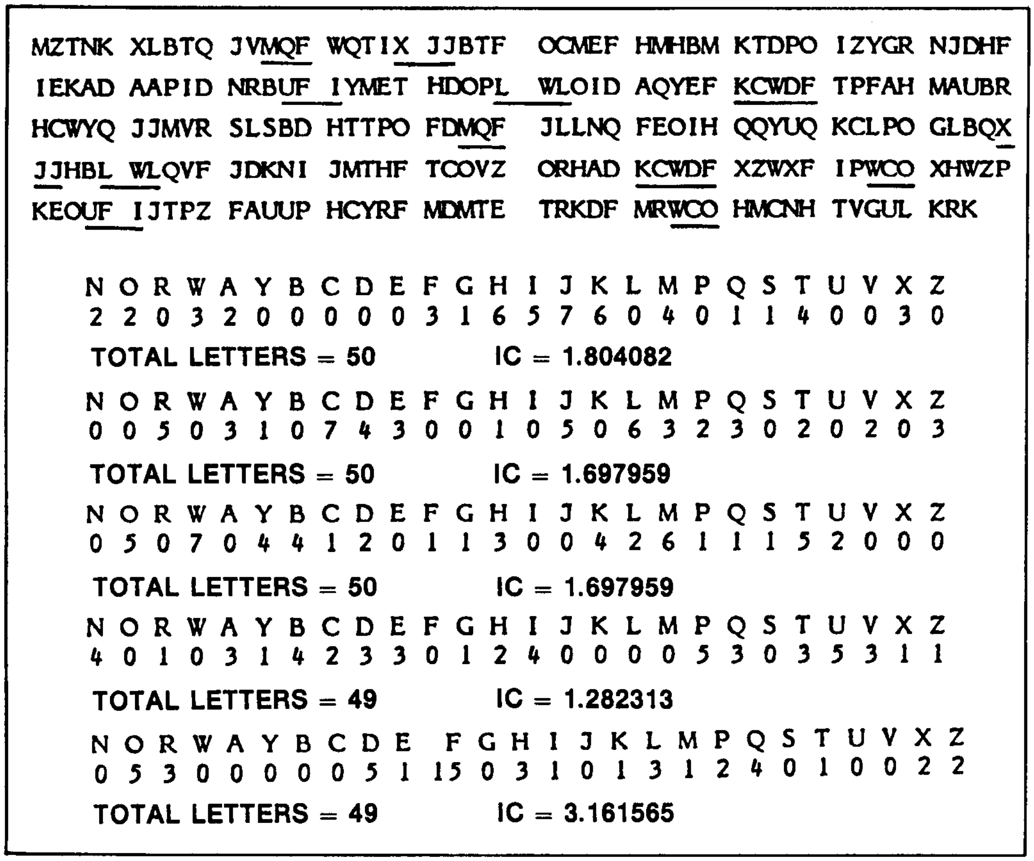
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	1	3	4	13	4	2	3	7	-	-	4	3	8	8	3	-	8	6	9	3	1	2	-	2	-

P	O	L	Y	A	H	B	E	T	I	C	D	F	G	J	K	M	N	Q	R	S	U	V	W	X	Z
3	8	4	2	7	3	1	13	9	7	3	4	4	2	-	-	3	8	-	8	6	3	1	2	-	-

The new pattern resulting from the mixed plaintext sequence is just as easy to match frequency counts to as the more familiar standard pattern. If it should prove difficult to match by eye alone, there is also a statistical test, called the chi test, which can be used to aid the matching process. Paragraph 9-7 demonstrates the use of the chi test.

9-7. Solving Periodics With Known Cipher Sequences

The technique of frequency matching can be used any time the cipher sequence is known, whether or not the plain sequence is also known. When the plain sequence is known, the frequency patterns of the cipher sequences are best matched to the expected plain pattern as explained in paragraph 9-6. When the plain sequence is unknown, the frequency patterns of the cipher sequences can be matched to each other. In either case, the key is that the known cipher sequence allows the frequency count to be arranged in the order of the original cipher sequence. The following problem demonstrates frequency matching with a known cipher component sequence. The cipher component sequence in the problem in Figure 9-3 is a keyword mixed sequence based on NORWAY.



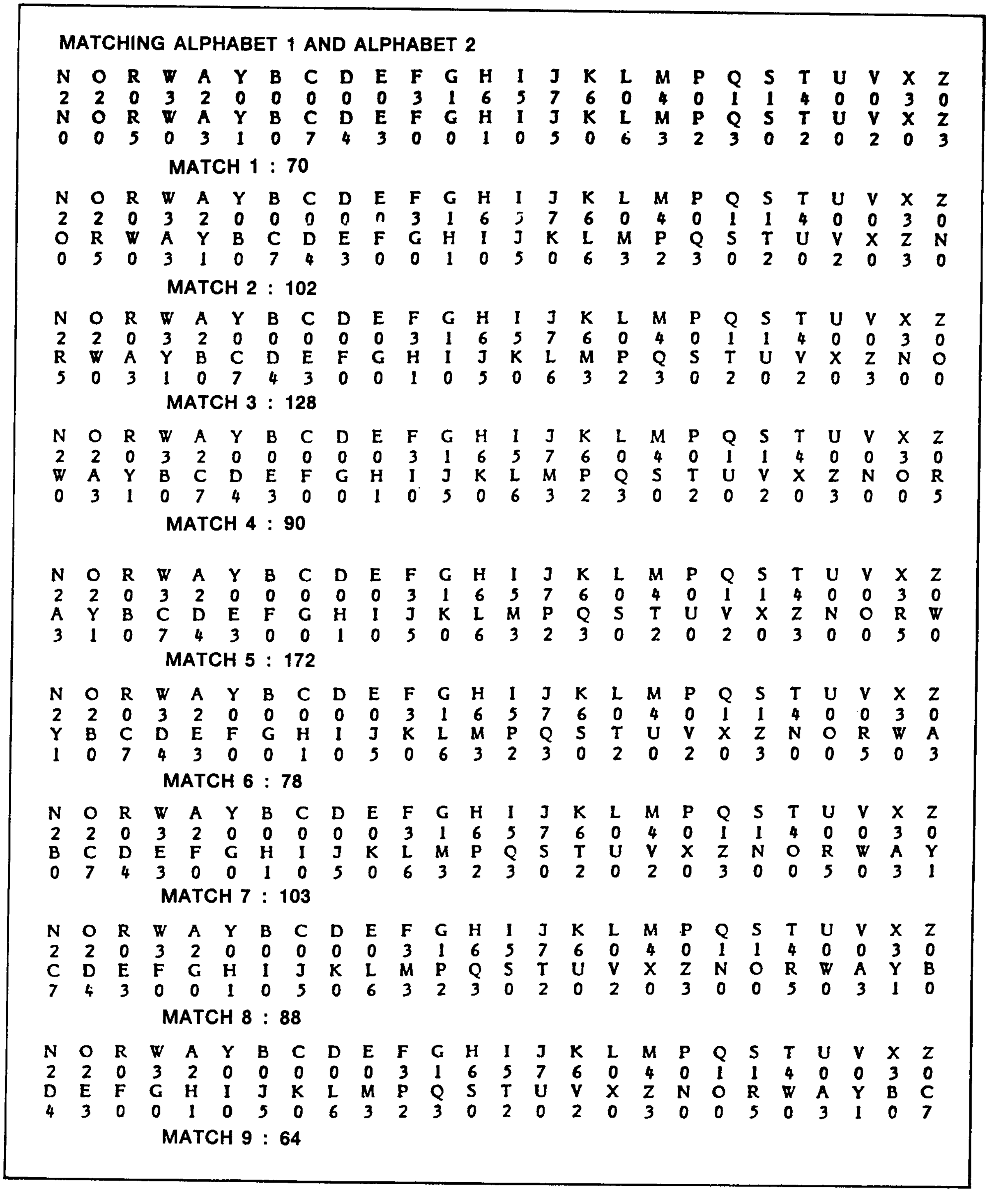
```
MZTNK XLBTQ JVMQF WQTIX JJBTF  OCMEF HMHBM KTDPO IZYGR NJDHF
IEKAD AAPID NRBUF IYMET HDOPL  WLOID AQYEF KCWDF TPFAH MAUBR
HCWYQ JJMVR SLSBD HTTPO FDMQF  JLLNQ FEOIH QQYUQ KCLPO GLBQX
JJHBL WLQVF JDKNI JMTHF TCOVZ  ORHAD KCWDF XZWXF IPWCO XHWZP
KEOUF IJTPZ FAUUP HCYRF MDMTE  TRKDF MRWCO HMCNH TVGUL KRK

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
TOTAL LETTERS = 50          IC = 1.804082
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
0 0 5 0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3
TOTAL LETTERS = 50          IC = 1.697959
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
0 5 0 7 0 4 4 1 2 0 1 1 3 0 0 4 2 6 1 1 1 5 2 0 0 0
TOTAL LETTERS = 50          IC = 1.697959
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
4 0 1 0 3 1 4 2 3 3 0 1 2 4 0 0 0 0 5 3 0 3 5 3 1 1
TOTAL LETTERS = 49          IC = 1.282313
N O R W A Y B C D E  F G H I J K L M P Q S T U V X Z
0 5 3 0 0 0 0 0 5 1 15 0 3 1 0 1 3 1 2 4 0 1 0 0 2 2
TOTAL LETTERS = 49          IC = 3.161565
```

Figure 9-3. Known cipher components.

a. Examination of the frequency patterns in Figure 9-3 shows that they do not match the usual standard sequence-pattern. This means that the plain component sequence was not a standard sequence.

b. If the cipher sequences can be correctly matched against each other, the cryptogram can then be reduced to monoalphabetic terms and solved easily.

c. Figure 9-4 is a portion of a computer listing that matches the frequency count of the cipher letters of the first alphabet with the frequency count of second alphabet letters at every possible alignment. The alignments are evaluated by the chi test. In the chi test, each pair of frequencies for an alignment is multiplied. The products of all the pairs are totaled to produce the chi value for that alignment. Figure 9-5 shows the computation carried out for the first alignment. The chi test is also called the cross-product test.



```
MATCHING ALPHABET 1 AND ALPHABET 2
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
0 0 5 0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3
         MATCH 1 : 70
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
O R W A Y B C D E F G H I J K L M P Q S T U V X Z N
0 5 0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0
         MATCH 2 : 102
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
R W A Y B C D E F G H I J K L M P Q S T U V X Z N O
5 0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0
         MATCH 3 : 128
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
W A Y B C D E F G H I J K L M P Q S T U V X Z N O R
0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5
         MATCH 4 : 90

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
A Y B C D E F G H I J K L M P Q S T U V X Z N O R W
3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5 0
         MATCH 5 : 172
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
Y B C D E F G H I J K L M P Q S T U V X Z N O R W A
1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5 0 3
         MATCH 6 : 78
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
B C D E F G H I J K L M P Q S T U V X Z N O R W A Y
0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5 0 3 1
         MATCH 7 : 103
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
C D E F G H I J K L M P Q S T U V X Z N O R W A Y B
7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5 0 3 1 0
         MATCH 8 : 88
N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
D E F G H I J K L M P Q S T U V X Z N O R W A Y B C
4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3 0 0 5 0 3 1 0 7
         MATCH 9 : 64
```

Figure 9-4. Chi test computer extract.

```
N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
0  0  5  0  3  1  0  7  4  3  0  0  1  0  5  0  6  3  2  3  0  2  0  2  0  3

0 +0 +0 +0 +6 +0 +0 +0 +0 +0 +0 +0 +6 +0+35 +0 +0+12 +0 +3 +0 +8 +0 +0 +0 +0
```

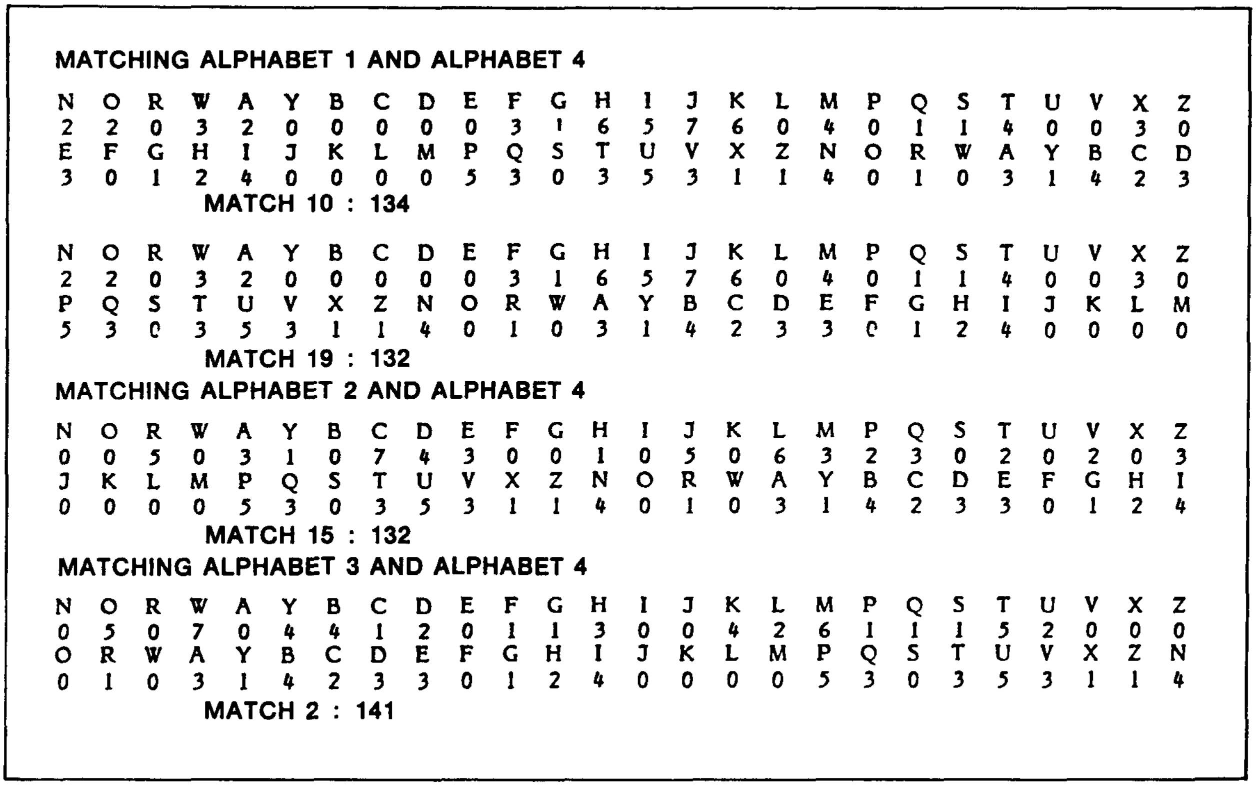
Figure 9-5. Computation of chi value.

d. Figure 9-6 shows the highest chi values for each match of the first alphabet with the other four alphabets. For all matches except the fourth alphabet, the chi values were clearly the highest. Two matches are shown for the fourth alphabet, because the difference between the two values is not significant. Either match could be the correct one.

```
MATCHING ALPHABET 1 AND ALPHABET 2

N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z  N  O  R  W
3  1  0  7  4  3  0  0  1  0  5  0  6  3  2  3  0  2  0  2  0  3  0  0  5  0
         MATCH 5 : 172
MATCHING ALPHABET 1 AND ALPHABET 3
N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
M  P  Q  S  T  U  V  X  Z  N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L
6  1  1  1  5  2  0  0  0  0  5  0  7  0  4  4  1  2  0  1  1  3  0  0  4  2
         MATCH 18 : 170
MATCHING ALPHABET 1 AND ALPHABET 4
N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z  N  O  R  W  A  Y  B  C  D
3  0  1  2  4  0  0  0  0  5  3  0  3  5  3  1  1  4  0  1  0  3  1  4  2  3
         MATCH 10 : 134

N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
P  Q  S  T  U  V  X  Z  N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M
5  3  0  3  5  3  1  1  4  0  1  0  3  1  4  2  3  3  0  1  2  4  0  0  0  0
         MATCH 19 : 132
MATCHING ALPHABET 1 AND ALPHABET 5
N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V  X  Z
2  2  0  3  2  0  0  0  0  0  3  1  6  5  7  6  0  4  0  1  1  4  0  0  3  0
X  Z  N  O  R  W  A  Y  B  C  D  E  F  G  H  I  J  K  L  M  P  Q  S  T  U  V
2  2  0  5  3  0  0  0  0  0  5  1  15 0  3  1  0  1  3  1  2  4  0  1  0  0
         MATCH 25 : 185
```

Figure 9-6. Best matches.

e. To resolve which of the two matches with the fourth alphabet is correct, the highest chi values for matches between the second and fourth and the third and fourth alphabets have also been determined. These are shown in Figure 9-7.



```
MATCHING ALPHABET 1 AND ALPHABET 4

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
E F G H I J K L M P Q S T U V X Z N O R W A Y B C D
3 0 1 2 4 0 0 0 0 5 3 0 3 5 3 1 1 4 0 1 0 3 1 4 2 3
          MATCH 10 : 134

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
2 2 0 3 2 0 0 0 0 0 3 1 6 5 7 6 0 4 0 1 1 4 0 0 3 0
P Q S T U V X Z N O R W A Y B C D E F G H I J K L M
5 3 0 3 5 3 1 1 4 0 1 0 3 1 4 2 3 3 0 1 2 4 0 0 0 0
          MATCH 19 : 132
MATCHING ALPHABET 2 AND ALPHABET 4

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
0 0 5 0 3 1 0 7 4 3 0 0 1 0 5 0 6 3 2 3 0 2 0 2 0 3
J K L M P Q S T U V X Z N O R W A Y B C D E F G H I
0 0 0 0 5 3 0 3 5 3 1 1 4 0 1 0 3 1 4 2 3 3 0 1 2 4
          MATCH 15 : 132
MATCHING ALPHABET 3 AND ALPHABET 4

N O R W A Y B C D E F G H I J K L M P Q S T U V X Z
0 5 0 7 0 4 4 1 2 0 1 1 3 0 0 4 2 6 1 1 1 5 2 0 0 0
O R W A Y B C D E F G H I J K L M P Q S T U V X Z N
0 1 0 3 1 4 2 3 3 0 1 2 4 0 0 0 0 5 3 0 3 5 3 1 1 4
          MATCH 2 : 141
```

Figure 9-7. Matches with the fourth alphabet.

f. The matches of alphabet four with alphabets two and three clarify which of the matches with the first alphabet was correct. This becomes apparent when we set up the other four alphabets.

1: N O R W A Y B C D E F G H I J K L M P Q S T U V X Z

2: A Y B C D E F G H I J K L M P Q S T U V X Z N O R W

3: M P Q S T U V X Z N O R W A Y B C D E F G H I J K L

4:

5: X Z N O R W A Y B C D E F G H I J K L M P Q S T U V

g. The match of N of the first alphabet with P of the fourth alphabetic correct. The second alphabet and third alphabet matches confirm this.

h. The next step in the solution is to reduce the cryptogram to monoalphabetic terms using the matches just determined. An A through Z sequence is arbitrarily used for the plain component, and the message is decrypted just as if it were the original.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z	N	O	R	W
M	P	Q	S	T	U	V	X	Z	N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L
P	Q	S	T	U	V	X	Z	N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M
X	Z	N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V

```
rveir ympdv otabm dpeva okpdm   bdarm mnvot prrad nvote akrum
MZTNK XLBTQ JVMQF WQTIX JJBTF   OCMEF HMHBM KTDPO IZYGR NJDHF

nfymk eabvk aypem nbarx mekas   dmkvk eporm pdmqm votmo rafoe
IEKAD AAPID NRBUF IYMET HDOPL   WLOID AQYEF KCWDF TPFAH MAUBR

mdmnv okafe umdok mread keabm   omziv kfkvo tpoev pdzad lmpba
HCWYQ JJMVR SLSBD HTTPO FDMQF   JLLNQ FEOIH QQYUQ KCLPO GLBQX

okvos dmcfm oeyip oneum vdkfb   byvmk pdmqm yvmgm nompd yimhu
JJHBL WLQVF JDKNI JMTHF TCOVZ   ORHAD KCWDF XZWXF IPWCO XHWZP

pfkem nkeab kafeu mdokm readl   vyyqm rympd mnqio vtues pyy
KEOUF IJTPZ FAUUP HCYRF MDMTE   TRKDF MRWCO HMCNH TVGUL KRK
```

i. Reduced to monoalphabetic terms, many more repeats in the text that were suppressed by the multiple alphabets now appear. The solution is completed the same as any other monoalphabetic system.

9-8. Solving Periodics With Known Plaintext Sequences by Direct Symmetry

When the plaintext sequence is known, but not the ciphertext sequence, a solution technique known as direct symmetry is possible. Direct symmetry depends on the probable word method for the initial entry into the cryptogram. It makes use of the fact that the columns can be reconstructed in their original order as recoveries are made. Consider the next example, which uses a standard plaintext sequence.

```
MBNFQ ZLHQV ERNMS EXWFJ MBUFU   LWZIA LBSMK CFXKN WSNZW TREQA
XWHRN ACTKP EVBZJ PREZB TCZWH   TKTDN LBWAU PRZOQ KFEIW KBSRD
EVRWA MBIHO MBNFQ ZLHQV ERNMB   IVZIN MVCHR MXXRD EXDFU NLWGV
ITUCG JBUFW ALWML KFSLL IFQRX   YVIHE JKAHO
```

a. The period is five. The 14 letter repeat is probably *RECONNAISSANCE.*

```
recon naiss ance  a  o  re o          e e          c    n s
MBNFQ ZLHQV ERNMS EXWFJ MBUFU  LWZIA LBSMK CFXKN WSNZW TREQA

  i         a      n                  e     n           e
XWHRN ACTKP EVBZJ PREZB TCZWH  TKTDN LBWAU PRZOQ KFEIW KBSRD

a     re    recon naiss ance         r     r     a  o   a
EVRWA MBIHO MBNFQ ZLHQV ERNMB  IVZIN MVCHR MXXRD EXDFU NLWGV

       e o   a e
ITUCG JBUFW ALWML KFSLL IFQRX  YVIHE JKAHO
```

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
E													Z				M								
L				B									R												
		N						H																	
				M										F				Q							
													Q					V							

b. With recovered letters filled in, we can see that the beginning phrase is the stereotype, *RECONNAISSANCE PATROL REPORTS.*

```
recon naiss ancep atrol repor  ts    te e          c    n s
MBNFQ ZLHQV ERNMS EXWFJ MBUFU  LWZIA LBSMK CFXKN WSNZW TREQA

 si         a   l  n                 ter r  n  n        e
XWHRN ACTKP EVBZJ PREZB TCZWH  TKTDN LBWAU PRZOQ KFEIW KBSRD

a     re    recon naiss ance         r     rt    at or  ar s
EVRWA MBIHO MBNFQ ZLHQV ERNMB  IVZIN MVCHR MXXRD EXDFU NLWGV

  p    epo   are
ITUCG JBUFW ALWML KFSLL IFQRX  YVIHE JKAHO
```

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
E													Z				M		L						
L				B									R					W	X						
		N						H							U		W								
				M										F				Q							
											J		Q		S		U	V							

c. With a known plain component, the columns are in their original order. This means that the partially reconstructed cipher sequences are also in the right order. Each cipher sequence is the same sequence, and whatever one row reveals about the spacing of letters can be transferred to other rows as well. For example, in the second row, X follows immediately after W. X can then be placed after W in row three. Similarly, all common letters can be placed by carefully counting the intervals and placing the same letters at the same intervals in each row. Here is what the matrix looks like after all such values are placed.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
E	F	H	J		Q	R	S		U	V	W	X	Z				M		L			N	B		
L			N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M	
		N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M		L
Z				M		L			N	B			E	F	H	J		Q	R	S		U	V	W	X
	L			N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M

d. Filling all the new values into the text reveals many more possibilities. Completion of the solution is routine from this point.

```
recon naiss ancep atrol repor   tst   tene    is e locat  ngs
MBNFQ ZLHQV ERNMS EXWFJ MBUFU  LWZIA LBSMK CFXKN WSNZW TREQA

msite       ardal  ngaf   tyk       e ter r  nt n  ig t  ent
XWHRN ACTKP EVBZJ PREZB TCZWH  TKTDN LBWAU PRZOQ KFEIW KBSRD

army   re p recon naiss ancef   rt e rr po rtst  at or war s
EVRWA MBIHO MBNFQ ZLHQV ERNMB  IVZIN MVCHR MXXRD EXDFU NLWGV

  p   depot  areb  ingb  iltu   r pi  d  p
ITUCG JBUFW ALWML KFSLL IFQRX  YVIHE JKAHO
```

e. The direct symmetry technique can also be used as an alternate method when the cipher sequence is the known sequence. The matrix can be inverted, placing the cipher sequence on the top of the matrix and the plaintext equivalents inside in separate rows for each alphabet. Each row will be the plaintext sequence in the correct order. Horizontal intervals recovered in one row can then be duplicated in each sequence just as was demonstrated above for cipher sequence recovery. Unlike the technique of frequency matching, it depends on successful plaintext assumptions, however. It is not as powerful a method of solution, but if plaintext can be readily identified, it may be the quickest way to solve a cryptogram.

Section III

Solving Periodics With Unknown Sequences

9-9. Solving Periodics by Indirect Symmetry

When neither the plaintext nor the ciphertext sequence is known, the matrix cannot be initially recovered with sequences in the correct order. Frequency matching cannot be used, either. However, some of the interval relationships are preserved even when the columns are not placed in the correct order, and these interval relationships can be exploited to aid in matrix recovery.

a. To illustrate how interval relationships are preserved, consider the following two matrices. The first is the matrix in its original form. The second is the same matrix, rearranged with the plain component in A through Z order. This is the form in which you will normally recover a matrix with unknown sequences until enough is known to rearrange the columns in the correct order.

c	l	a	r	i	n	e	t	b	d	f	g	h	j	k	m	o	p	q	s	u	v	w	x	y	z
B	C	D	F	G	I	J	K	L	M	Q	R	T	U	V	W	Y	Z	S	A	X	O	P	H	N	E
M	Q	R	T	U	V	W	Y	Z	S	A	X	O	P	H	N	E	B	C	D	F	G	I	J	K	L
R	T	U	V	W	Y	Z	S	A	X	O	P	H	N	E	B	C	D	F	G	I	J	K	L	M	Q
K	L	M	Q	R	T	U	V	W	Y	Z	S	A	X	O	P	H	N	E	B	C	D	F	G	I	J

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	L	B	M	J	Q	R	T	G	U	V	C	W	I	Y	Z	S	F	A	K	X	O	P	H	N	E
R	Z	M	S	W	A	X	O	U	P	H	Q	N	V	E	B	C	T	D	Y	F	G	I	J	K	L
U	A	R	X	Z	O	P	H	W	N	E	T	B	Y	C	D	F	V	G	S	I	J	K	L	M	Q
M	W	K	Y	U	Z	S	A	R	X	O	L	P	T	H	N	E	Q	B	V	C	D	F	G	I	J

b. The key principle to understand when working with ananalyst's matrix, like the second one above, is that every pair of columns and every pair of rows represents an interval in the original matrix. To illustrate this, look at the plaintext A column and the plaintext G column in the bottom matrix. The letters D and R appear in the first cipher sequence. If you count the distance between the D and R in the original (top) matrix, you see that the interval is nine. Similarly, the interval for the other pairs in the two columns, R and X, U and P, and M and S, are also nine. For any two columns that you compare, the horizontal interval between the letters in each alphabet will be the same. The interval will not always be nine, of course. It depends on which two columns you are comparing. The point is that between any pairs in the same row in the same two columns, the interval will be the same.

c. Next compare the letters in the first cipher sequence and the second in the bottom matrix. In the first column, the letters D and R appear, which we already noted are nine letters apart horizontally in the original matrix. The letters R and X appear in another column in the first and second sequences, as do U and P, and M and S. The first and second cipher sequences are an interval of nine apart. Whichever pair of letters you look at in the first and second cipher sequences, they are nine apart in the original cipher sequence. Each pair of cipher sequences represents a different interval. For example, the interval between the first and third cipher sequence is eleven. The interval between the first and fourth is seven. The interval between the second and third is two, and so on.

d. There are a number of ways in which we can use an understanding of these interval relationships to help solve a polyalphabetic cryptogram. The use of interval relationships where sequences are unknown and columns are out of order is called indirect symmetry. This contrasts with the earlier situation with known sequences and columns in the correct order, where we used direct symmetry to aid in the solution.

e. To put indirect symmetry to use, consider the following example. Initial recoveries in a polyalphabetic system have produced the following information.

a	b	c	d	e	f	g	h	i	j	...
R	.	.	.	T	.	.	.	M	.	...
M	.	.	.	F	.	.	.	.	.	...
T	.	.	.	.	.	M	.	.	.	...

f. In comparing the plaintext A and E columns, we see that the letters R and T and the letters M and F are the same interval apart. We do not know what the interval is, but we know it is the same in each case.

g. The same interval appears when we compare the first and third cipher sequences, where R and T appear in the first column. Since we know the interval will be the same for any pair of letters between the first and third sequences, and we know M and F have the same interval as R and T, we can add the letter F in the plaintext I column in the third sequence under the letter M.

h. Any time we can establish an interval relationship for two pairs in a rectangular pattern as above, and can find three of the four letters, also in a rectangular pattern elsewhere, we can add the fourth letter to complete the pattern. The pairs must be read in the same direction in each case. Notice that we cannot add F in the plaintext G column in the first sequence. The interval from the first to the third sequence is not the same as the interval from the third to the first.

i. Matching pairs are usually found by reading horizontally in one case, and vertically with one letter in common in the second case, as in the above example. Matching relationships may be found anywhere in matrix, however, and are not restricted to cases with one letter in common. You can find most such matching pairs by examining every column in which you have recovered at least three letters. For each letter in the column, look for a match with letters on the same row that are the same as one of the other letters in the column. When you find such letters, check for every possible complete rectangular relationship, and see if you can find the same relationship with one letter missing elsewhere. Often the addition of one or two letters is all you need to recognize more plaintext in the cryptogram and complete a solution.

j. If you have reason to believe that the plaintext sequence is the same as the cipher sequences, you can use the plaintext sequence in establishing interval relationships, too. All the techniques that apply to the ciphertext sequences apply to the plaintext sequence as well, when it is the same sequence.

9-10. Extended Application of Indirect Symmetry

Indirect symmetry can be used in other ways, too. For example, when enough letters have been recovered, you can list all the pairs of letters between each pair of sequences, and develop partial decimated chains of letters for each, as was explained in paragraph 4-8 with monoalphabetic substitution. These partial chains from different alphabet combinations can then be combined together geometrically to recover the original sequence. This technique is illustrated in the following indirect symmetry problem.

```
refer encey ourme ssage numbe  reigh teigh tthre esixs top
SMHPT ZZOPH KRION FJTYN WRSFN  SMKYZ JMKYZ JNPVN ZJKRX JOFSB

JMILM JMPPM VEVST JMIZK CTWFN  SMWEY LNBKG KKRET VHMSG ZJIEL

         si xthre eeigh tfour  fours evens top
ZOGSJ RMBZV ANPVN ZMKYZ JCRCT  EOVVX ZWBLX JOFOA TMEXB PUBGA

          o nesev enzer ozero  hours
YBWPG ZYXJA WMNPF ZZJPT KFBVA  IOVVX HOSOM KZBZV AZRIN YUBV
```

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
				Z	E		I						W	K			S	F	J				A		
				M	C								Z	O				J	N	R	W				F
T		O		B	H		P	K				S		R	F		I	N		V					J
	F			P		Y						O	L				V	Z		C			R		
				N			Z	V						A			T	X			F			H	

a. Through recognition of the stereotyped beginnings and the use of many numbers, the text shown has been recovered, and the recovered values filled into the matrix.

More values can be filled into the text, but we will first concentrate on the application of indirect symmetry.

b. To recover additional values through indirect symmetry, examine each column with more than two recovered letters in it. Beginning with the fifth column, take each letter in turn, and scan the same row as the selected letter for letters that are the same as those in the column. The first letter, Z, has no letters in common in its row with the letters M, B, P, and N.

c. For the second letter, M, the common letter Z does appear in its row. Having found a common letter, examine each rectangular relationship that exists between the two columns. We first see that Z and W have the same interval as M and Z. Links with this common letter will not add any more values, however.

d. The next rectangular relationship shows that P and L have the same interval as M and Z. Reading M and Z vertically, we look for P or L on the same rows as the M and Z to complete the relationship. We find neither P in the second row nor L in the first row. If either occurred, we could fill in the other. The letters can be written in a column off to the side for future use.

e. Having observed all relationships from the column with the common letter Z, we look for another column with a common letter on the M row. B and P do not occur except in our added column. The letter N does occur in the second row, however. Examining relationships in the N column, we see that Z and J have the same interval as M and N reading horizontally. With that established, we read M and N vertically and look for Z in the second row or J in the last row. This time we find Z in the second row. We can add J in the last row in the same column with Z to complete the rectangular relationship.

f. Continuing this process, all the letters shown in bold print can be added to the matrix without making any new plaintext recoveries.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
		H		Z	E		I	C					W	K			S	F	J	O	T		A		
		K		M	C		L	H				A	Z	O				J	N	R	W		S		F
T	X	O		B	H		P	K				S	M	R	F		I	N		V	Z				J
S	F			P		Y						O	L	E	T		V	Z	M	C	I		R		W
				N	R		Z	V					J	A			T	X		S	F			H	

g. It would be easy at this point to return to plaintext recovery to complete the solution, but another technique can be used to recover the original cipher sequences and rebuild the matrix. This technique involves listing all links that result by matching each cipher sequence with every other cipher sequence. Sequence 1 is matched with sequences 2, 3, 4, and 5, in turn. Then sequence 2 is matched with 3, 4, and 5; sequence 3 is matched with 4 and 5; and sequence 4 is matched with 5. If the plaintext sequence were the same as the ciphertext sequence, it would only have been necessary to match the plaintext with each cipher sequence to get all combinations. When all links have been plotted and combined into partial chains wherever possible, the results are shown below.

```
1-2: ECHKOR TWZM FJN IL AS
1-3: EHOV TZB SIP WM KR FN
1-4: FZP WL KE SV JM OC TI AR
1-5: OSTFX IZN ER WJ KA CV
2-3: CHKORV WZMB FJN LP AS
2-4: AOE NMP SRC FWI JZL
2-5: LZJX CRS MN OA WF
3-4: XFTSO NZIVC BP ML RE JW
3-5: HRA BNX PZF KVS MJ IT
4-5: PN LJ EA VT CS IF ZX
```

h. Each set of partial chains represents a decimation of the original sequence. Sometimes, you will be fortunate at this point to find that one of the partial chains directly represents the original sequence (decimation one). When this happens, the original sequence is the obvious starting point. It does not occur in this example, so the best technique is usually to select a set with one of the longer chains as a starting point and relate all other sequence combinations to it. Notice that the chains produced by sequences 1-2 and by sequences 2-3 are obviously produced by the same interval, since many of the partial chains are identical. They make a good starting point for this problem. Begin by listing each chain fragment on paper, horizontally. Write the separate chains in different rows so they will not run into each other.

```
E C H K O R V
  T W Z M B
    F J N
    I L P
     A S
```

i. The next step is to relate other chains to the existing plot. By examining the intervals or patterns that letters from other chains have in relation to the starting chains, they can be added by following the same rule. For example, the 1-3 combination can be added by observing that it will fit the starting chains by skipping every other letter. This will also enable linking the fifth fragment, AS, with the fourth. After adding all the 1-3 chains, the plot looks like this example.

E C H K O R V
T W Z M B
F J N
E C H
A S . I L P

j. Next, search for another combination that can be added to the plot. The 3-4 combination links by counting backwards every fifth letter, as shown by the V and C of the NZIVC chain. This ties all the chain fragments together into one longer chain. When all combinations are added, each by their own rule, it results in almost complete recovery.

E C H K O R V . A S . I L P T W Z M B F J N . . X .

k. This technique is known as linear chaining. Sometimes you will be unable to combine the fragments into one long chain. When all intervals are even, you will always end with two separate 13-letter chains, which may be combined by trial and error or by figuring out the structure of the original matrix. A second technique, called geometric chaining, which could have been applied here also, is explained in paragraph 9-11.

l. Continuing, the chain above must be a decimation of the original sequence. Since V, W, and X are spaced consistently nine apart, trying a decimation of 9 produces the next sequence.

V W X . Z . A M E S B C . F H I J . L N O P . R T .

m. With G missing from alphabetical progression, the sequence is keyword mixed, based on GAMES. We can now return to the polyalphabetic matrix and rearrange the columns using the GAMES sequence on each cipher row.

o	a	.	u	.	b	.	v	y	.	n	.	m	e	.	x	p	f	r	z	i	g	s	c	h	t
K	L	N	O	P	Q	R	T	U	V	W	X	Y	Z	G	A	M	E	S	B	C	D	F	H	I	J
O	P	Q	R	T	U	V	W	X	Y	Z	G	A	M	E	S	B	C	D	F	H	I	J	K	L	N
R	T	U	V	W	X	Y	Z	G	A	M	E	S	B	C	D	F	H	I	J	K	L	N	O	P	Q
E	S	B	C	D	F	H	I	J	K	L	N	O	P	Q	R	T	U	V	W	X	Y	Z	G	A	M
A	M	E	S	B	C	D	F	H	I	J	K	L	N	O	P	Q	R	T	U	V	W	X	Y	Z	G

n. The unused letters can be determined by returning to the plaintext and deciphering the rest of the message. The plaintext sequence turns out to be a simple transposition mixed sequence based on OLYMPIC. The repeating key is KOREA.

o. The approach shown to solving this problem is not necessarily the way in which you would solve it in actual practice. It would probably be more effective to return to the plaintext earlier than was done in this example. This approach was selected to show the variety of indirect symmetry techniques that can be used, not necessarily because it would yield the quickest solution.

9-11. Solution of Isologs

Whenever isologs are encountered between periodic messages with different period lengths, it is possible to recover the original cipher sequences without any initial plaintext recovery. The cryptograms can then be reduced to monoalphabetic terms and quickly solved. Two different techniques may be used, depending on whether the same alphabets or different alphabets are used in the isologs.

a. When isologous cryptograms use the same alphabets with different repeating keys, the cipher sequences can be recovered by the indirect symmetry process. Take the following two messages, for example.

Message 1:

```
AOPDY JBFKW ATILB XCTKZ KIKVN  SHUAJ COWLA PDBRU KRXAT WALBZ
ZVYZZ YRNCI FPPOJ OBYJQ SESQK  SPGUK XIKVW AVUCW MYTXY ZCYZB
PHBJE SCWXC TKZKV PKN
                              (period 3)
```

Message 2:

```
DCFHC SBOHH BOENY GMGKB HQOQF  FIXHS CVURB KKWUX UEXEQ HBFHP
SYCCZ NZSFZ MDFST WBNFB VNXEB  VYDUS VQOQR TMXMI MNQJR VJOSE
YQBQC CFSAX KODTV WHS
                              (period 4)
```

(1) To solve the isologs, the two messages are first superimposed with the alphabets numbered for each.

```
1: AOPDY JBFKW ATILB XCTKZ KIKVN   SHUAJ COWLA PDBRU KRXAT WALBZ
   12312 31231 23123 12312 31231   23123 12312 31231 23123 12312
2: DCFHC SBOHH BOENY GMGKB HQOQF   FIXHS CVURB KKWUX UEXEQ HBFHP
   12341 23412 34123 41234 12341   23412 34123 41234 12341 23412

1: ZVYZZ YRNCI FPPOJ OBYJQ SESQK   SPGUK XIKVW AVUCW MYTXY ZCYZB
   31231 23123 12312 31231 23123   12312 31231 23123 12312 31231
2: SYCCZ NZSFZ MDFST WBNFB VNXEB   VYDUS VQOQR TMXMI MNQJR VJOSE
   34123 41234 12341 23412 34123   41234 12341 23412 34123 41234

1: PHBJE SCWXC TKZKV PKN
   23123 12312 31231 231
2: YQBQC CFSAX KODTV WHS
   12341 23412 34123 412
```

(2) With periods of 3 and 4, there are 12 different ways in which the alphabets of the first are matched to the alphabets of the second. These begin with the first alphabet of message 1 matched with the first alphabet of message 2 and continue through alphabet 3 matched with alphabet 4. After these 12 matches, the cycle of matches starts over again. For other periods, the number of different alphabet matches is the least common multiple of the two period lengths. The least common multiple of 6 and 4 is 12. The least common multiple of 6 and 9 is 18. For periods of 8 and 9, 72 different alphabet matches are required.

(3) Analysis continues by plotting the links for each alphabet pair. For example, the first link is A1=D1, the second link is O2=C2, and the third link is P3=F3. The next example shows all links plotted and combined into partial chains.

```
1-1: SXADK IE NFM BH WR CJ
2-2: YOCX LN SF BW ZPD QE AT
3-3: TKBY PF HI RU ZS VM
1-4: KOSVY UXG DH BE
2-1: PYCM AH KU JT ZD
3-2: KTGD OWI JS RE ZC HQ
1-3: BB KK (all links the same)
2-4: FOV ZB AE YN KS JQ PW
3-1: KH WU TQ RZ JF XV EC
1-2: IQB NSC WH LR XJ
2-3: AB KO CF SV YR
3-4: IZVQ TO PK LF EN WS
```

(4) The 1-3 plot shows that the same alphabets were used in both these positions.

(5) The partial chains can be combined into one long chain by a process of geometric chaining. Geometric chaining will often produce results when linear chaining is not effective. Geometric chaining is plotted horizontally and vertically, instead of in one straight line. Relationships between alphabet matches can be discovered more readily with this method.

(6) Geometric chaining begins, as with linear chaining, by selecting one alphabet match to plot horizontally. We can select the 1-1 match for its 5-letter chain as a starting point. Next, select a second alphabet match to intersect it plotted vertically. For our example, we will use the 2-2 match, producing the following initial plot.

			Y					
			O					
			C					
		S	X	A	D	K		

(7) To this initial plot, we add as many other fragments from the 1-1 and 2-2 matches as we can at this time. We can also set up plots separated from these for each one that cannot be linked to it.

												Y											
												O		Z									
												C	J	P									
										L	S	X	A	D	K								
										N	F	M	T										
			B	H																Q			
			W	R															I	E			

(8) The next step is to find another alphabet match that can easily be added to the plot. For example, the 1-2 match proceeds in the diagram along a lower left to upper right diagonal, as shown by the NSC and XJ fragments. All the 1-2 fragments can be added by the same diagonal rule. This ties in the separate plots from above, also.

							Y						
					B	H	O	.	Z				
				Q	W	R	C	J	P				
			I	.	L	S	X	A	D	K			
					N	F	M	T					

(9) Each additional alphabet combination can be added to the plot now. In many cases, you may see different possibilities for rules. For example, the 3-4 match can be seen to proceed by an up 3, left 1 rule, as shown by the TO link. A simpler equivalent is to plot by the upper left to lower right diagonal, as shown by the PK link. The simplest way to describe the 3-3 match is up 1, right 2, as shown by the TK or BY links. This is similar to a knight's move in chess. When all matches are plotted, they produce this diagram.

						T	Y	I	E	L	S	
			V	G	B	H	O	U	Z	N	F	
	A	D	K	Q	W	R	C	J	P	V	G	
	T	Y	I	E	L	S	X	A	D	K	Q	
		O	U	Z	N	F	M	T	Y	I	E	
			J	P	V	G	B	H	O	U		

(10) The rows can easily be extended into one 26-letter chain at this point, but if alphabetic progression can be spotted by any other rule, it can be used instead. For example, starting with the V in the upper left part of the diagram, VWXY appears by a descending knight's move. Continuing from the Y that repeats near the left side, the sequence can be extended further. The complete sequence appears below.

G R A I N B C D E F H J K L M O P Q S T U V W X Y Z

(11) Using the new recovered sequence and the relationships between the alphabets of messages 1 and 2, the matrices for both messages can be set up. Using the first cipher sequence for message 1, all the cipher sequences for message 2 can be lined up with it using the links already plotted. Here is how the message 2 alphabets line up with alphabet one. The first 1-1, 1-2, 1-3, and 1-4 links from the isologs are shown in bold print to demonstrate how they were lined up.

```
C1: G R A I N B C D E F H J K L M O P Q S T U V W X Y Z
C2:
C3: ___________________________________________________
C1: B C D E F H J K L M O P Q S T U V W X Y Z G R A I N
C2: M O P Q S T U V W X Y Z G R A I N B C D E F H J K L
C3: G R A I N B C D E F H J K L M O P Q S T U V W X Y Z
C4: I N B C D E F H J K L M O P Q S T U V W X Y Z G R A
```

(12) Similarly, the alphabets in the first matrix can be completed by plotting the relationships between the second message and the first. The solution then becomes a matter of reducing them to monoalphabetic terms.

(13) In cases where the two periods have a common factor, the sequences can still be recovered, but they cannot be fully aligned. In this case, the chi test can be used to match the sequences by frequencies, if necessary, once the sequences are known.

b. A different technique must be used if different alphabets are used between the isologs, not just different repeating keys. For example, consider the next two messages.

Message 1:

```
AUUJB NFMOI AXCQD LHXPE OCPZD  XMZAN HUGQV OIAZZ POPAA FOZUY
OQEOX BRDHA MVUUO SFBNW XJXWO  XVEZP IPHYM WODOT CMOTU CTUPT
UOYRO SBBMP CMMXA ATYAN
                            (period 3)
```

Message 2:

```
ZCIPY RZXLG ZXSNP CNLNH LQDZU  FXALR SIGIH MQTCA GTNMQ TCZGG
ZYZTG GORIB NDISF YZGUB KGKEZ  IMDJS HLIYN EZKFF XXLOG CYCSG
KTHJL VTINA ORDLW MPDZK
                            (period 4)
```

(1) The sequences are different in the two messages, and they cannot be directly chained together. If you listed the links resulting from the two messages using the previous technique, they would lead nowhere and contradictions would quickly develop. The cipher sequences of each must be kept separate.

(2) The method of recovering the cipher sequences when they are different is to set up periodic matrices one over the other, as shown below. Message 1 and message 2 equivalents are then plotted in the correct sequence for each in the same columns. Initially, this will result in more than 26 columns, but as incomplete columns are combined with each other, the matrices will collapse to the correct width. This method could be used with more than two isologs also, by superimposing as many matrices as there are isologous messages.

```
1: AUUJB NFMOI AXCQD LHXPE OCPZD  XMZAN HUGQV OIAZZ POPAA FOZUY
   12312 31231 23123 12312 31231  23123 12312 31231 23123 12312
2: ZCIPY RZXLG ZXSNP CNLNH LQDZU  FXALR SIGIH MQTCA GTNMQ TCZGG
   12341 23412 34123 41234 12341  23412 34123 41234 12341 23412

1: OQEOX BRDHA MVUUO SFBNW XJXWO  XVEZP IPHYM WODOT CMOTU CTUPT
   31231 23123 12312 31231 23123  12312 31231 23123 12312 31231
2: ZYZTG GORIB NDISF YZGUB KGKEZ  IMDJS HLIYN EZKFF XXLOG CYCSG
   34123 41234 12341 23412 34123  41234 12341 23412 34123 41234

1: UOYRO SBBMP CMMXA ATYAN
   23123 12312 31231 23123
2: KTHJL VTINA ORDLW MPDZK
   12341 23412 34123 41234
```

Message 1:

1	A			J			F			I			C		
2		U			B			M			A			Q	
3			U			N			O			X			D

Message 2:

1	Z				Y				L				S		
2		C				R				G				N	
3			I				Z				Z				P
4				P				X				X			

(3) The first three groups of each message are plotted above. Each time a previously used letter appears in the same sequence, the two columns can be combined. For example, in message 2, the Zs in the third sequence allow those two columns to be combined, and similarly, the Xs in the fourth sequence can be combined. In the next example, the complete messages are plotted and all possible columns are combined.

Message 1:

1	A	X	M	J	T	D	F	P		I		L	C			Y		Q		W	U			Z		S	H
2	E	U	H		B		A	M		Y	W			Q		V					P	O	X		R		
3		B	U		J	N	O	X	I	A		C	M		D	E	S	Y	R		G	Z	T				P

Message 2:

1	Z	K	N		Y	U	L	D	H	Q			S			M			O		G	F	P			V	
2		C			O	R	T	L		G	E		Q	N		D	Y	I		B	A		F				
3	W	G	I		T		Z	N				O	X		P	H					D	C	K	J			S
4	H	I	R	P	G	K	M	X		B		C						Y			S	Z		A	J		

(4) These matrices can easily be completed by direct symmetry, remembering that the sequence in each matrix is different.

Message 1:

1	G	I	L	B	E	R	T	A	C	D	F	H	J	K	M	N	O	P	Q	S	U	V	W	X	Y	Z
2	X	Y	Z	G	I	L	B	E	R	T	A	C	D	F	H	J	K	M	N	O	P	Q	S	U	V	W
3	T	A	C	D	F	H	J	K	M	N	O	P	Q	S	U	V	W	X	Y	Z	G	I	L	B	E	R

Message 2:

1	P	Q	R	T	W	X	Y	Z	S	U	L	I	V	A	N	B	C	D	E	F	G	H	J	K	M	O
2	F	G	H	J	K	M	O	P	Q	R	T	W	X	Y	Z	S	U	L	I	V	A	N	B	C	D	E
3	K	M	O	P	Q	R	T	W	X	Y	Z	S	U	L	I	V	A	N	B	C	D	E	F	G	H	J
4	N	B	C	D	E	F	G	H	J	K	M	O	P	Q	R	T	W	X	Y	Z	S	U	L	I	V	A

(5) Either cryptogram can now be reduced to monoalphabetic terms and solved, as before.

CHAPTER 10

APERIODIC POLYALPHABETIC CIPHERS

10-1. Simple Manual Aperiodic Systems

Chapter 9 showed that periodic polyalphabetic systems are generally more secure than monoalphabetic systems. However, the regular, repeating nature of the keys in periodic systems are a weakness that an analyst can exploit. Using factor analysis or the phi test, the analyst can readily determine how many alphabets there are and which letters are enciphered by which alphabets. Aperiodic polyalphabetic systems eliminate the regular, repeating use of alphabets so the analyst cannot easily tell which letters are enciphered by which alphabets. There area number of ways to use a limited set of alphabets but suppress their regular repetition. The following subparagraphs show the most common types of these, and briefly discuss their weaknesses and approaches to their solution. They are presented to make you aware of the possibility that such techniques can be used, but no detailed explanation of their solution is given.

a. **Word Length Aperiodic.** The simplest type of aperiodic changes alphabets with each word instead of each letter. The analyst cannot tell which letters are encrypted by which alphabet until the text is recovered. However, the major weakness of this system is that when repeats occur, they are likely to be word length, and plaintext word patterns show through as clearly as with monoalphabetics. When alphabets are known, the generatrix method makes the plaintext obvious.

b. **Numerically Keyed Aperiodic.** Another approach, similar to word-length encipherment, is to change alphabets after a number of letters, determined by a numerical key. The numerical key is often based on the repeating key. The key is generated by the same process used with a numerically keyed transposition sequence. The letters in the repeating keyword are numbered alphabetically. Then the key determines how many letters are enciphered consecutively by each alphabet. For example, here is a short message enciphered by a numerically keyed aperiodic based on the keyword BLACK.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
5	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
4	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

2	5	1	3	4	2	5	1	3
en	emyat	t	ack	ingo	na	llfro	n	ts
FO	PXJLE	T	CEM	SXQY	OB	WWQCZ	N	VU

This system, while more complicated than a word-length aperiodic, allows many repeats and patterns to appear. When the alphabets are known, use of the generatrix method also quickly reveals the plaintext.

c. **Interruptor Letter Aperiodic.** Another approach to breaking up the cyclic nature of periodic systems is through the use of an interruptor letter. In interruptor letter systems, the alphabets are used in rotation like a periodic system, but whenever a preselected plaintext (or alternatively, ciphertext) letter is encountered, the rotation is interrupted and encipherment returns to the first alphabet. This is a more secure method than the previous two, but it can have the effect of creating repeats that would not otherwise occur. For example, if a plaintext R is used as an interruptor letter, every time REINFORCEMENTS appears in the text, encipherment from the second letter on will be identical every time. The letter after the initial R will be enciphered by the first alphabet each time because of the interruption. The same thing will happen with any word that begins with the interruptor letter. Use of a ciphertext interruptor letter instead of a plaintext letter will avoid many of these repeats, but the interruptions will generally occur much less often in such a case.

10-2. Long-Running Key Aperiodic

Much more common than the simple manual aperiodic systems described in the previous paragraph are those that use a long-running, ever changing key. These systems may be enciphered manually, by cipher machine, or by computer, as first discussed in paragraph 8-1. Figure 8-1 gave an example of using a book key where the key letters were a quotation. A quotation, particularly from a book, provides a ready source of long-running keys, but it is relatively unsecure, because the key itself is so orderly. More often, the keys will be random or pseudorandom. The keys are applied to the plaintext using an alphabet chart like the Vigenere square in Figure 8-1. The keys may be generated by a pseudorandom, repeatable process or by a random, nonrepeatable process. Both the sending and receiving cryptographer must have a copy of the same book or pad of keys. When these are intended for single usage of the keys, the system is called a one-time pad system. Truly random one-time pad systems are absolutely unbreakable when used properly. When keys are reused, however, whether by mistake or by design, the messages with the reused keys are likely to be recoverable. Manual one-time pad systems are slow systems to use and present logistics problems for any large scale usage. The volume of keys must be at least equal to the volume of messages to be sent, When more than one communications link shares the use of copies of the same pad, careful procedures must be set up to prevent reuse of the same keys by different users.

10-3. Solution of Long-Running Key Aperiodic

The solution of messages enciphered in long-running key systems may be possible in three situations. First, the key generation process may be known in advance from prior recoveries or other sources. Second, the keys may be so orderly that they are recognizable when partially recovered, as can occur when plaintext is used as the source of keys. Third, the same sequence of keys is reused. We are primarily concerned with the third case, where keys are reused.

a. **Depth Recognition.** A reuse of long-running keys is called a **depth.** Messages using the same keys are called messages in depth. If the keys begin at the same point in two or more messages, the messages are in flush depth. If the keys begin at different points in two or more messages, but include reused keys for at least part of the messages, they are in offset depth. The solution of messages in depth first requires you to recognize that the depth exists.

(1) One way to recognize depth is through exploitation of indicator systems. In one-time pad systems and in many types of cipher machine or computer systems, the starting point or settings for the keys must be known by the enciphering and deciphering cryptographers. This information on the keys is often passed from cryptographer to cryptographer through the use of an indicator system. The first way to recognize a depth is to find two messages or transmissions with identical indicators. Identical indicators will often tip-off that a flush depth is occurring.

(2) The second way to recognize depth is to find repeated text between two or more messages. Except for short accidental repeats, repeated ciphertext will only occur when the same plaintext is enciphered with the same keys. In periodic

systems and simple manual aperiodic, this will often occur within a single message as the same keys are reused. With long-running key aperiodic, this will only occur between messages when keys are reused. If all depths are expected to be flush depths, the search for repeats is a matter of superimposing messages and looking for repeats in the same position in each message. If depths are offset, they are more difficult to find by inspection alone.

(3) The third way to recognize depth is to use a type of coincidence test known as the kappa test. Whether whole words and phrases are repeated using the same keys or not, individual characters using the same keys will occur frequently when depths are present. When two messages are matched together, letter by letter, and do not use the same keys, 1 out of 26 letters (or 3.85 percent) will randomly match. Of course, if a different alphabet is used, or if characters other than letters are also used, the expected number of matches by chance alone will be 1 out of the total number of different characters used. On the other hand, if the messages are correctly placed in depth, a letter by letter comparison (the kappa test) will produce matches about 6.67 percent of the time. Also, the results can be expressed as a kappa index of coincidence showing the ratio of observed coincidences to random expectation. As with searching for repeats, it is much easier to find flush depths than it is to find offset depths, but with computer support, messages can be matched in every possible alignment to search for depths.

(4) As an example of depth recognition, consider the three messages that follow. Each has similar indicator groups that suggest the messages may be in depth with each other. Messages 1 and 2 have identical indicators. Message 3 differs only in the last digit of the second group.

Message 1:

```
JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
```

Message 2:

```
JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
```

Message 3:

```
JJ632 0407 KDHYW QOEBJ DBJGH  PYGEP HOQNY OOISH UYMHX MGTUC
EYWTG RLRKQ YKISC QNPTB JFCRA  EKZXA LLCOZ HIKYE UJPKC SHWHN
VWAXF APEVG XJDQS FISYL SQLCY  JAGRP JJ632
```

(5) There are no repeats longer than three letters between any of the three messages. Because of the identical indicators, we first try to match messages 1 and 2 at a flush depth using the kappa test. The number of matches multiplied by 26 and divided by the number of comparisons equals the kappa IC. Do not count the indicator groups in the comparisons.

```
1: JJ632 0406 HJJBW KBZGA OWSON SRJCF AGORU EOGVA CNWIH GLVZX
                        -   --  -      -     -     -
2: JJ632 0406 FWFQA VSAIA UOSOS SHMQD YGLNO YOOQV GNVSD BOIIG
                        -   --  -      -     -     -

1: MDSAF EMFGP VNNNN ABJPZ TJNVL QMGGN TVBAP MDODN ODMIO NOIWO
    - --           -                                     -
2: XDRAF GFEMM GTCZN VMYSN UHCYM GZBPP BOVYW BLQIO AKEXM NMNTN
    - --           -                                     -

1: XANAC CNLXS EMBWV CVZYD FTPUC TQNAW ZUTUH JJ632
          -
2: SODPA UNBMO QYYQS GOBMA WSUQL JJ632
          -
```

2 to 1: offset 0
13 matches out of 115 comparisons
Kappa IC = 2.94

(6) As shown by the kappa test, the number of matches is well above random expectation. The two messages appear to be in flush depth with each other. Next we try message 3 matched with the first two at a flush depth.

```
1: JJ632 0406 HJJBW KBZGA OWSON SRJCF AGORU EOGVA CNWIH GLVZX
                  -                          -
2: JJ632 0406 FWFQA VSAIA UOSOS SHMQD YGLNO YOOQV GNVSD BOIIG
                                         -   -
3: JJ632 0407 KDHYW QOEBJ DBJGH PYGEP HOQNY OOISH UYMHX MGTUC
                  -                      -   -

1: MDSAF EMFGP VNNNN ABJPZ TJNVL QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM GZBPP BOVYW BLQIO AKEXM NMNTN
                             -                               -
3: EYWTG RLRKQ YKISC QNPTB JFCRA EKZXA LLCOZ HIKYE UJPKC SHWHN
                             -                               -

1: XANAC CNLXS EMBWV CVZYD FTPUC TQNAW ZUTUH JJ632
                        -
2: SODPA UNBMO QYYQS GOBMA WSUQL JJ632
                  --
3: VWAXF APEVG XJDQS FISYL SQLCY JAGRP JJ632
                  --    -
```

3 to 1 and 2: offset 0
9 matches out of 235 comparisons
Kappa IC = 1.00

(7) The flush match of message 3 is clearly not a correct match, because of the low kappa index of coincidence. We next try offsets of 1, 2, 3, 4, and 6 letters to the right.

```
1:  JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2:  JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3:  JJ632 0407  KDHY WQOEB JDBJG  HPYGE PHOQN YOOIS HUYMH XMGTU

1:  MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2:  XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3:  CEYWT GRLRK QYKIS CQNPT BJFCR  AEKZX ALLCO ZHIKY EUJPK CSHWH

1:  XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2:  SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3:  NVWAX FAPEV GXJDQ SFISY LSQLC  YJAGR PJJ63 2
```

3 to 1 and 2: offset 1
13 matches out of 234 comparisons
Kappa IC = 1.44

```
1:  JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2:  JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3:  JJ632 0407   KDH YWQOE BJDBJ  GHPYG EPHOQ NYOOI SHUYM HXMGT

1:  MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2:  XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3:  UCEYW TGRLR KQYKI SCQNP TBJFC  RAEKZ XALLC OZHIK YEUJP KCSHW

1:  XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2:  SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3:  HNVWA XFAPE VGXJD QSFIS YLSQL  CYJAG RPJJ6 32
```

3 to 1 and 2: offset 2
8 matches out of 233 comparisons
Kappa IC = 0.89

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407    KD HYWQO EBJDB  JGHPY GEPHO QNYOO ISHUY MHXMG

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: TUCEY WTGRL RKQYK ISCQN PTBJF  CRAEK ZXALL COZHI KYEUJ PKCSH

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: WHNVW AXFAP EVGXJ DQSFI SYLSQ  LCYJA GRPJJ 632
```

3 to 1 and 2: offset 3
6 matches out of 232 comparisons
Kappa IC = 0.67

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407       K DHYWQ OEBJD  BJGHP YGEPH OQNYO OISHU YMHXM

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: GTUCE YWTGR LRKQY KISCQ NPTBJ  FCRAE KZXAL LCOZH IKYEU JPKCS

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: HWHNV WAXFA PEVGX JDQSF ISYLS  QLCYJ AGRPJ J632

3 to 1 and 2: offset 4
9 matches out of 231 comparisons
Kappa IC = 1.01
```

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407       KDHYW QOEBJ  DBJGH PYGEP HOQNY OOISH UYMHX

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: MGTUC EYWTG RLRKQ YKISC QNPTB  JFCRA EKZXA LLCOZ HIKYE UJPKC

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: SHWHN VWAXF APEVG XJDQS FISYL  SQLCY JAGRP JJ632

3 to 1 and 2: offset 5
17 matches out of 230 comparisons
Kappa IC = 1.92
```

(8) The offset of five is clearly the best match of those tried, and the kappa index of coincidence is a good value for a correct match. The three messages are now correctly placed in depth.

b. **Depth Reading.** When the messages are superimposed properly, they can be solved by a process known as depth reading. With only a few messages, the process of applying the key must be known. With manual systems, standard alphabets are commonly used. With cipher machine or computer based systems, the process of baud addition is usually known or can be figured out easily. The three messages in our example use the standard alphabet Vigenere square of Figure 10-1.

Plaintext

Key	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 10-1. Vigenere square.

(1) With three messages in depth, almost any correct assumption of plaintext will lead to a quick solution. For example, trying the word *REPLACEMENT* as the first word of message 3 produces the results shown below.

```
                               rchte amarr   i
1:  JJ632  0406  HJJBW  KBZGA  OWSON   SRJCF  AGORU  EOGVA  CNWIH  GLVZX

                               ctive gearw   i
2:  JJ632  0406  FWFQA  VSAIA  UOSOS   SHMQD  YGLNO  YOOQV  GNVSD  BOIIG

                               repla cemen   t
3:  JJ632  0407         KDHYW  QOEBJ   DBJGH  PYGEP  HOQNY  OOISH  UYMHX

Key:                    TZSNW  OKSXW   K

1:  MDSAF  EMFGP  VNNNN  ABJPZ  TJNVL   QMGGN  TVBAP  MDODN  ODMIO  NOIWO
2:  XDRAF  GFEMM  GTCZN  VMYSN  UHCYM   GZBPP  BOVYW  BLQIO  AKEXM  NMNTN
3:  MGTUC  EYWTG  RLRKQ  YKISC  QNPTB   JFCRA  EKZXA  LLCOZ  HIKYE  UJPKC

1:  XANAC  CNLXS  EMBWV  CVZYD  FTPUC   TQNAW  ZUTUH  JJ632
2:  SODPA  UNBMO  QYYQS  GOBMA  WSUQL   JJ632
3:  SHWHN  VWAXF  APEVG  XJDQS  FISYL   SQLCY  JAGRP  JJ632
```

(2) Recovering the key from the assumption of *REPLACEMENT* and using it to decipher the other two messages produces good segments of plaintext in each message. It is easy to build on these assumptions to recover additional plaintext. For example, assuming that the second message begins *PROTECTIVE GEAR* and that the word after *TEAM* in the first message is *ARRIVING* leads to additional recoveries.

```
                        resea  rchte  amarr   iving
1:  JJ632  0406  HJJBW  KBZGA  OWSON   SRJCF  AGORU  EOGVA  CNWIH  GLVZX

                        prote  ctive  gearw   illbe
2:  JJ632  0406  FWFQA  VSAIA  UOSOS   SHMQD  YGLNO  YOOQV  GNVSD  BOIIG

                               repla  cemen   tfiri
3:  JJ632  0407         KDHYW  QOEBJ   DBJGH  PYGEP  HOQNY  OOISH  UYMHX

Key:             QFRXW  TZSNW  OKSXW   KWBPZ

1:  MDSAF  EMFGP  VNNNN  ABJPZ  TJNVL   QMGGN  TVBAP  MDODN  ODMIO  NOIWO
2:  XDRAF  GFEMM  GTCZN  VMYSN  UHCYM   GZBPP  BOVYW  BLQIO  AKEXM  NMNTN
3:  MGTUC  EYWTG  RLRKQ  YKISC  QNPTB   JFCRA  EKZXA  LLCOZ  HIKYE  UJPKC

1:  XANAC  CNLXS  EMBWV  CVZYD  FTPUC   TQNAW  ZUTUH  JJ632
2:  SODPA  UNBMO  QYYQS  GOBMA  WSUQL   JJ632
3:  SHWHN  VWAXF  APEVG  XJDQS  FISYL   SQLCY  JAGRP  JJ632
```

(3) This process of assuming text can be continued to a complete solution. Correct assumptions are easily verified. Incorrect assumptions are quickly disproved.

(4) The most difficult step is making the first correct assumption. Message beginnings are the most likely area to yield results, because they are likely to be very stereotyped. Sometimes, just trying the letters RE at the beginning of a message will be enough to suggest the text of the messages in depth with it. When message beginnings do not yield results, more powerful techniques are available.

c. **Crib Dragging.** When you cannot assume the beginning of a message, you can still often correctly assume a particular word that will be in a message. The assumptions can come from familiarity with previous messages, results of traffic analysis and direction finding, or other intelligence sources. Once you suspect a word is in one of two or more messages in depth, you can systematically try the word at every position, recover the keys each position would produce, and try the keys in the other message or messages to see if the keys produce more plaintext. This is a laborious process performed manually, but a sure one. Fortunately, there are some short cuts that can be used to simplify the process.

(1) Two messages in depth can generally be combined in such a way that you can skip the step of key recovery and proceed directly to checking for plaintext. With the Vigenere square of Figure 10-1, this can be accomplished by treating one message as if it were plaintext, the other as ciphertext, and producing the resulting key stream, which is actually a combination of the two ciphertexts. To demonstrate this process, consider the beginnings of messages 1 and 2 from the previous example. If we combine message 1 and message 2 as if they were plaintext and ciphertext respectively, it produces a combination text for the first groups of YNWPE, Message 1 letters are used as keys in the Vigenere square. Message 2 letters represent the internals of the Vigenere square. For example, key H matched against internal F produces plaintext Y.

Message 1:	H	J	J	B	W	. . .
Message 2:	F	W	F	Q	A	. . .
Combination:	Y	N	W	P	E	. . .

(2) If we now apply the correct plaintext of message 1 to the combination text using the Vigenere square, it will directly produce the plaintext of message 2. The

combination text is again found in the key letter position in the square, and the plaintext is found in the same position for each message as the original ciphertexts.

```
   Message 1: H J J B W ...
   Message 2: F W F Q A ...
 Combination: Y N W P E ...
   Message 1: r e s e a ...
   Message 2: p r o t e ...
```

(3) The combination text can be systematically used to try out a plaintext assumption in every position by a process known as crib dragging. *Crib* is a common synonym for *assumption* in cryptanalysts. Consider the following two messages in depth. The first message was sent by a unit undergoing an artillery barrage. It is likely that the word *ARTILLERY* will be found in the message.

```
Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
```

(4) The first step to trying out *ARTILLERY* in message 1 is to create the combination text. Message 1 is treated as plaintext and message 2 as ciphertext.

```
  Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
  Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
```

(5) The results of trying *ARTILLERY* in each of the first three positions are shown below.

```
  Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
  Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
          1: artil lery
          2: mngxp zysc

Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
          1:  arti llery
          2:  weim zffva

Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
          1:   art iller y
          2:   ngx wfmit f
```

(6) Obviously, not one of the first three tries is the correct placement of *ARTILLERY.* The process can be speeded up, however, by plotting the crib vertically and the resulting text for message 2 on a descending diagonal.

```
 Message 1:    IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
 Message 2:    UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination:   MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
       Crib: a mwn
             r  neg
             t   gix
             i    xm w
             l     p zf
             l       zfm
             e        yfi
             r         svt
             y          ca f
```

(7) The plot above is identical in results to the three separate plots that preceded. Once this format is adopted, it is easier to write in a whole row at a time.

```
 Message 1:    IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
 Message 2:    UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination:   MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
       Crib: a mwnpe oubec hlxvo wmkze jgcio  wb
             r  negv flsvt ycomf ndbqv axtzf  nsu
             t   gix hnuxv aeqoh pfdsx czvbh  puwn
             i    xm wcjmk ptfdw eushm rokqw  ejlcn
             l     p zfmpn swigz hxvkp urntz  hmofq w
             l       zfmpn swigz hxvkp urntz  hmofq wz
             e        yfig lpbzs aqodi nkgms  afhyj psn
             r         svt ycomf ndbqv axtzf  nsulw cfag
             y          ca fjvtm ukixc heagm  uzbsd jmhop
```

(8) The plaintext for message 2 appears on the sixth diagonal, as highlighted above. Once the text is spotted and the crib confirmed, it becomes a matter of depth reading, as before. The worksheet can now be set up and the rest of the text recovered.

```
                  artil lery
Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT

                  olumn spot
Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK

Key:              ESILZ PGAB
```

(9) With cipher machine and computer based systems that use baud addition, adding two messages in depth together by baud addition eliminates the key. The baud addition of the two ciphertexts is identical to the baud addition of the two original plaintexts.

(10) Whatever type of alphabet square or system of combining bauds is used, there is usually a way to combine texts in depth to eliminate the effects of the key. If you are unsure how to approach a particular type of system, test samples you create for yourself in the system to see how ciphertext can be combined to eliminate the effect of the key.

PART FIVE

Transposition Systems

CHAPTER 11

TYPES OF TRANSPOSITION SYSTEMS

11-1. Nature of Transposition

Transposition systems are fundamentally different from substitution systems. In substitution systems, plaintext values are replaced with other values. In transposition systems, plaintext values are rearranged without otherwise changing them. All the plaintext characters that were present before encipherment are still present after encipherment. Only the order of the text changes.

a. Most transposition systems rearrange text by single letters. It is possible to rearrange complete words or groups of letters rather than single letters, but these approaches are not very secure and have little practical value. Larger groups than single letters preserve too much recognizable plaintext.

b. Some transposition systems go through a single transposition process. These are called single transposition. Others go through two distinctly separate transposition processes. These are called double transposition.

c. Most transposition systems use a geometric process. Plaintext is written into a geometric figure, most commonly a rectangle or square, and extracted from the geometric figure by a different path than the way it was entered. When the geometric figure is a rectangle or square, and the plaintext is entered by rows and extracted by columns, it is called columnar transposition. When some route other than rows and columns is used, it is called route transposition.

d. Another category of transposition is grille transposition. There are several types of grilles, but each type uses a mask with cut out holes that is placed over the worksheet. The mask may in turn be rotated or turned over to provide different patterns when placed in different orientations. At each position, the holes lineup with different spaces on the worksheet. After writing plaintext into the holes, the mask is removed and the ciphertext extracted by rows or columns. In some variations, the plaintext may be written in rows or columns and the ciphertext extracted using the grille. These systems may be difficult to identify initially when first encountered, but once the process is recognized, the systems are generally solvable.

e. Transposition systems are easy to identify. Their frequency counts will necessarily look just like plaintext, since the same letters are still present. There should be no repeats longer than two or three letters, except for the rare longer accidental repeat. The monographic phi will be within plaintext limits, but a digraphic phi should be lower, since repeated digraphs are broken up by transposition. Identifying which type of transposition is used is much more difficult initially, and you may have to try different possibilities until you find the particular method used or take advantage of special situations which can occur.

f. Columnar transposition systems can be exploited when keys are reused with messages of the same length. As will be explained in Chapter 13, the plaintext to messages with reused keys can often be recovered without regard to the actual method of encipherment. Once the plaintext is recovered, the method can be reconstructed.

11-1. Examples of Columnar Transposition

The most common type of transposition is columnar transposition. It is the easiest to train and use consistently.

a. **Simple Columnar Transposition.** At its simplest, columnar transposition enters the plaintext into a rectangle of a predetermined width and extracts ciphertext by columns from left to right. For example, a simple columnar transposition with a width of seven is shown below.

Plaintext: ENEMY TANKS APPROACHING HILL EIGHT SIX THREE STOP

E	N	E	M	Y	T	A
N	K	S	A	P	P	R
O	A	C	H	I	N	G
H	I	L	L	E	I	G
H	T	S	I	X	T	H
R	E	E	S	T	O	P

Ciphertext:

ENOHH RNKAI TEESC LSEMA HLISY PIEXT TPNIT OARGG HPXXX

(1) The cryptographer receiving the above message knows only that a width of 7 was originally used. The cryptographer rebuilds the matrix by determining the length of each column and writing the ciphertext back into the columns. With a width of 7 and a length of 42, each column must have 6 letters. Inscribing the ciphertext into columns from left to right recreates the original matrix, and the plaintext can be read by rows.

(2) Not all messages will come out even on the bottom row. Here is the same message with *STOP* omitted. The columns are not all the same length. In this case, the matrix is called an incompletely filled matrix.

E	N	E	M	Y	T	A
N	K	S	A	P	P	R
O	A	C	H	I	N	G
H	I	L	L	E	I	G
H	T	S	I	X	T	H
R	E	E				

Ciphertext:

ENOHH RNKAI TEESC LSEMA HLIYP IEXTP NITAR GGHXX

(3) The deciphering cryptographer must now perform the additional step of determining which columns will be longer than the others. With 38 letters and a given width of 7, dividing 38 by 7 produces 5 with a remainder of 3. This means that the basic column length is 5, but the first 3 columns are 1 letter longer. Sometimes, cryptographers will avoid this additional step by padding message texts so that the bottom row is always completely filled.

(4) The solution of these systems is extremely easy. The security depends on just one number, the matrix width. All you have to do to solve a message enciphered by simple columnar transposition is to try different matrix widths until you find the right one. To try each width, you just do exactly what the deciphering cryptographer does. Divide the total length by the trial width and the result and remainder will tell you the basic column length and how many longer columns there are.

(5) If you suspect that only completely filled matrices are being used, the solution is easier. You only need to test widths that evenly divide into the message length in that case. For example, with a length of 56, you would try widths of 7 and 8. If neither of these worked, you would also try 4, 14, 2, and 28 to cover all possibilities. It is better to try the possibilities closest to a perfect square before you try very tall and very wide matrices.

b. **Numerically-Keyed Columnar Transposition.** Numerically-keyed transposition systems are considerably more secure than simple columnar transposition. You cannot exhaust all possibilities with just a few tries as you can with the simple systems. The transposition process is similar to that used to produce transposition mixed sequences.

(1) The numerical key is commonly based on a keyword or key phrase. Unlike keywords used to produce mixed sequences, the keyword may have repeated letters in it. To produce a numerical key from a keyword with repeated letters, the repeated letters are numbered from left to right.

1	2	6	4	8	3	7	5
A	A	R	D	V	A	R	K

12	9	1	4	10	8	6	11	2	13	3	7	5
T	R	A	N	S	P	O	S	I	T	I	O	N

(2) As with simple columnar transposition, matrices may be completely filled or incompletely filled. In either case, the plaintext is written horizontally and the ciphertext is extracted by column in the order determined by the numerical key. The following example shows an incompletely filled matrix.

5	6	1	4	3	2
O	R	A	N	G	E
R	E	Q	U	E	S
T	R	E	I	N	F
O	R	C	E	M	E
N	T	S	I	M	M
E	D	I	A	T	E
L	Y				

Ciphertext:

QECSI SFEME ENMMT UIEIA RTONE LERRT DYXXX

(3) The decipherment process for the receiving cryptographer is more complicated than with simple columnar transposition. The cryptographer must decide the column lengths, as before. With the above message, the cryptographer divides the length of the message by the length of the numerical key. In this case, 32 divided by 6 is 5 with a remainder of 2. The basic column length is 5 with two longer columns at the left. The cryptographer then sets up a matrix with the key at the top and marks the column lengths.

5	6	1	4	3	2
O	R	A	N	G	E
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•				

(4) The ciphertext is now entered by columns according to the numerical key to produce the plaintext.

(5) The solution of numerically-keyed systems is more complex than for simple columnar transposition. It is more than just trying all possibilities. The solution of numerically-keyed columnar transposition is explained in Chapter 12.

11-3. Route Transposition

There are many other ways to transpose messages than columnar transposition using squares and rectangles. The shape of the geometric figure used can be varied, and the method of inscribing and extracting text can be varied. Columnar methods are the most common in military usage, because they are the easiest to learn and use reliably, but other methods may be encountered. Some of these common methods are shown below.

a. Route transposition using other geometric figures.

(1) The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.

			N						M						R						G			
		I		F				E		E				A		R				N		N		
	E				O		C				N		S				I		I				O	
R						R						T						V						W

Ciphertext: NMRGI FEEAR NNEOC NSIIO RRTVW

(2) The triangular pattern is inscribed by rows and extracted by columns.

				R				
			E	I	N			
		F	O	R	C	E		
	M	E	N	T	S	A	R	
R	I	V	I	N	G	N	O	W

Ciphertext:

RMIFE VEONI RIRTN NCSGE ANROW

b. The next examples show just some of the possibilities for route transposition using squares or rectangles. Each example is based on *REINFORCEMENTS ARRIVING NOW* to help you see how the route was entered. The route can be:

(1) Inscribed by spiral, out by columns.

R	E	I	N	F
R	R	I	V	O
A	O	W	I	R
S	N	G	N	C
T	N	E	M	E

Ciphertext:

RRAST ERONN IIWGE NVINM FORCE

(2) Inscribed by diagonals, out by alternating rows.

R	I	O	M	A
E	F	E	S	V
N	C	T	I	G
R	N	R	N	O
E	R	I	N	W

Ciphertext:

RIOMA VSEFE NCTIG ONRNR ERINW

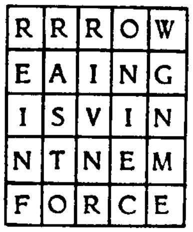
(3) In by outward spiral, out by alternating diagonals.

N	G	N	O	W
I	R	C	E	M
V	O	R	E	E
I	F	N	I	N
R	R	A	S	T

Ciphertext:

NIGNR VIOCO WERFR RNEME IASNT

(4) In by L-pattern, out by spiral from lower right.



R	R	R	O	W
E	A	I	N	G
I	S	V	I	N
N	T	N	E	M
F	O	R	C	E

Ciphertext:

ECROF NIERR ROWGN MENTS AINIV

c. Completely filled squares or rectangles are more common with route transposition than with columnar transposition. The reason is that it is often difficult for the cryptographers to figure out how to handle an incompletely filled matrix. It is simpler in practice to completely fill each matrix than to provide rules to cover every incompletely filled situation.

d. The solution of route transposition is largely a matter of trial and error. When you suspect route transposition, see if the message length is a perfect square or if the matrix can be set up as a completely filled rectangle. Then try entering the ciphertext by different routes, and look for visible plaintext by another route.

CHAPTER 12

SOLUTION OF NUMERICALLY-KEYED COLUMNAR TRANSPOSITION CIPHERS

12-1. Completely Filled Matrices - Determining Matrix Size

When completely filled matrices are known or suspected, the first step in their solution is to determine the matrix size. As discussed in Chapter 11 for simple columnar transposition, the correct width must be an even divisor of the message length. With simple columnar transposition, the correct width could be confirmed easily, because plaintext will appear on the rows when the width is correctly selected. It is not as simple with numerically-keyed transposition. Although each row will contain the letters of plaintext for that row when the width is correctly selected, the letters will be out of order. The key to recognition is the vowel count on each row. Vowels should appear consistently with fairly even counts on each row when the correct width is tried. In plaintext, vowels appear about 40 percent of the time even in small samples of text. This is necessary for text to be pronounceable. If some of the rows have too many or too few vowels, you probably have the wrong width. Consider the next cryptogram.

```
ERESO RIERU GRFPT TEOAE OOSNN   MNIEU SDEES MTSUR FYSBW TEARC

EUXRQ GXXXX
```

a. The cryptogram has 56 letters, assuming the final Xs are all nulls. If a completely filled matrix is suggested by past experience, then the matrix is probably either 7 or 8 letters wide. Write the cryptogram by columns into a trial matrix of each width and count the vowels in each row.

E	R	E	N	E	F	R	3
R	U	O	M	E	Y	C	3
E	G	A	N	S	S	E	3
S	R	E	I	M	B	U	3
O	F	O	U	T	W	X	3
R	P	O	E	S	T	R	2
I	T	S	S	U	E	Q	3
E	T	N	D	R	A	G	2

E	E	T	O	U	M	S	C	4
R	R	T	S	E	T	B	E	2
E	U	E	N	S	S	W	U	4
S	G	O	N	D	U	T	X	2
O	R	A	M	E	R	E	R	4
R	F	E	N	E	F	A	Q	3
I	P	O	I	S	Y	R	G	3

b. The first matrix, with a width of seven letters, has the more regular spacing of vowels. The letter Q in the first matrix also has a U on the same row, whereas the second matrix does not. The first matrix is clearly the better possibility.

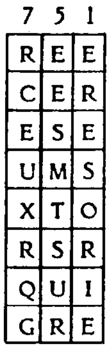
12-2. Matrix Reconstruction by Anagramming

Continuing the same problem, the object now is to rearrange the columns into the original order. The rearrangement of letters to find the original plaintext order is called anagramming. You may be able to see possibilities for complete words on some of the rows, but the Q and the U on the seventh row provide the most obvious starting point. To recover the numerical key at the same time, number the columns in numerical order before starting reconstruction.

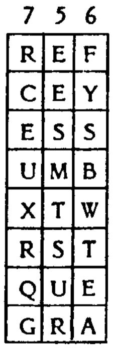
1	2	3	4	5	6	7
E	R	E	N	E	F	R
R	U	O	M	E	Y	C
E	G	A	N	S	S	E
S	R	E	I	M	B	U
O	F	O	U	T	W	X
R	P	O	E	S	T	R
I	T	S	S	U	E	Q
E	T	N	D	R	A	G

7	5			
R	E			
C	E			
E	S			
U	M			
X	T			
R	S			
Q	U			
G	R			

a. All the letter combinations produced by placing columns 7 and 5 together look reasonable for plaintext. At this point, you can see that the last two rows should both be followed by vowels. Both the 1 and 6 columns end with two vowels. Here is what each looks like when added to the initial two columns.

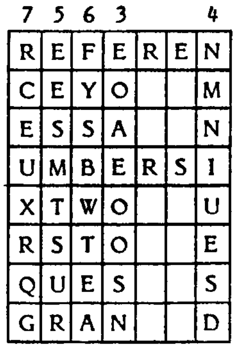


7	5	1
R	E	E
C	E	R
E	S	E
U	M	S
X	T	O
R	S	R
Q	U	I
G	R	E



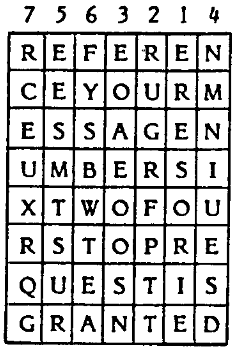
7	5	6
R	E	F
C	E	Y
E	S	S
U	M	B
X	T	W
R	S	T
Q	U	E
G	R	A

b. Both possibilities give good plaintext letter combinations, but at this point, several words are suggested in the second match. REF.. ..CE could be part of *REFERENCE.* XTW could be part of *SIX TWO,* and the UMB in that case would suggest *NUMBER.* With these probable words, clearly column 3 follows 756. Column 7 is the left-hand column, because the letters needed for *REFERENCE, SIX*, and *NUMBER* are on the row above in column 4. Adding columns 3 and 4 produces the next matrix.



7	5	6	3			4
R	E	F	E	R	E	N
C	E	Y	O			M
E	S	S	A			N
U	M	B	E	R	S	I
X	T	W	O			U
R	S	T	O			E
Q	U	E	S			S
G	R	A	N			D

c. The remaining two columns are easily filled in to complete the solution.



7	5	6	3	2	1	4
R	E	F	E	R	E	N
C	E	Y	O	U	R	M
E	S	S	A	G	E	N
U	M	B	E	R	S	I
X	T	W	O	F	O	U
R	S	T	O	P	R	E
Q	U	E	S	T	I	S
G	R	A	N	T	E	D

12-3. Incompletely Filled Matrices - Hat Diagrams

Incompletely filled matrices are also solved by anagramming, but it is a more difficult process because you cannot initially tell which letters are on the same row with each other. If you know or can correctly assume the width of the matrix, you can limit the possibilities. Consider the next cryptogram, which is expected to have a matrix width of eight letters.

EARTR RGHRE TALOA OXUWA UETNE IOTAE ROCTT EROTE EAOSN GHNRD

SEDOO TELHT COEAI TONQR DIMSF EXXXX

a. With a length of 76 letters and a suspected width of 8, there must be four columns with 10 letters and four columns with 9 letters. We can show the range of letters that could be placed in each column by trying the first four columns as the longer columns and alternately, the last four columns as the long columns. The true arrangement is probably neither, but it will serve to show the possible range of first and last letters for each column.

E	T	U	R	E	D	H	N
A	A	E	O	A	S	T	Q
R	L	T	C	O	E	C	R
T	O	N	T	S	D	O	D
R	A	E	T	N	O	E	I
R	O	I	E	G	O	A	M
G	X	O	R	H	T	I	S
H	U	T	O	N	E	T	F
R	W	A	T	R	L	O	E
E	A	E	E				

E	E	W	T	R	H	E	O
A	T	A	A	O	N	L	N
R	A	U	E	T	R	H	Q
T	L	E	R	E	D	T	R
R	O	T	O	E	S	C	D
R	A	N	C	A	E	O	I
G	O	E	T	O	D	E	M
H	X	I	T	S	O	A	S
R	U	O	E	N	O	I	F
				G	T	T	E

b. These two extreme situations can be combined into a single diagram, called a hat diagram. It is constructed by using the first diagram. Next, combine the letters that the second diagram shows can precede the already listed letters by adding them to the top of the first diagram. Similarly, draw a line across the bottom of the first diagram to show the possible bottom letters. The altered first matrix is now the completed hat diagram.

1	2	3	4	5	6	7	8
				R			
			T	O	H		
		W	A	T	N	E	
	E	A	E	E	R	L	O
E	T	U	R	E	D	H	N
A	A	E	O	A	S	T	Q
R	L	T	C	O	E	C	R
T	O	N	T	S	D	O	D
R	A	E	T	N	O	E	I
R	O	I	E	G	O	A	M
G	X	O	R	H	T	I	S
H	U	T	O	N	E	T	F
R	W	A	T	R	L	O	E
E	A	E	E				

c. The completed hat diagram can now be used as a guide to show how columns may be aligned together. Its value can be seen if you try to place the Q in the text before a U. There are two Us in the cryptogram. The Q is necessarily near the top of the matrix. The U in column 2 can only be at the bottom of the matrix. The U in column 3 can only be at or near the top of the matrix. The correct U to place with the Q is now obvious. Lining up the Q in column 8 with the U from column 3 produces an initial reconstruction.

8	3	
O	W	
N	A	
Q	U	
R	E	
D	T	
I	N	
M	E	
S	I	
F	O	
E	T	

d. Next, there is an X near the bottom of the matrix in column 2. It will combine well with the SI of the first two columns to produce *SIX*.

8	3	2
O	W	E
N	A	T
Q	U	A
R	E	L
D	T	O
I	N	A
M	E	O
S	**I**	**X**
F	O	U
E	T	W

e. *SIX* is not the only number near the bottom of the matrix. *FOUR* and *TWO* are likely on the last two rows, and column 4 is available with RO near the bottom.

8	3	2	4
O	W	E	A
N	A	T	E
Q	U	A	R
R	E	L	O
D	T	O	C
I	N	A	T
M	E	O	T
S	I	X	E
F	O	U	R
E	T	W	O

f. The E after *SIX* suggests *EIGHT*. The numbers themselves suggest the word *COORDINATES,* which appears in the middle of the matrix. With these words written in, the rest of the columns can be placed.

8	3	2	4	7	5	1	6
O	W	E	A	L	T	E	R
N	A	T	E	H	E	A	D
Q	U	A	R	T	E	R	S
R	E	L	O	C	A	T	E
D	T	O	C	O	O	R	D
I	N	A	T	E	S	R	O
M	E	O	T	A	N	G	O
S	I	X	E	I	G	H	T
F	O	U	R	T	H	R	E
E	T	W	O	O	N	E	L

g. All letters are now used, but several letters appear at both the top and bottom of the matrix. The first word of the message is *ALTERNATE,* and the letters before it all appear correctly at the bottom of columns. The L at the bottom after *ONE* correctly appears as part of *ALTERNATE* at the top. Removing the duplicated letters and shifting *ALTERNATE* to begin at the left-hand column completes the solution.

4	7	5	1	6	8	3	2
A	L	T	E	R	N	A	T
E	H	E	A	D	Q	U	A
R	T	E	R	S	R	E	L
O	C	A	T	E	D	T	O
C	O	O	R	D	I	N	A
T	E	S	R	O	M	E	O
T	A	N	G	O	S	I	X
E	I	G	H	T	F	O	U
R	T	H	R	E	E	T	W
O	O	N	E				

h. This solution depended on correctly identifying the width of the matrix and the fortunate appearance of the Q and U. Without the Q and U and without any indication of the width, a great deal more trial and error would be required for a successful solution. Hat diagrams can be constructed for different possible widths, for example, and probable words searched for within the structure of the diagram. The solution is still possible in most cases, although it will often take longer than the example did. When the same keys are reused for a period, special situations can arise which make the solution much easier. The next chapter shows the techniques that can be used in these special situations.

CHAPTER 13

TRANSPOSITION SPECIAL SOLUTIONS

13-1. Special Exploitable Situations

Military forces are rarely equipped to change cryptosystem keys with every message transmitted. The logistics and management problems of providing enough different keys and controlling their use are difficult to handle. Normally, keys will be reused for a period before they are changed. With transposition systems, several special situations can arise when keys are reused that make a solution possible when the system might otherwise resist successful analysis. One of these situations arises in columnar transposition whenever similar beginnings and endings are used with the same width matrix. The keys do not have to be the same in this case as long as the width is the same. Another more general situation occurs whenever two or more different messages of the same length occur using exactly the same keys. Each of these situations is explained in the following paragraphs.

13-2. Similar Beginnings and Endings

With columnar transposition, repeated message beginnings or endings can cause an easily recognizable and exploitable situation. When the same width keys are used and the beginnings are the same, the tops of the columns in each message will consist of the same letters. When the length of the repeated beginning is several times as long as the width of the matrix, these repeated letters are easy to spot.

a. The next two messages demonstrate the techniques that can be used when similar beginnings are encountered. Repeated segments between the two messages are underlined.

Message 1:

```
ASOLI LBOAE WDLIR ACIEL NSAIR IEDLS NDWND TQNIH UAOTL FMLIF
1             2             3               4            5
AMPES DBREU SCEPV NELOM YEODC SHCAI TIELT MNAEE IDERA
          6               7            8
```

Message 2:

```
QNILB TSROI RRIEP LIHUE OZYAS OLSUT ARZEO LTMUI MTQBR OAUSC
1            2               3              4              5
IEEHT RXOLI RSWBO DSERD EODPL TIAFS EIFAE SDEEE ZT
         6              7            8
```

(1) There are eight repeated segments in each, which shows that the messages are each eight columns wide. The repeated segments are not in the same order, which shows that the two messages use different numerical keys.

(2) Message 1 has 95 letters. Dividing 8 into 95 gives 11 with a remainder of 7. This means that all but one column must have 12 letters. The distance between repeats shows that this is true. All segments have 12 letters except for the fifth segment, which has 11 letters. The fifth segment, beginning IFA, must be the right-hand column of the matrix.

(3) Message 2 has 92 letters. Four columns have 12 letters and four columns have 11 letters.

(4) All repeated segments contain three letters except for the ASOL segment. The column beginning ASOL is probably the left-hand column.

(5) As a result of these observations, we can place the first and last columns in each matrix, and we can separate the middle six columns into two groups of three, based on the length of the columns in message 2.

Message 1:

1		3	8	2		4	6	7		5
A		R	L	L		Q	U	E		I
S		I	T	I		N	S	O		F
O		E	M	R		I	C	D		A
L		D	N	A		H	E	C		M
I		L	A	C		U	P	S		P
L		S	E	I		A	V	H		E
B		N	E	E		O	N	C		S
O		D	I	L		T	E	A		D
A		W	D	N		L	L	I		B
E		N	E	S		F	O	T		R
W		D	R	A		M	M	I		E
D		T	A	I		L	Y	E		

Message 2:

3		2	4	6		1	5	7		8
A		R	L	L		Q	U	E		I
S		I	T	I		N	S	O		F
O		E	M	R		I	C	D		A
L		P	U	S		L	I	P		E
S		L	I	W		B	E	L		S
U		I	M	B		T	E	T		D
T		H	T	O		S	H	I		E
A		U	Q	D		R	T	A		E
R		E	B	S		O	R	F		E
Z		O	R	E		I	X	S		Z
E		Z	O	R		R	O	E		T
O		Y	A	D						

(6) Completion of the solution from here is straightforward. Anagram each group of three columns in each message, and the solution is complete. The similar beginning is *ALL REQUISITIONS FOR MEDICAL.*

b. Messages with similar endings, such as a repeated signature block, show repeated segments which represent the bottoms of columns instead of the top. The solution is approached the same way, except that the text will not necessarily appear in the same columns in both messages.

13-3. Messages With the Same Length and Keys

Whenever two or more messages have the same length and are transposed with the same keys, they can be solved together. The more messages you find that are the same length and use the same keys, the easier they are to solve. This technique can be used regardless of the type of transposition system.

a. Solving messages with the same length and keys is particularly effective with columnar transposition. The next example shows how the solution can be approached. The five messages all use the same keys. Their positions have been numbered for easy reference and to aid in key recovery.

										1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
Message 1:	L	P	Q	R	Y	T	T	L	P	U	A	R	R	S	I	U	E	D	E	O	E	T	S	R	E
Message 2:	Q	S	N	E	T	B	B	U	H	B	H	R	S	M	D	R	E	D	A	A	O	A	E	E	E
Message 3:	A	O	E	E	W	O	V	G	U	C	M	T	N	I	S	F	R	D	E	R	E	S	O	T	E
Message 4:	I	O	O	O	E	O	D	N	R	N	N	N	P	O	H	T	T	Y	G	E	T	T	W	R	A
Message 5:	J	N	U	O	T	E	K	U	F	R	R	C	V	A	D	O	O	N	N	I	T	A	I	F	E

(1) The Q in message 2 in position 1 must certainly be followed by the U in position 8.

(2) Position 1 must be at the top of a column in the original matrix, since columns are extracted beginning at the top. Position 8 is also probably at the top of a column. This applies not just to message 2, but to all five messages. The position 1 column can be written next to position 8.

1	8
L	L
Q	U
A	G
I	N
J	U

(3) Position 2 must be from the second row of the matrix. If position 8 is from the top row, then position 9 must be from the second row, also. Similarly, positions

3 and 10 are from the third row. Positions 4 and 11 are from the fourth row. Positions 5 and 12 are probably from the fifth row, although these are short messages and there might not be as many as five rows.

	1	8	2	9	3	10	4	11	5	12
Message 1:	L	L	P	P	Q	U	R	A	Y	R
Message 2:	Q	U	S	H	N	B	E	H	T	R
Message 3:	A	G	O	U	E	C	E	M	W	T
Message 4:	I	N	O	R	O	N	O	N	E	N
Message 5:	J	U	N	F	U	R	O	R	T	C

(4) Now the task is to find additional columns to add to the fragments already started. For example, the QU in message 2 should be followed by a vowel, and the most likely letter after JU in message 5 is N. There are three columns with an N in message 5, and only one of these, position 19, has a vowel in message 2. Therefore, we will add columns 19, 20, 21, 22, and 23 to our fragments.

	1	8	19	2	9	20	3	10	21	4	11	22	5	12	23
Message 1:	L	L	E	P	P	O	Q	U	E	R	A	T	Y	R	S
Message 2:	Q	U	A	S	H	A	N	B	O	E	H	A	T	R	E
Message 3:	A	G	E	O	U	R	E	C	E	E	M	S	W	T	O
Message 4:	I	N	G	O	R	E	O	N	T	O	N	T	E	N	W
Message 5:	J	U	N	N	F	I	U	R	T	O	R	A	T	C	I

(5) All of the fragments produce good plaintext except, possibly, the last one. QUA will usually be followed by an R. Of the two columns with an R in message 2, column 12 provides the best combinations.

	1	8	19	12	2	9	20	13	3	10	21	14	4	11	22	15	5	12	23	16
Message 1:	L	L	E	R	P	P	O	R	Q	U	E	S	R	A	T	I	Y	R	S	U
Message 2:	Q	U	A	R	S	H	A	S	N	B	O	M	E	H	A	D	T	R	E	R
Message 3:	A	G	E	T	O	U	R	N	E	C	E	I	E	M	S	S	W	T	O	F
Message 4:	I	N	G	N	O	R	E	P	O	N	T	O	O	N	T	H	E	N	W	T
Message 5:	J	U	N	C	N	F	I	V	U	R	T	A	O	R	A	D	T	C	I	O

(6) All of the matches give good plaintext, except the fifth set, which clearly does not belong now. It is easy now to see words to build on, such as *ARTILLERY*, *QUARTERS* or *HEADQUARTERS*, *JUNCTION*, *SUPPORT*, *FIVE*, and others. All of these leads are added to the completely anagrammed messages.

	1		2	1			1	1		2	1			2	1		2	1		1	2	1		2	1
	1	4	2	5	1	8	9	2	5	3	6	2	9	0	3	6	4	7	3	0	1	4	7	5	8
Message 1:	A	R	T	I	L	L	E	R	Y	S	U	P	P	O	R	T	R	E	Q	U	E	S	T	E	D
Message 2:	H	E	A	D	Q	U	A	R	T	E	R	S	H	A	S	B	E	E	N	B	O	M	B	E	D
Message 3:	M	E	S	S	A	G	E	T	W	O	F	O	U	R	N	O	T	R	E	C	E	I	V	E	D
Message 4:	N	O	T	H	I	N	G	N	E	W	T	O	R	E	P	O	R	T	O	N	T	O	D	A	Y
Message 5:	R	O	A	D	J	U	N	C	T	I	O	N	F	I	V	E	F	O	U	R	T	A	K	E	N

(7) The final step in the solution is to recover the numerical keys. Looking at the beginning, the pattern starts to repeat after seven letters, so the original matrix was seven letters wide. The numerical key, derivable by observing the order in which the columns were extracted, was 4275136.

b. The technique of solving messages of the same length and keys can be used with any transposition system. It can be used as the basis for recovery of more difficult transposition systems such as large grilles and double transposition. The cyclic pattern of columnar transposition aided the solution of the example above. Given four or more messages of the same length and keys, however, the complete messages can often be anagrammed without the help of the cyclic pattern.

PART SIX

Analysis of Code Systems

CHAPTER 14

TYPES OF CODE SYSTEMS

14-1. The Nature of Code Systems

As explained in Chapter 1, the key feature that distinguishes a code from a substitution cipher is that a code will substitute for words as well as characters.

a. Codes range in size from small charts or lists on a single sheet of paper to books as large as an unabridged dictionary.

b. Plaintext values are replaced by code groups or code words. A code group or word may replace anything from a single character to a whole sentence.

c. Since codes can compress whole sentences into a small code group, not all codes are used for security purposes. Some are used for economy instead, by replacing common sentences and phrases with a single group. For example, radio operators use Q and Z signals as a brevity code. Q and Z signals are three letter code groups beginning with Q or Z that stand for common communications procedures. A single code Q or Z signal replaces sentences or phrases such as QSA, *My signal strength is* ... and ZNN, *I have nothing now.* Operators memorize the Q and Z signals that they commonly use and the result is quicker, more economical communications.

d. Some codes are used for prearranged messages only. Limited in size and purpose, a single code group may be transmitted as a signal to begin a preplanned attack, for example. Prearranged message codes are sometimes referred to as pamcodes. Prearranged message codes may also take the form of innocent communications, so that an apparently harmless message contains a secret meaning. The message, *Les sanglots longs des violons de l'automne,* a harmless sentence in French, signaled the French underground in World War II that the Allied invasion of France was to begin soon. Codes with an innocent appearance but a secret meaning are known as open codes.

e. Prearranged message codes can only be used for limited, preplanned purposes. General purpose codes which can be used for any communications are more common. All general purpose codes must include within them, a provision for spelling words that are not included in their vocabulary. Even when very large book codes are used, proper names will sometimes need to be encoded that are not in the code's vocabulary. General purpose codes thus share some of the characteristics of substitution ciphers.

f. Codes are at their weakest when they are used to spell words. Most codes are broken into through spelling. Large codes attempt to defeat this weakness by providing many variants for letters and common syllables. The letter E might be encoded by 10 different code groups in a large code, for example. Other code groups would represent common syllables with E in them like RE, ER, EN, and ENT. In this respect, codes are similar to syllabary squares, and the initial approach to analysis can be similar between syllabary squares and codes.

g. When a high degree of security is required using codes, there are two approaches to increasing the security of codes. One is to use very large book codes, since the larger the code, the more secure it is. The other is to further encipher the code to produce an enciphered code. Any of the cipher procedures discussed earlier in this manual can be used, but the most common is to use polyalphabetic encipherment. Repeating keys and long-running keys may be used. It is one way to combine the advantages of brevity with the added security of polyalphabetics, although such procedures are time-consuming to use. They cannot be used practically in rapidly changing combat situations, for example, when speed of communications is important. Large codes and enciphered codes were common earlier in this century when a high degree of security was desired. Today, with advances in electronics, cipher machine and computer based systems are more common when a high degree of security is required.

14-2. Book Codes

Codes too large to be printed on just one or two pages are called book codes. They may range from small pamphlets to large bound books.

a. The code values in book codes may consist of letters, numbers, or a combination of letters and numbers. Usually, the code groups are a constant length, but there are occasional exceptions. Code values used primarily for voice communications will sometimes consist of pronounceable words rather than regular length groupings of characters. We will refer to only code groups in the rest of this chapter and the next, but you should understand that comments about code groups also apply to code words.

b. The simplest book codes consist of a single orderly listing of code groups and their meanings. The code groups are listed in the book in alphabetical or numerical order, and their meanings are also in a logical order. This single listing is used for encoding and decoding, and is called a one-part code. The plaintext values may be strictly alphabetical in arrangement or may be separated into separate sections for words, letters and syllables, and numbers. Occasionally, they will be arranged topically with such things as units in one section, weapons systems in another, place-names in another, and so on. The key feature of one-part codes is that when the code groups are listed in order, their plaintext meanings will also be in a logical order. A sample portion of a one-part code is shown below.

CODE GROUP:	PLAINTEXT:
AAB	A
ABD	AB
ACF	ABANDON
ADH	ABOUT
AEJ	ACCIDENT
AFL	ACTION
AGN	ACTIVE
AHP	ACTIVITY
...	...
...	...

c. The orderly structure of one-part codes makes them easy to use, but greatly reduces their security. The analyst can use the structure to narrow down possible meanings for code groups. More secure codes are randomly arranged, and are necessarily printed in two parts. One section lists the code groups in order, and it is used for decoding. The other section, containing exactly the same information, lists the plaintext values in order, and is used for encoding. This type of code is called a two-part code. Portions of the encoding and decoding sections of a two-part code are shown below. Note that one group occurs in common between the two parts.

ENCODING SECTION:		DECODING SECTION:	
KTOL	A	ABAB	RESISTANCE
YNIF	A	ABEC	SIZE
ACEJ	AB	ABID	CHEMICAL
VAUW	ABANDON ING S	ABOF	T-72
WHOD	ABILITY	ABUG	QUALITY
AOUT	ABLE	ACAH	15
LWOQ	ABLE TO	ACEJ	AB
TEER	ABOUT	ACIK	VERIFY ING S
...	...	...	...
...	...	...	...

14-3. Matrix Codes and Code Charts

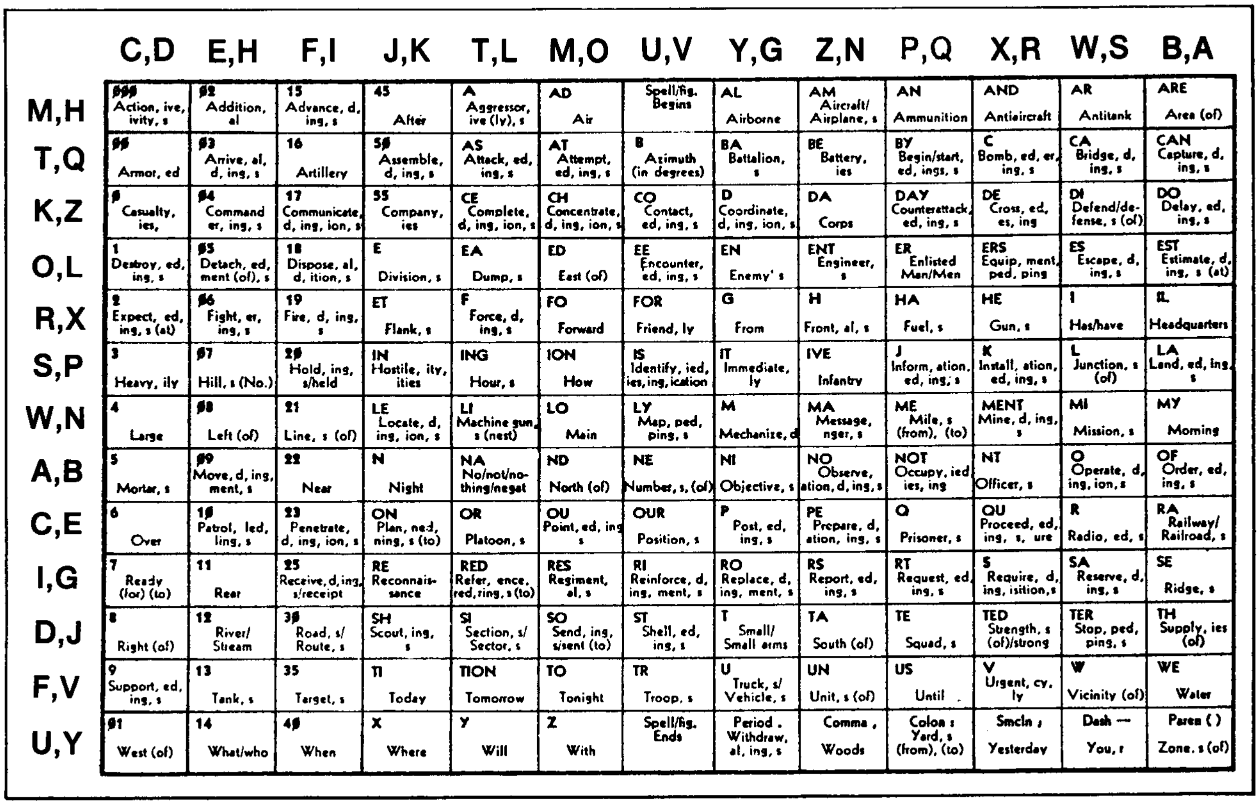
Small codes can be conveniently printed in the form of a small coordinate matrix system.

a. Typically 10 by 10 or larger, matrix codes, also known as code charts, can contain letters, syllables, numbers, and a small vocabulary of words. They are very easy to use, and communicators can be trained in their use quickly and easily. They also offer more security than most simple ciphers.

b. Code charts are easily changed from one cryptoperiod to the next by simply changing the coordinates, while retaining the same matrix.

c. They are a very close relative to the syllabary square cipher. If the syllabary square shown in Chapter 5 contained some words as well as letters, syllables, and numbers, it would be a code instead of a cipher.

d. One type of code chart places two plaintext values in each cell—an upper value and a lower value. The lower values are all words. The upper values are all numbers, letters, or syllables. Two of the cells are set aside as shift values to indicate whether to read the upper values or lower values in the code groups that follow. A sample chart of this type is shown in Figure 14-1. This example uses letters for coordinates, and has variants on each row and column. The word *ARTILLERY*, for example, could be encoded as TF, TI, QF, or QI. The cells MU and UU are begin and end spell indicators. The bottom values in each cell are used until a begin spell group is sent. Then the top values are used until the end spell group is used to shift back to the lower values.



	C,D	E,H	F,I	J,K	T,L	M,O	U,V	Y,G	Z,N	P,Q	X,R	W,S	B,A
M,H	ØØØ Action, ive, ivity, s	Ø2 Addition, al	15 Advance, d, ing, s	45 After	A Aggressor, ive (ly), s	AD Air	Spell/fig. Begins	AL Airborne	AM Aircraft/ Airplane, s	AN Ammunition	AND Antiaircraft	AR Antitank	ARE Area (of)
T,Q	ØØ Armor, ed	Ø3 Arrive, al, d, ing, s	16 Artillery	5Ø Assemble, d, ing, s	AS Attack, ed, ing, s	AT Attempt, ed, ing, s	B Azimuth (in degrees)	BA Battalion, s	BE Battery, ies	BY Begin/start, ed, ings, s	C Bomb, ed, er, ing, s	CA Bridge, d, ing, s	CAN Capture, d, ing, s
K,Z	Ø Casualty, ies,	Ø4 Command er, ing, s	17 Communicate, d, ing, ion, s	55 Company, ies	CE Complete, d, ing, ion, s	CH Concentrate, d, ing, ion, s	CO Contact, ed, ing, s	D Coordinate, d, ing, ion, s	DA Corps	DAY Counterattack, ed, ing, s	DE Cross, ed, es, ing	DI Defend/de-fense, s (of)	DO Delay, ed, ing, s
O,L	1 Destroy, ed, ing, s	Ø5 Detach, ed, ment (of), s	18 Dispose, al, d, ition, s	E Division, s	EA Dump, s	ED East (of)	EE Encounter, ed, ing, s	EN Enemy' s	ENT Engineer, s	ER Enlisted Man/Men	ERS Equip, ment, ped, ping	ES Escape, d, ing, s	EST Estimate, d, ing, s (at)
R,X	2 Expect, ed, ing, s (at)	Ø6 Fight, er, ing, s	19 Fire, d, ing, s	ET Flank, s	F Force, d, ing, s	FO Forward	FOR Friend, ly	G From	H Front, al, s	HA Fuel, s	HE Gun, s	I Has/have	IL Headquarters
S,P	3 Heavy, ily	Ø7 Hill, s (No.)	2Ø Hold, ing, s/held	IN Hostile, ity, ities	ING Hour, s	ION How	IS Identify, ied, ies, ing, ication	IT Immediate, ly	IVE Infantry	J Inform, ation, ed, ing, s	K Install, ation, ed, ing, s	L Junction, s (of)	LA Land, ed, ing, s
W,N	4 Large	Ø8 Left (of)	21 Line, s (of)	LE Locate, d, ing, ion, s	LI Machine gun, s (nest)	LO Main	LY Map, ped, ping, s	M Mechanize, d	MA Message, nger, s	ME Mile, s (from), (to)	MENT Mine, d, ing, s	MI Mission, s	MY Morning
A,B	5 Mortar, s	Ø9 Move, d, ing, ment, s	22 Near	N Night	NA No/not/no-thing/negat	ND North (of)	NE Number, s, (of)	NI Objective, s	NO Observe, ation, d, ing, s	NOT Occupy, ied ies, ing	NT Officer, s	O Operate, d, ing, ion, s	OF Order, ed, ing, s
C,E	6 Over	1Ø Patrol, led, ling, s	23 Penetrate, d, ing, ion, s	ON Plan, ned, ning, s (to)	OR Platoon, s	OU Point, ed, ing s	OUR Position, s	P Post, ed, ing, s	PE Prepare, d, ation, ing, s	Q Prisoner, s	QU Proceed, ed, ing, s, ure	R Radio, ed, s	RA Railway/ Railroad, s
I,G	7 Ready (for) (to)	11 Rear	25 Receive, d, ing, s/receipt	RE Reconnais-sance	RED Refer, ence, red, ring, s (to)	RES Regiment, al, s	RI Reinforce, d, ing, ment, s	RO Replace, d, ing, ment, s	RS Report, ed, ing, s	RT Request, ed, ing, s	S Require, d, ing, isition, s	SA Reserve, d, ing, s	SE Ridge, s
D,J	8 Right (of)	12 River/ Stream	3Ø Road, s/ Route, s	SH Scout, ing, s	SI Section, s/ Sector, s	SO Send, ing, s/sent (to)	ST Shell, ed, ing, s	T Small/ Small arms	TA South (of)	TE Squad, s	TED Strength, s (of)/strong	TER Stop, ped, ping, s	TH Supply, ies (of)
F,V	9 Support, ed, ing, s	13 Tank, s	35 Target, s	TI Today	TION Tomorrow	TO Tonight	TR Troop, s	U Truck, s/ Vehicle, s	UN Unit, s (of)	US Until	V Urgent, cy, ly	W Vicinity (of)	WE Water
U,Y	Ø1 West (of)	14 What/who	4Ø When	X Where	Y Will	Z With	Spell/fig. Ends	Period . Withdraw, al, ing, s	Comma , Woods	Colon : Yard, s (from), (to)	Smcln ; Yesterday	Dash — You, r	Paren ( ) Zone, s (of)

Figure 14-1. Sample code chart.

CHAPTER 15

ANALYSIS OF SYLLABARY SPELLING

15-1. Identification of Syllabary Spelling

The key to breaking into codes and syllabary ciphers is to identify and exploit syllabary spelling. If possible, try to locate instances where the same word is spelled in different ways by combining the syllables and letters in different combinations each time. This situation can be exploited fairly easily.

a. Identifying repeated syllabary spelling in syllabary squares was demonstrated in Chapter 5.

b. In codes, only certain groups represent letters and syllables, but these tend to cluster together. With code charts, if begin spell or letter shift groups are used, identifying these special purpose groups serves to point right to groups used for spelling. Often begin spell-end spell groups or letter shift-word shift groups are the highest frequency groups and tend to alternate in the text. This makes them quite easy to spot.

c. In codes where no shift groups are used, the code groups that represent letters and syllables tend to cluster together, just as code groups that represent numbers do. If necessary, computer produced indexes of code groups and the code groups they appear with will help to isolate those used for spelling.

15-2. Recovery of Syllabary Spelling

By comparing different spellings of the same word, you can often figure out which groups represent single letters and which represents syllables. Then, the groups which represent syllables can be replaced by groups that represent single letters. Reduction to single letter terms, in turn, enables recognition of word patterns. This approach to recovery of syllabary spelling applies equally to syllabary squares, code charts, and book codes. The segments below, each of which represents the same plaintext, illustrates how spelling can be recovered.

```
A: 81 35 25 74 60 60 11 54 88 88 14 28

B: 83 29 60 60 11 59 88 14 28

C: 81 35 29 60 60 11 59 88 11 60 25 35

D: 83 25 76 60 11 59 88 14 25 35
```

a. The first three segments all include the text 60 60 preceded by two, three, or four dinomes. If we suppose that the four dinome spelling is all single letters because it is longer than the others, then the two dinomes in segment B must each represent digraphs. Segment C with its three dinomes helps to confirm this breakout.

b. Similarly, segments A and B end with 88 14 28. Segment D ends 88 14 25 35; therefore, 28 must equate to 25 35.

c. Similar comparisons show that 14 equates to 11 60, 59 equates to 54 88, and 76 equates to 74 60.

d. We now take the first segment, for example, and replace all the dinomes that equate to two other dinomes with the single letter equivalents.

```
   Segment A: 81 35 25 74 60 60 11 65 88 88   14      28
                                             /\      /\
 Replacement: 81 35 25 74 60 60 11 54 88 88 11 60  25 35
```

e. Reduced to single letter terms, the word pattern for the replacement segment is -ABCDDEFGGEHBA. This word pattern equates to the word *RECONNAISSANCE.*

f. These recoveries can, in turn, be used to recover additional plaintext. Whether the system is a syllabary square, a code chart, or a book code, the initial entry is the hardest part. Once the first confirmed recoveries are made, follow-on recoveries are easier.

g. The example above depended on finding sufficient repeated text to reduce the segments to single letter equivalents. This will not always be possible, but it is only one of the approaches an analyst can use to aid in recovery of the system. Anything that provides clues to the plaintext can help solve the system. Information from other sources such as traffic analysis and direction finding can help. Traffic passed in other systems may provide isologs or clear clues to the content of the text. If the code is a one-part or uses an orderly matrix, the orderliness itself is a major aid in recovering plaintext. Encoded numbers may also help.

15-3. Recovery of Numbers

Another vulnerable point of entry in syllabary squares and codes is encrypted numbers, as has been demonstrated with other systems. Numbers, whether spelled out or encrypted by direct equivalents tend to occur with each other. Grid coordinates will typically occur in groups of four or six digits. Times are usually four digits, and tend to be rounded off into multiples of 5, 10, or 15 minutes. Times always begin with 0, 1, or 2. The third digit of a time is always 5 or less. Because of these characteristics, it is often quite easy to recognize the equivalents of 0, 1, 2, 3, 4, and 5. Even when variants are used, they tend to stand out. Given these six values, others readily follow. Recovered grid coordinates, in turn, give major clues to the rest of the text. Numbers like 7.62 (millimeter), 47 (AK-47 rifle), 45 (caliber), and 72 (T-72 tank) all provide clues to surrounding text.

15-4. Recovery of Words

Initial entry into code systems is often made through the elements that are most like a cipher. Spelled out words and encoded numbers are the weakest points in a code. Once these cipher-like groups are recovered, making further recoveries depends on recognizing the meaning of code groups that represent words and phrases. Slightly different skills are required to recover the vocabulary of a code than are required for ciphers. Cipher analysis tends to be more mathematical in nature.

a. Code recovery is more related to language skills, particularly when the text is not in English. Although words can be recovered as their English equivalents, the actual foreign language words must be known to take advantage of any alphabetic structure in the code. In languages where the sentence structure varies from English, the characteristic structures must be familiar to make sense of the code.

b. Codes are less apt to be fully recovered than ciphers. Code groups cannot be recovered until they are used, and large codes may contain many groups that remain unused for a long time. Each code group must be observed in use several times before its plaintext value can be confidently assigned. Errors are very common in encrypted traffic, and a group must be reused several times just to be sure it is not in error. It also takes repeated usage, in many cases, to be sure which of several words with similar meanings represent a particular code group. Recovery of book codes may never be completed, even when most text becomes readable at an early stage.

APPENDIX A

FREQUENCY DISTRIBUTIONS OF ENGLISH DIGRAPHS

Frequency distributions of English digraphs appearing in 50,000 letters of government plaintext telegrams, reduced to 5,000 digraphs.

Table A-1. Frequency distribution digraphs.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	TOTAL
A	3	6	14	27	1	4	6	2	17	1	2	32	14	64	2	12		44	41	47	13	7	3		12		374
B	4				18				2	1		6	1		4			2	1	1	2				7		49
C	20		3	1	32	1		14	7		4	5	1	1	41			4	1	14	4		1		1		155
D	32	4	4	8	33	8	2	2	27	1		3	5	4	16	5	2	12	13	15	5	3	4		1		209
E	35	4	32	60	42	18	4	7	27	1		29	14	111	12	20	12	87	54	37	3	20	7	7	4	1	648
F	5		2	1	10	11	1		39			2	1		40	1		9	3	11	3		1		1		141
G	7		2	1	14	2	1	20	5	1		2	1	3	6	2		5	3	4	2		1				82
H	20	1	3	2	20	5			33			1	2	3	20	1	1	17	4	28	8		1		1		171
I	8	2	22	6	13	10	19				2	23	9	75	41	7		27	35	27		25		15		2	368
J	1				2										2						2						7
K	1		1		6				2			1		1					1								13
L	8	3	3	9	37	3	1	1	20			27		1	13	3		2	6	8	2	2	2		10		183
M	36	6	3	1	26	1		1	9				13		10	8		2	4	2	2				2		126
N	26	3	19	52	57	9	27	4	30	1	2	5	5	8	18	3	1	4	24	82	7	3	3		5		397
O	7	4	8	12	3	25	2	3	5	1	2	19	25	77	6	25		64	14	19	37	7	8	1	2		376
P	14	1	1	1	23	2		3	6			13	4	1	17	11		18	6	8	3	1	1		1		135
Q													1					1			15						17
R	39	2	9	17	98	6	7	3	30	1	1	5	9	7	28	13		11	31	42	5	5	4		9		382
S	24	3	13	5	49	12	2	26	34		1	2	3	4	15	10		5	19	63	11	1	4		1		307
T	28	3	6	6	71	7	1	78	45			5	6	7	50	2	1	17	19	19	5		36		41	1	454
U	5	3	3	3	11	1	8		5			6	5	21	1			31	12	12		1					130
V	6				57				12						1					1							77
W	12				22			4	13			1		2	19			1	1						1		76
X	2		2	1	1	1		1	2					1	1	2		1	1	7							23
Y	6	2	4	4	9	11	1	1	3			2	2	6	10	3		4	11	15	1		1				96
Z	1				2				1																		4
TOTAL	370	46	154	217	657	137	82	170	374	8	14	189	123	397	373	130	17	368	304	462	130	75	77	23	99	4	5000

Table A-2. The 428 digraphs of Table A-1, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
EN	111	2.05	.99	AL	32	1.51	.76	HO	20	1.30	.67	SC	13	1.11	.59
RE	98	1.99	.96	CE	32	1.51	.76	LI	20	1.30	.67	WI	13	1.11	.59
ER	87	1.94	.94	DA	32	1.51	.76	IG	19	1.28	.67	AP	12	1.08	.58
NT	82	1.91	.93	EC	32	1.51	.76	NC	19	1.28	.67	AY	12	1.08	.58
TH	78	1.89	.92	RS	31	1.49	.75	OL	19	1.28	.67	DR	12	1.08	.58
ON	77	1.89	.92	UR	31	1.49	.75	OT	19	1.28	.67	EO	12	1.08	.58
IN	75	1.88	.92	NI	30	1.48	.75	SS	19	1.28	.67	EQ	12	1.08	.58
TE	71	1.85	.91	RI	30	1.48	.75	TS	19	1.28	.67	OD	12	1.08	.58
AN	64	1.81	.89	EL	29	1.46	.74	TT	19	1.28	.67	SF	12	1.08	.58
OR	64	1.81	.89	HT	28	1.45	.74	WO	19	1.28	.67	US	12	1.08	.58
ST	63	1.80	.88	LA	28	1.45	.74	BE	18	1.26	.66	UT	12	1.08	.58
ED	60	1.78	.88	RO	28	1.45	.74	EF	18	1.26	.66	VI	12	1.08	.58
NE	57	1.76	.87	TA	28	1.45	.74	NO	18	1.26	.66	WA	12	1.08	.58
VE	57	1.76	.87		[2]2,495			PR	18	1.26	.66	FF	11	1.04	.56
ES	54	1.73	.86					AI	17	1.23	.64	FT	11	1.04	.56
ND	52	1.72	.85	AD	27	1.43	.73	HR	17	1.23	.64	PP	11	1.04	.56
TO	50	1.70	.84	DI	27	1.43	.73	PO	17	1.23	.64	RR	11	1.04	.56
SE	49	1.69	.84	EI	27	1.43	.73	RD	17	1.23	.64	SU	11	1.04	.56
	[1]1,249			IR	27	1.43	.73	TR	17	1.23	.64	UE	11	1.04	.56
				IT	27	1.43	.73	DO	16	1.20	.63	YF	11	1.04	.56
AT	47	1.67	.83	LL	27	1.43	.73	DT	15	1.18	.62	YS	11	1.04	.56
TI	45	1.65	.82	NG	27	1.43	.73	IX	15	1.18	.62	FE	10	1.00	.55
AR	44	1.64	.82	ME	26	1.41	.72	QU	15	1.18	.62	IF	10	1.00	.55
EE	42	1.62	.81	NA	26	1.41	.72	SO	15	1.18	.62	LY	10	1.00	.55
RT	42	1.62	.81	SH	26	1.41	.72	YT	15	1.18	.62	MO	10	1.00	.55
AS	41	1.61	.80	IV	25	1.40	.72	AC	14	1.15	.61	SP	10	1.00	.55
CO	41	1.61	.80	OF	25	1.40	.72	AM	14	1.15	.61	YO	10	1.00	.55
IO	41	1.61	.80	OM	25	1.40	.72	CH	14	1.15	.61	FR	9	0.95	.53
TY	41	1.61	.80	OP	25	1.40	.72	CT	14	1.15	.61	IM	9	0.95	.53
FO	40	1.60	.80	NS	24	1.38	.71	EM	14	1.15	.61	LD	9	0.95	.53
FI	39	1.59	.80	SA	24	1.38	.71	GE	14	1.15	.61	MI	9	0.95	.53
RA	39	1.59	.80	IL	23	1.36	.70	OS	14	1.15	.61	NF	9	0.95	.53
ET	37	1.57	.79	PE	23	1.36	.70	PA	14	1.15	.61	RC	9	0.95	.53
LE	37	1.57	.79	IC	22	1.34	.69	AU	13	1.11	.59	RM	9	0.95	.53
OU	37	1.57	.79	WE	22	1.34	.69	DS	13	1.11	.59	RY	9	0.95	.53
MA	36	1.56	.78	UN	21	1.32	.68	IE	13	1.11	.59	YE	9	0.95	.53
TW	36	1.56	.78	CA	20	1.30	.67	LO	13	1.11	.59	DD	8	0.90	.51
EA	35	1.54	.78	EP	20	1.30	.67		[3]3,745			DF	8	0.90	.51
IS	35	1.54	.78	EV	20	1.30	.67					HU	8	0.90	.51
SI	34	1.53	.77	GH	20	1.30	.67	MM	13	1.11	.59	IA	8	0.90	.51
DE	33	1.52	.77	HA	20	1.30	.67	PL	13	1.11	.59	LT	8	0.90	.51
HI	33	1.52	.77	HE	20	1.30	.67	RP	13	1.11	.59	MP	8	0.90	.51

[1] The 18 digraphs above this line compose 25 percent of the total.
[2] The 53 digraphs above this line compose 50 percent of the total.
[3] The 117 digraphs above this line compose 75 percent of the total.

Table A-2—*Continued*

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
NN	8	0.90	.51	DP	5	0.70	.42	SW	4	0.60	.38	BR	2	0.30	.25
OC	8	0.90	.51	DU	5	0.70	.42	WH	4	0.60	.38	BU	2	0.30	.25
OW	8	0.90	.51	FA	5	0.70	.42	YC	4	0.60	.38	DG	2	0.30	.25
PT	8	0.90	.51	GI	5	0.70	.42	YD	4	0.60	.38	DH	2	0.30	.25
UG	8	0.90	.51	GR	5	0.70	.42	YR	4	0.60	.38	DQ	2	0.30	.25
AV	7	0.85	.48	HF	5	0.70	.42	AA	3	0.48	.33	FC	2	0.30	.25
BY	7	0.85	.48	NL	5	0.70	.42	AW	3	0.48	.33	FL	2	0.30	.25
CI	7	0.85	.48	NM	5	0.70	.42	CC	3	0.48	.33	GC	2	0.30	.25
EH	7	0.85	.48	NY	5	0.70	.42	DL	3	0.48	.33	GF	2	0.30	.25
EW	7	0.85	.48	OI	5	0.70	.42	DV	3	0.48	.33	GL	2	0.30	.25
EX	7	0.85	.48	RL	5	0.70	.42	EU	3	0.48	.33	GP	2	0.30	.25
GA	7	0.85	.48	RU	5	0.70	.42	FS	3	0.48	.33	GU	2	0.30	.25
IP	7	0.85	.48	RV	5	0.70	.42	FU	3	0.48	.33	HD	2	0.30	.25
NU	7	0.85	.48	SD	5	0.70	.42	GN	3	0.48	.33	HM	2	0.30	.25
OA	7	0.85	.48	SR	5	0.70	.42	GS	3	0.48	.33	IB	2	0.30	.25
OV	7	0.85	.48	TL	5	0.70	.42	HC	3	0.48	.33	IK	2	0.30	.25
RG	7	0.85	.48	TU	5	0.70	.42	HN	3	0.48	.33	IZ	2	0.30	.25
RN	7	0.85	.48	UA	5	0.70	.42	LB	3	0.48	.33	JE	2	0.30	.25
TF	7	0.85	.48	UI	5	0.70	.42	LC	3	0.48	.33	JO	2	0.30	.25
TN	7	0.85	.48	UM	5	0.70	.42	LF	3	0.48	.33	JU	2	0.30	.25
XT	7	0.85	.48	AF	4	0.60	.38	LP	3	0.48	.33	KI	2	0.30	.25
AB	6	0.78	.45	BA	4	0.60	.38	MC	3	0.48	.33	LM	2	0.30	.25
AG	6	0.78	.45	BO	4	0.60	.38	NP	3	0.48	.33	LR	2	0.30	.25
BL	6	0.78	.45	CK	4	0.60	.38	NV	3	0.48	.33	LU	2	0.30	.25
GO	6	0.78	.45	CR	4	0.60	.38	NW	3	0.48	.33	LV	2	0.30	.25
ID	6	0.78	.45	CU	4	0.60	.38	OE	3	0.48	.33	LW	2	0.30	.25
KE	6	0.78	.45	DB	4	0.60	.38	OH	3	0.48	.33	MR	2	0.30	.25
LS	6	0.78	.45	DC	4	0.60	.38	PH	3	0.48	.33	MT	2	0.30	.25
MB	6	0.78	.45	DN	4	0.60	.38	PU	3	0.48	.33	MU	2	0.30	.25
OO	6	0.78	.45	DW	4	0.60	.38	RH	3	0.48	.33	MY	2	0.30	.25
PI	6	0.78	.45	EB	4	0.60	.38	SB	3	0.48	.33	NB	2	0.30	.25
PS	6	0.78	.45	EG	4	0.60	.38	SM	3	0.48	.33	NK	2	0.30	.25
RF	6	0.78	.45	EY	4	0.60	.38	TB	3	0.48	.33	OG	2	0.30	.25
TC	6	0.78	.45	GT	4	0.60	.38	UB	3	0.48	.33	OK	2	0.30	.25
TD	6	0.78	.45	HS	4	0.60	.38	UC	3	0.48	.33	OY	2	0.30	.25
TM	6	0.78	.45	MS	4	0.60	.38	UD	3	0.48	.33	PF	2	0.30	.25
UL	6	0.78	.45	NH	4	0.60	.38	YI	3	0.48	.33	RB	2	0.30	.25
VA	6	0.78	.45	NR	4	0.60	.38	YP	3	0.48	.33	SG	2	0.30	.25
YA	6	0.78	.45	OB	4	0.60	.38	AH	2	0.30	.25	SL	2	0.30	.25
YN	6	0.78	.45	PM	4	0.60	.38	AK	2	0.30	.25	TP	2	0.30	.25
CL	5	0.70	.42	RW	4	0.60	.38	AO	2	0.30	.25	UP	2	0.30	.25
DM	5	0.70	.42	SN	4	0.60	.38	BI	2	0.30	.25	WN	2	0.30	.25

Table A-2—*Continued*

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
XA 2	0.30	.25	FD 1	0.00	.13	LN 1	0.00	.13	UF 1	0.00	.13
XC 2	0.30	.25	FG 1	0.00	.13	MD 1	0.00	.13	UO 1	0.00	.13
XI 2	0.30	.25	FM 1	0.00	.13	MF 1	0.00	.13	UV 1	0.00	.13
XP 2	0.30	.25	FP 1	0.00	.13	MH 1	0.00	.13	VO 1	0.00	.13
YB 2	0.30	.25	FW 1	0.00	.13	NJ 1	0.00	.13	VT 1	0.00	.13
YL 2	0.30	.25	FY 1	0.00	.13	NQ 1	0.00	.13	WL 1	0.00	.13
YM 2	0.30	.25	GD 1	0.00	.13	OJ 1	0.00	.13	WR 1	0.00	.13
ZE 2	0.30	.25	GG 1	0.00	.13	OX 1	0.00	.13	WS 1	0.00	.13
AE 1	0.00	.13	GJ 1	0.00	.13	PB 1	0.00	.13	WY 1	0.00	.13
AJ 1	0.00	.13	GM 1	0.00	.13	PC 1	0.00	.13	XD 1	0.00	.13
BJ 1	0.00	.13	GW 1	0.00	.13	PD 1	0.00	.13	XE 1	0.00	.13
BM 1	0.00	.13	HB 1	0.00	.13	PN 1	0.00	.13	XF 1	0.00	.13
BS 1	0.00	.13	HL 1	0.00	.13	PV 1	0.00	.13	XH 1	0.00	.13
BT 1	0.00	.13	HP 1	0.00	.13	PW 1	0.00	.13	XN 1	0.00	.13
CD 1	0.00	.13	HQ 1	0.00	.13	PY 1	0.00	.13	XO 1	0.00	.13
CF 1	0.00	.13	HW 1	0.00	.13	QM 1	0.00	.13	XR 1	0.00	.13
CM 1	0.00	.13	HY 1	0.00	.13	QR 1	0.00	.13	XS 1	0.00	.13
CN 1	0.00	.13	JA 1	0.00	.13	RJ 1	0.00	.13	YG 1	0.00	.13
CS 1	0.00	.13	KA 1	0.00	.13	RK 1	0.00	.13	YH 1	0.00	.13
CW 1	0.00	.13	KC 1	0.00	.13	SK 1	0.00	.13	YU 1	0.00	.13
CY 1	0.00	.13	KL 1	0.00	.13	SV 1	0.00	.13	YW 1	0.00	.13
DJ 1	0.00	.13	KN 1	0.00	.13	SY 1	0.00	.13	ZA 1	0.00	.13
DY 1	0.00	.13	KS 1	0.00	.13	TG 1	0.00	.13	ZI 1	0.00	.13
EJ 1	0.00	.13	LG 1	0.00	.13	TQ 1	0.00	.13	5,000		
EZ 1	0.00	.13	LH 1	0.00	.13	TZ 1	0.00	.13			

Table A-3. The 18 digraphs composing 25 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters.

(1) ACCORDING TO THEIR INITIAL LETTERS						(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES					
F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
AN........64	1.81	.89	ON........77	1.89	.92	AN........64	1.81	.89	ON........77	1.89	.92
			OR........64	1.81	.89				OR........64	1.81	.89
ED........60	1.78	.88	RE........98	1.99	.96	EN...... 111	2.05	.99	RE........98	1.99	.96
EN...... 111	2.05	.99				ER........87	1.94	.94			
ER........87	1.94	.94	SE........49	1.69	.84	ED........60	1.78	.88	ST........63	1.80	.88
ES........54	1.73	.86	ST........63	1.80	.88	ES........54	1.73	.86	SE........49	1.69	.84
			TE........71	1.85	.91				TH........78	1.89	.92
IN.........75	1.89	.92	TH........78	1.89	.92	IN.........75	1.88	.92	TE........71	1.85	.91
			TO........50	1.70	.84				TO........50	1.70	.84
ND........52	1.72	.85	VE........57	1.76	.87	NT........82	1.91	.93	VE........57	1.76	.87
NE........57	1.76	.87	1,249			NE........57	1.76	.87	1,249		
NT........82	1.91	.93				ND........52	1.72	.85			

Table A-4. The 53 digraphs composing 50 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters.

(1) ACCORDING TO THEIR INITIAL LETTERS						(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES					
F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
AL 32	1.51	.76	MA 36	1.56	.78	AN........64	1.81	.89	MA 36	1.56	.78
AN........64	1.81	.89				AT 47	1.67	.83			
AR 44	1.64	.82	ND........52	1.72	.85	AR 44	1.64	.82	NT........82	1.91	.93
AS 41	1.61	.80	NE........57	1.76	.87	AS 41	1.61	.80	NE........57	1.76	.87
AT 47	1.67	.83	NI.........30	1.48	.75	AL 32	1.51	.76	ND........52	1.72	.85
			NT........82	1.91	.93				NI.........30	1.48	.75
CE 32	1.51	.76				CO 41	1.61	.80			
CO 41	1.61	.80	ON........77	1.89	.92	CE 32	1.51	.76	ON........77	1.89	.92
			OR........64	1.81	.89				OR........64	1.81	.89
DA 32	1.51	.76	OU........37	1.57	.79	DE 33	1.52	.77	OU........37	1.57	.79
DE 33	1.52	.77				DA 32	1.51	.76			
			RA 39	1.59	.80				RE 98	1.99	.96
EA 35	1.54	.78	RE 98	1.99	.96	EN...... 111	2.05	.99	RT 42	1.62	.81
EC 32	1.51	.76	RI 30	1.48	.75	ER 87	1.94	.94	RA 39	1.59	.80
ED 60	1.78	.88	RO 28	1.45	.74	ED 60	1.78	.88	RS 31	1.49	.75
EE 42	1.62	.81	RS 31	1.49	.75	ES 54	1.73	.86	RI 30	1.48	.75
EL 29	1.46	.74	RT 42	1.62	.81	EE 42	1.62	.81	RO 28	1.45	.74
EN...... 111	2.05	.99				ET 37	1.57	.79			
ER 87	1.94	.94	SE 49	1.69	.84	EA 35	1.54	.78	ST 63	1.80	.88
ES 54	1.73	.86	SI..........34	1.53	.77	EC 32	1.51	.76	SE 49	1.69	.84
ET 37	1.57	.79	ST 63	1.80	.88	EL 29	1.46	.74	SI..........34	1.53	.77
FI..........39	1.59	.80	TA 28	1.45	.74	FO 40	1.60	.80	TH........78	1.89	.92
FO 40	1.60	.80	TE 71	1.85	.91	FI..........39	1.59	.80	TE 71	1.85	.91
			TH........78	1.89	.92				TO 50	1.70	.84
HI.........33	1.52	.77	TI 45	1.65	.82	HI.........33	1.52	.77	TI 45	1.65	.82
HT........28	1.45	.74	TO 50	1.70	.84	HT........28	1.45	.74	TY 41	1.61	.80
			TW 36	1.56	.78				TW 36	1.56	.78
IN 75	1.88	.92	TY 41	1.61	.80	IN 75	1.88	.92	TA 28	1.45	.74
IO 41	1.61	.80				IO 41	1.61	.80			
IS..........35	1.54	.78	UR........31	1.49	.75	IS..........35	1.54	.78	UR........31	1.49	.75
LA 28	1.45	.74	VE 57	1.76	.87	LE 37	1.57	.79	VE 57	1.76	.87
LE 37	1.57	.79	2,495			LA 28	1.45	.74	2,495		

Table A-5. The 117 digraphs composing 75 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters.

(1) ACCORDING TO THEIR INITIAL LETTERS											
F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
AC........14	1.15	.61	EP........20	1.30	.67	LL.........27	1.43	.73	RE........98	1.99	.96
AD........27	1.43	.73	ER........87	1.94	.94	LO........13	1.11	.59	RI.........30	1.48	.75
AI.........17	1.23	.64	ES........54	1.73	.86				RO........28	1.45	.74
AL........32	1.51	.76	ET........37	1.57	.79	MA.......36	1.56	.78	RS........31	1.49	.75
AM.......14	1.15	.61	EV........20	1.30	.67	ME.......26	1.41	.72	RT........42	1.62	.81
AN........64	1.81	.89									
AR........44	1.64	.82	FI..........39	1.59	.80	NA........26	1.41	.72	SA........24	1.38	.71
AS........41	1.61	.80	FO........40	1.60	.80	NC........19	1.28	.67	SE........49	1.69	.84
AT........47	1.67	.83				ND........52	1.72	.85	SH........26	1.41	.72
AU........13	1.11	.59	GE........14	1.15	.61	NE........57	1.76	.87	SI..........34	1.53	.77
			GH.......20	1.30	.67	NG........27	1.43	.73	SO........15	1.18	.62
BE........18	1.26	.66				NI.........30	1.48	.75	SS.........19	1.28	.67
			HA........20	1.30	.67	NO........18	1.26	.66	ST........63	1.80	.88
CA........20	1.30	.67	HE........20	1.30	.67	NS........24	1.38	.71			
CE........32	1.51	.76	HI.........33	1.52	.77	NT........82	1.91	.93	TA........28	1.45	.74
CH........14	1.15	.61	HO........20	1.30	.67				TE........ 71	1.85	.91
CO........41	1.61	.80	HR........17	1.23	.64	OF........25	1.40	.72	TH........78	1.89	.92
CT........14	1.15	.61	HT........28	1.45	.74	OL........19	1.28	.67	TI.........45	1.65	.82
						OM.......25	1.40	.72	TO........50	1.70	.84
DA........32	1.51	.76	IC.........22	1.34	.69	ON........77	1.89	.92	TR........17	1.23	.64
DE........33	1.52	.77	IE.........13	1.11	.59	OP........25	1.40	.72	TS........19	1.28	.67
DI.........27	1.43	.73	IG.........19	1.28	.67	OR........64	1.81	.89	TT........19	1.28	.67
DO........16	1.20	.63	IL.........23	1.36	.70	OS........14	1.15	.61	TW.......36	1.56	.78
DS........13	1.11	.59	IN.........75	1.88	.92	OT........19	1.28	.67	TY........41	1.61	.80
DT........15	1.18	.62	IO.........41	1.61	.80	OU........37	1.57	.79			
			IR.........27	1.43	.73				UN........21	1.32	.68
EA........35	1.54	.78	IS..........35	1.54	.78	PA........14	1.15	.61	UR........31	1.49	.75
EC........32	1.51	.76	IT.........27	1.43	.73	PE........23	1.36	.70			
ED........60	1.78	.88	IV.........25	1.40	.72	PO........17	1.23	.64	VE........57	1.76	.87
EE........42	1.62	.81	IX.........15	1.18	.62	PR........18	1.26	.66			
EF........18	1.26	.66							WE.......22	1.34	.69
EI.........27	1.43	.73				QU........15	1.18	.62	WO.......19	1.28	.67
EL........29	1.46	.74	LA........28	1.45	.74						
EM.......14	1.15	.61	LE........37	1.57	.79	RA........39	1.59	.80	YT........15	1.18	.62
EN...... 111	2.05	.99	LI.........20	1.30	.67	RD........17	1.23	.64	3,745		

Table A-5—*Continued*

(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN	64	1.81	.89	EI	27	1.43	.73	LI	20	1.30	.67	RA	39	1.59	.80
AT	47	1.67	.83	EP	20	1.30	.67	LO	13	1.11	.59	RS	31	1.49	.75
AR	44	1.64	.82	EV	20	1.30	.67					RI	30	1.48	.75
AS	41	1.61	.80	EF	18	1.26	.66	MA	36	1.56	.78	RO	28	1.45	.74
AL	32	1.51	.76	EM	14	1.15	.61	ME	26	1.41	.72	RD	17	1.23	.64
AD	27	1.43	.73												
AI	17	1.23	.64	FO	40	1.60	.80	NT	82	1.91	.93	ST	63	1.80	.88
AC	14	1.15	.61	FI	39	1.59	.80	NE	57	1.76	.87	SE	49	1.69	.84
AM	14	1.15	.61					ND	52	1.72	.85	SI	34	1.53	.77
AU	13	1.11	.59	GH	20	1.30	.67	NI	30	1.48	.75	SH	26	1.41	.72
				GE	14	1.15	.61	NG	27	1.43	.73	SA	24	1.38	.71
BE	18	1.26	.66					NA	26	1.41	.72	SS	19	1.28	.67
				HI	33	1.52	.77	NS	24	1.38	.71	SO	15	1.18	.62
CO	41	1.61	.80	HT	28	1.45	.74	NC	19	1.28	.67				
CE	32	1.51	.76	HA	20	1.30	.67	NO	18	1.26	.66	TH	78	1.89	.92
CA	20	1.30	.67	HE	20	1.30	.67					TE	71	1.85	.91
CH	14	1.15	.61	HO	20	1.30	.67	ON	77	1.89	.92	TO	50	1.70	.84
CT	14	1.15	.61	HR	17	1.23	.64	OR	64	1.81	.89	TI	45	1.65	.82
								OU	37	1.57	.79	TY	41	1.61	.80
DE	33	1.52	.77	IN	75	1.88	.92	OF	25	1.40	.72	TW	36	1.56	.78
DA	32	1.51	.76	IO	41	1.61	.80	OM	25	1.40	.72	TA	28	1.45	.74
DI	27	1.43	.73	IS	35	1.54	.78	OP	25	1.40	.72	TS	19	1.28	.67
DO	16	1.20	.63	IR	27	1.43	.73	OL	19	1.28	.67	TT	19	1.28	.67
DT	15	1.18	.62	IT	27	1.43	.73	OT	19	1.28	.67	TR	17	1.23	.64
DS	13	1.11	.59	IV	25	1.40	.72	OS	14	1.15	.61				
				IL	23	1.36	.70					UR	31	1.49	.75
EN	111	2.05	.99	IC	22	1.34	.69	PE	23	1.36	.70	UN	21	1.32	.68
ER	87	1.94	.94	IG	19	1.28	.67	PR	18	1.26	.66				
ED	60	1.78	.88	IX	15	1.18	.62	PO	17	1.23	.64	VE	57	1.76	.87
ES	54	1.73	.86	IE	13	1.11	.59	PA	14	1.15	.61				
EE	42	1.62	.81									WE	22	1.34	.69
ET	37	1.57	.79					QU	15	1.18	.62	WO	19	1.28	.67
EA	35	1.54	.78	LE	37	1.57	.79								
EC	32	1.51	.76	LA	28	1.45	.74	RE	98	1.99	.96	YT	15	1.18	.62
EL	29	1.46	.74	LL	27	1.43	.73	RT	42	1.62	.81		3,745		

Table A-6. The 428 digraphs of Table A-1, arranged in alphabetic order by initial letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
AN........64	1.81	.89	CI.......... 7	0.85	.48	EE........42	1.62	.81	GA......... 7	0.85	.48
AT........47	1.67	.83	CL......... 5	0.70	.42	ET........37	1.57	.79	GO......... 6	0.78	.45
AR........44	1.64	.82	CK......... 4	0.60	.38	EA........35	1.54	.78	GI.......... 5	0.70	.42
AS........41	1.61	.80	CR......... 4	0.60	.38	EC........32	1.51	.76	GR......... 5	0.70	.42
AL........32	1.51	.76	CU......... 4	0.60	.38	EL........29	1.46	.74	GT......... 4	0.60	.38
AD........27	1.43	.73	CC......... 3	0.48	.33	EI.........27	1.43	.73	GN......... 3	0.48	.33
AI.........17	1.23	.64	CD......... 1	0.00	.13	EP........20	1.30	.67	GS......... 3	0.48	.33
AC........14	1.15	.61	CF......... 1	0.00	.13	EV........20	1.30	.67	GC......... 2	0.30	.25
AM.......14	1.15	.61	CM........ 1	0.00	.13	EF........18	1.26	.66	GF......... 2	0.30	.25
AU........13	1.11	.59	CN......... 1	0.00	.13	EM.......14	1.15	.61	GL......... 2	0.30	.25
AP........12	1.08	.58	CS......... 1	0.00	.13	EO........12	1.08	.58	GP......... 2	0.30	.25
AY........12	1.08	.58	CW........ 1	0.00	.13	EQ........12	1.08	.58	GU......... 2	0.30	.25
AV......... 7	0.85	.48	CY......... 1	0.00	.13	EH......... 7	0.85	.48	GD......... 1	0.00	.13
AB......... 6	0.78	.45				EW........ 7	0.85	.48	GG......... 1	0.00	.13
AG......... 6	0.78	.45	DE........33	1.52	.77	EX......... 7	0.85	.48	GJ.......... 1	0.00	.13
AF......... 4	0.60	.38	DA........32	1.51	.76	EB......... 4	0.60	.38	GM........ 1	0.00	.13
AA......... 3	0.48	.33	DI.........27	1.43	.73	EG......... 4	0.60	.38	GW........ 1	0.00	.13
AW........ 3	0.48	.33	DO........16	1.20	.63	EY......... 4	0.60	.38			
AH......... 2	0.30	.25	DT........15	1.18	.62	EU......... 3	0.48	.33	HI.........33	1.52	.77
AK......... 2	0.30	.25	DS........13	1.11	.59	EJ.......... 1	0.00	.13	HT........28	1.45	.74
AO......... 2	0.30	.25	DR........12	1.08	.58	EZ......... 1	0.00	.13	HA........20	1.30	.67
AE......... 1	0.00	.13	DD......... 8	0.90	.51				HE........20	1.30	.67
AJ.......... 1	0.00	.13	DF......... 8	0.90	.51	FO........40	1.60	.80	HO........20	1.30	.67
			DM........ 5	0.70	.42	FI..........39	1.59	.80	HR........17	1.23	.64
BE........18	1.26	.66	DP......... 5	0.70	.42	FF.........11	1.04	.56	HU......... 8	0.90	.51
BY......... 7	0.85	.48	DU......... 5	0.70	.42	FT.........11	1.04	.56	HF......... 5	0.70	.42
BL......... 6	0.78	.45	DB......... 4	0.60	.38	FE........10	1.00	.55	HS......... 4	0.60	.38
BA......... 4	0.60	.38	DC......... 4	0.60	.38	FR......... 9	0.95	.53	HC......... 3	0.48	.33
BO......... 4	0.60	.38	DN......... 4	0.60	.38	FA......... 5	0.70	.42	HN......... 3	0.48	.33
BI.......... 2	0.30	.25	DW........ 4	0.60	.38	FS.......... 3	0.48	.33	HD......... 2	0.30	.25
BR......... 2	0.30	.25	DL......... 3	0.48	.33	FU......... 3	0.48	.33	HM........ 2	0.30	.25
BU......... 2	0.30	.25	DV......... 3	0.48	.33	FC......... 2	0.30	.25	HB......... 1	0.00	.13
BJ.......... 1	0.00	.13	DG......... 2	0.30	.25	FL.......... 2	0.30	.25	HL......... 1	0.00	.13
BM........ 1	0.00	.13	DH......... 2	0.30	.25	FD......... 1	0.00	.13	HP......... 1	0.00	.13
BS......... 1	0.00	.13	DQ......... 2	0.30	.25	FG......... 1	0.00	.13	HQ......... 1	0.00	.13
BT......... 1	0.00	.13	DJ.......... 1	0.00	.13	FM......... 1	0.00	.13	HW........ 1	0.00	.13
			DY......... 1	0.00	.13	FP.......... 1	0.00	.13	HY......... 1	0.00	.13
CO........41	1.61	.80				FW......... 1	0.00	.13			
CE........32	1.51	.76	EN...... 111	2.05	.99	FY......... 1	0.00	.13	IN.........75	1.88	.92
CA........20	1.30	.67	ER........87	1.94	.94				IO.........41	1.61	.80
CH........14	1.15	.61	ED........60	1.78	.88	GH........20	1.30	.67	IS..........35	1.54	.78
CT........14	1.15	.61	ES........54	1.73	.86	GE........14	1.15	.61	IR.........27	1.43	.73

Table A-6—*Continued*

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
IT 27	1.43	.73	LM......... 2	0.30	.25	NH......... 4	0.60	.38	PT 8	0.90	.51
IV 25	1.40	.72	LR 2	0.30	.25	NR......... 4	0.60	.38	PI 6	0.78	.45
IL 23	1.36	.70	LU 2	0.30	.25	NP......... 3	0.48	.33	PS.......... 6	0.78	.45
IC 22	1.34	.69	LV 2	0.30	.25	NV......... 3	0.48	.33	PM......... 4	0.60	.38
IG 19	1.28	.67	LW......... 2	0.30	.25	NW........ 3	0.48	.33	PH......... 3	0.48	.33
IX 15	1.18	.62	LG 1	0.00	.13	NB......... 2	0.30	.25	PU 3	0.48	.33
IE 13	1.11	.59	LH 1	0.00	.13	NK......... 2	0.30	.25	PF.......... 2	0.30	.25
IF..........10	1.00	.55	LN 1	0.00	.13	NJ 1	0.00	.13	PB 1	0.00	.13
IM 9	0.95	.53				NQ......... 1	0.00	.13	PC 1	0.00	.13
IA 8	0.90	.51	MA 36	1.56	.78				PD 1	0.00	.13
IP 7	0.85	.48	ME 26	1.41	.72	ON........77	1.89	.92	PN 1	0.00	.13
ID 6	0.78	.45	MM.......13	1.11	.59	OR........64	1.81	.89	PV 1	0.00	.13
IB 2	0.30	.25	MO 10	1.00	.55	OU........37	1.57	.79	PW......... 1	0.00	.13
IK.......... 2	0.30	.25	MI 9	0.95	.53	OF 25	1.40	.72	PY 1	0.00	.13
IZ 2	0.30	.25	MP......... 8	0.90	.51	OM 25	1.40	.72			
			MB 6	0.78	.45	OP 25	1.40	.72	QU........15	1.18	.62
JE.......... 2	0.30	.25	MS......... 4	0.60	.38	OL 19	1.28	.67	QM 1	0.00	.13
JO.......... 2	0.30	.25	MC 3	0.48	.33	OT 19	1.28	.67	QR......... 1	0.00	.13
JU.......... 2	0.30	.25	MR 2	0.30	.25	OS 14	1.15	.61			
JA.......... 1	0.00	.13	MT 2	0.30	.25	OD........12	1.08	.58	RE 98	1.99	.96
			MU 2	0.30	.25	OC 8	0.90	.51	RT 42	1.62	.81
KE......... 6	0.78	.45	MY 2	0.30	.25	OW 8	0.90	.51	RA 39	1.59	.80
KI.......... 2	0.30	.25	MD 1	0.00	.13	OA......... 7	0.85	.48	RS 31	1.49	.75
KA......... 1	0.00	.13	MF......... 1	0.00	.13	OV......... 7	0.85	.48	RI 30	1.48	.75
KC......... 1	0.00	.13	MH........ 1	0.00	.13	OO......... 6	0.78	.45	RO 28	1.45	.74
KL......... 1	0.00	.13				OI 5	0.70	.42	RD 17	1.23	.64
KN......... 1	0.00	.13				OB......... 4	0.60	.38	RP 13	1.11	.59
KS 1	0.00	.13	NT........82	1.91	.93	OE......... 3	0.48	.33	RR 11	1.04	.56
			NE........57	1.76	.87	OH......... 3	0.48	.33	RC 9	0.95	.53
LE 37	1.57	.79	ND........52	1.72	.85	OG......... 2	0.30	.25	RM 9	0.95	.53
LA 28	1.45	.74	NI 30	1.48	.75	OK......... 2	0.30	.25	RY 9	0.95	.53
LL.........27	1.43	.73	NG........27	1.43	.73	OY 2	0.30	.25	RG 7	0.85	.48
LI 20	1.30	.67	NA........26	1.41	.72	OJ.......... 1	0.00	.13	RN 7	0.85	.48
LO 13	1.11	.59	NS 24	1.38	.71	OX......... 1	0.00	.13	RF 6	0.78	.45
LY 10	1.00	.55	NC........19	1.28	.67				RL 5	0.70	.42
LD 9	0.95	.53	NO........18	1.26	.66				RU 5	0.70	.42
LT 8	0.90	.51	NF......... 9	0.95	.53	PE 23	1.36	.70	RV 5	0.70	.42
LS.......... 6	0.78	.45	NN......... 8	0.90	.51	PR 18	1.26	.66	RW 4	0.60	.38
LB 3	0.48	.33	NU......... 7	0.85	.48	PO 17	1.23	.64	RH......... 3	0.48	.33
LC 3	0.48	.33	NL 5	0.70	.42	PA 14	1.15	.61	RB 2	0.30	.25
LF.......... 3	0.48	.33	NM 5	0.70	.42	PL.........13	1.11	.59	RJ.......... 1	0.00	.13
LP.......... 3	0.48	.33	NY......... 5	0.70	.42	PP.........11	1.04	.56	RK......... 1	0.00	.13

Table A-6—*Continued*

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
ST	63	1.80	.88	TS	19	1.28	.67	UF	1	0.00	.13	XN	1	0.00	.13
SE	49	1.69	.84	TT	19	1.28	.67	UO	1	0.00	.13	XO	1	0.00	.13
SI	34	1.53	.77	TR	17	1.23	.64	UV	1	0.00	.13	XR	1	0.00	.13
SH	26	1.41	.72	TF	7	0.85	.48					XS	1	0.00	.13
SA	24	1.38	.71	TN	7	0.85	.48	VE	57	1.76	.87				
SS	19	1.28	.67	TC	6	0.78	.45	VI	12	1.08	.58	YT	15	1.18	.62
SO	15	1.18	.62	TD	6	0.78	.45	VA	6	0.78	.45	YF	11	1.04	.56
SC	13	1.11	.59	TM	6	0.78	.45	VO	1	0.00	.13	YS	11	1.04	.56
SF	12	1.08	.58	TL	5	0.70	.42	VT	1	0.00	.13	YO	10	1.00	.55
SU	11	1.04	.56	TU	5	0.70	.42					YE	9	0.95	.53
SP	10	1.00	.55	TB	3	0.48	.33	WE	22	1.34	.69	YA	6	0.78	.45
SD	5	0.70	.42	TP	2	0.30	.25	WO	19	1.28	.67	YN	6	0.78	.45
SR	5	0.70	.42	TG	1	0.00	.13	WI	13	1.11	.59	YC	4	0.60	.38
SN	4	0.60	.38	TQ	1	0.00	.13	WA	12	1.08	.58	YD	4	0.60	.38
SW	4	0.60	.38	TZ	1	0.00	.13	WH	4	0.60	.38	YR	4	0.60	.38
SB	3	0.48	.33					WN	2	0.30	.25	YI	3	0.48	.33
SM	3	0.48	.33	UR	31	1.49	.75	WL	1	0.00	.13	YP	3	0.48	.33
SG	2	0.30	.25	UN	21	1.32	.68	WR	1	0.00	.13	YB	2	0.30	.25
SL	2	0.30	.25	US	12	1.08	.58	WS	1	0.00	.13	YL	2	0.30	.25
SK	1	0.00	.13	UT	12	1.08	.58	WY	1	0.00	.13	YM	2	0.30	.25
SV	1	0.00	.13	UE	11	1.04	.56					YG	1	0.00	.13
SY	1	0.00	.13	UG	8	0.90	.51	XT	7	0.85	.48	YH	1	0.00	.13
				UL	6	0.78	.45	XA	2	0.30	.25	YU	1	0.00	.13
TH	78	1.89	.92	UA	5	0.70	.42	XC	2	0.30	.25	YW	1	0.00	.13
TE	71	1.85	.91	UI	5	0.70	.42	XI	2	0.30	.25				
TO	50	1.70	.84	UM	5	0.70	.42	XP	2	0.30	.25				
TI	45	1.65	.82	UB	3	0.48	.33	XD	1	0.00	.13	ZE	2	0.30	.25
TY	41	1.61	.80	UC	3	0.48	.33	XE	1	0.00	.13	ZA	1	0.00	.13
TW	36	1.56	.78	UD	3	0.48	.33	XF	1	0.00	.13	ZI	1	0.00	.13
TA	28	1.45	.74	UP	2	0.30	.25	XH	1	0.00	.13		5,000		

Table A-7. The 428 digraphs of Table A-1, arranged in alphabetic order by final letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
RA	39	1.59	.80	EC	32	1.51	.76	RE	98	1.99	.96	MF	1	0.00	.13
MA	36	1.56	.78	IC	22	1.34	.69	TE	71	1.85	.91	UF	1	0.00	.13
EA	35	1.54	.78	NC	19	1.28	.67	NE	57	1.76	.87	XF	1	0.00	.13
DA	32	1.51	.76	AC	14	1.15	.61	VE	57	1.76	.87				
LA	28	1.45	.74	SC	13	1.11	.59	SE	49	1.69	.84	NG	27	1.43	.73
TA	28	1.45	.74	RC	9	0.95	.53	EE	42	1.62	.81	IG	19	1.28	.67
NA	26	1.41	.72	OC	8	0.90	.51	LE	37	1.57	.79	UG	8	0.90	.51
SA	24	1.38	.71	TC	6	0.78	.45	DE	33	1.52	.77	RG	7	0.85	.48
CA	20	1.30	.67	DC	4	0.60	.38	CE	32	1.51	.76	AG	6	0.78	.45
HA	20	1.30	.67	YC	4	0.60	.38	ME	26	1.41	.72	EG	4	0.60	.38
PA	14	1.15	.61	CC	3	0.48	.33	PE	23	1.36	.70	DG	2	0.30	.25
WA	12	1.08	.58	HC	3	0.48	.33	WE	22	1.34	.69	OG	2	0.30	.25
IA	8	0.90	.51	LC	3	0.48	.33	HE	20	1.30	.67	SG	2	0.30	.25
GA	7	0.85	.48	MC	3	0.48	.33	BE	18	1.26	.66	FG	1	0.00	.13
OA	7	0.85	.48	UC	3	0.48	.33	GE	14	1.15	.61	GG	1	0.00	.13
VA	6	0.78	.45	FC	2	0.30	.25	IE	13	1.11	.59	LG	1	0.00	.13
YA	6	0.78	.45	GC	2	0.30	.25	UE	11	1.04	.56	TG	1	0.00	.13
FA	5	0.70	.42	XC	2	0.30	.25	FE	10	1.00	.55	YG	1	0.00	.13
UA	5	0.70	.42	KC	1	0.00	.13	YE	9	0.95	.53				
BA	4	0.60	.38	PC	1	0.00	.13	KE	6	0.78	.45	TH	78	1.89	.92
AA	3	0.48	.33					OE	3	0.48	.33	SH	26	1.41	.72
XA	2	0.30	.25					JE	2	0.30	.25	GH	20	1.30	.67
JA	1	0.00	.13					ZE	2	0.30	.25	CH	14	1.15	.61
KA	1	0.00	.13	ED	60	1.78	.88	AE	1	0.00	.13	EH	7	0.85	.48
ZA	1	0.00	.13	ND	52	1.72	.85	XE	1	0.00	.13	NH	4	0.60	.38
				AD	27	1.43	.73					WH	4	0.60	.38
				RD	17	1.23	.64	OF	25	1.40	.72	OH	3	0.48	.33
AB	6	0.78	.45	OD	12	1.08	.58	EF	18	1.26	.66	PH	3	0.48	.33
MB	6	0.78	.45	LD	9	0.95	.53	SF	12	1.08	.58	RH	3	0.48	.33
DB	4	0.60	.38	DD	8	0.90	.51	FF	11	1.04	.56	AH	2	0.30	.25
EB	4	0.60	.38	ID	6	0.78	.45	XF	11	1.04	.56	DH	2	0.30	.25
OB	4	0.60	.38	TD	6	0.78	.45	IF	10	1.00	.55	LH	1	0.00	.13
LB	3	0.48	.33	SD	5	0.70	.42	NF	9	0.95	.53	MH	1	0.00	.13
SB	3	0.48	.33	YD	4	0.60	.38	DF	8	0.90	.51	XH	1	0.00	.13
TB	3	0.48	.33	UD	3	0.48	.33	TF	7	0.85	.48	YH	1	0.00	.13
UB	3	0.48	.33	HD	2	0.30	.25	RF	6	0.78	.45				
IB	2	0.30	.25	CD	1	0.00	.13	HF	5	0.70	.42	TI	45	1.65	.82
NB	2	0.30	.25	FD	1	0.00	.13	AF	4	0.60	.38	FI	39	1.59	.80
RB	2	0.30	.25	GD	1	0.00	.13	LF	3	0.48	.33	SI	34	1.53	.77
YB	2	0.30	.25	MD	1	0.00	.13	GF	2	0.30	.25	HI	33	1.52	.77
HB	1	0.00	.13	PD	1	0.00	.13	PF	2	0.30	.25	NI	30	1.48	.75
PB	1	0.00	.13	XD	1	0.00	.13	CF	1	0.00	.13	RI	30	1.48	.75

Table A-7—*Continued*

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
DI.........27	1.43	.73	UL......... 6	0.78	.45	TN......... 7	0.85	.48	SP.........10	1.00	.55
EI.........27	1.43	.73	CL......... 5	0.70	.42	YN......... 6	0.78	.45	MP......... 8	0.90	.51
LI.........20	1.30	.67	NL......... 5	0.70	.42	DN......... 4	0.60	.38	IP......... 7	0.85	.48
AI.........17	1.23	.64	RL......... 5	0.70	.42	SN......... 4	0.60	.38	DP......... 5	0.70	.42
WI.........13	1.11	.59	TL......... 5	0.70	.42	GN......... 3	0.48	.33	LP......... 3	0.48	.33
VI.........12	1.08	.58	DL......... 3	0.48	.33	HN......... 3	0.48	.33	NP......... 3	0.48	.33
MI......... 9	0.95	.53	FL......... 2	0.30	.25	WN......... 2	0.30	.25	YP......... 3	0.48	.33
CI......... 7	0.85	.48	GL......... 2	0.30	.25	CN......... 1	0.00	.13	GP......... 2	0.30	.25
PI......... 6	0.78	.45	SL......... 2	0.30	.25	KN......... 1	0.00	.13	TP......... 2	0.30	.25
GI......... 5	0.70	.42	YL......... 2	0.30	.25	LN......... 1	0.00	.13	UP......... 2	0.30	.25
OI......... 5	0.70	.42	HL......... 1	0.00	.13	PN......... 1	0.00	.13	XP......... 2	0.30	.25
UI......... 5	0.70	.42	KL......... 1	0.00	.13	XN......... 1	0.00	.13	FP......... 1	0.00	.13
YI......... 3	0.48	.33	WL......... 1	0.00	.13				HP......... 1	0.00	.13
BI......... 2	0.30	.25				TO.........50	1.70	.84			
KI......... 2	0.30	.25	OM.........25	1.40	.72	CO.........41	1.61	.80	EQ.........12	1.08	.58
XI......... 2	0.30	.25	AM.........14	1.15	.61	IO.........41	1.61	.80	DQ......... 2	0.30	.25
ZI......... 1	0.00	.13	EM.........14	1.15	.61	FO.........40	1.60	.80	HQ......... 1	0.00	.13
			MM.........13	1.11	.59	RO.........28	1.45	.74	NQ......... 1	0.00	.13
AJ......... 1	0.00	.13	IM......... 9	0.95	.53	HO.........20	1.30	.67	TQ......... 1	0.00	.13
BJ......... 1	0.00	.13	RM......... 9	0.95	.53	WO.........19	1.28	.67			
DJ......... 1	0.00	.13	TM......... 6	0.78	.45	NO.........18	1.26	.66	ER.........87	1.94	.94
EJ......... 1	0.00	.13	DM......... 5	0.70	.42	PO.........17	1.23	.64	OR.........64	1.81	.89
GJ......... 1	0.00	.13	NM......... 5	0.70	.42	DO.........16	1.20	.63	AR.........44	1.64	.82
NJ......... 1	0.00	.13	UM......... 5	0.70	.42	SO.........15	1.18	.62	UR.........31	1.49	.75
OJ......... 1	0.00	.13	PM......... 4	0.60	.38	LO.........13	1.11	.59	IR.........27	1.43	.73
RJ......... 1	0.00	.13	SM......... 3	0.48	.33	EO.........12	1.08	.58	PR.........18	1.26	.66
			HM......... 2	0.30	.25	MO.........10	1.00	.55	HR.........17	1.23	64
CK......... 4	0.60	.38	LM......... 2	0.30	.25	YO.........10	1.00	.55	TR.........17	1.23	.64
AK......... 2	0.30	.25	YM......... 2	0.30	.25	GO......... 6	0.78	.45	DR.........12	1.08	.58
IK......... 2	0.30	.25	BM......... 1	0.00	.13	OO......... 6	0.78	.45	RR.........11	1.04	.56
NK......... 2	0.30	.25	CM......... 1	0.00	.13	BO......... 4	0.60	.38	FR......... 9	0.95	.53
OK......... 2	0.30	.25	FM......... 1	0.00	.13	AO......... 2	0.30	.25	GR......... 5	0.70	.42
RK......... 1	0.00	.13	GM......... 1	0.00	.13	JO......... 2	0.30	.25	SR......... 5	0.70	.42
SK......... 1	0.00	.13	QM......... 1	0.00	.13	UO......... 1	0.00	.13	CR......... 4	0.60	.38
						VO......... 1	0.00	.13	NR......... 4	0.60	.38
AL.........32	1.51	.76	EN...... 111	2.05	.99	XO......... 1	0.00	.13	YR......... 4	0.60	.38
EL.........29	1.46	.74	ON.........77	1.89	.92				BR......... 2	0.30	.25
LL.........27	1.43	.73	IN.........75	1.88	.92	OP.........25	1.40	.72	LR......... 2	0.30	.25
IL.........23	1.36	.70	AN.........64	1.81	.89	EP.........20	1.30	.67	MR......... 2	0.30	.25
OL.........19	1.28	.67	UN.........21	1.32	.68	RP.........13	1.11	.59	QR......... 1	0.00	.13
PL.........13	1.11	.59	NN......... 8	0.90	.51	AP.........12	1.08	.58	WR......... 1	0.00	.13
BL......... 6	0.78	.45	RN......... 7	0.85	.48	PP.........11	1.04	.56	XR......... 1	0.00	.13

Table A-7—*Continued*

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
ES	54	1.73	.86	OT	19	1.28	.67	JU	2	0.30	.25	HW	1	0.00	.13
AS	41	1.61	.80	TT	19	1.28	.67	LU	2	0.30	.25	PW	1	0.00	.13
IS	35	1.54	.78	DT	15	1.18	.62	MU	2	0.30	.25	YW	1	0.00	.13
RS	31	1.49	.75	YT	15	1.18	.62	YU	1	0.00	.13				
NS	24	1.38	.71	CT	14	1.15	.61					IX	15	1.18	.62
SS	19	1.28	.67	UT	12	1.08	.58	IV	25	1.40	.72	EX	7	0.85	.48
TS	19	1.28	.67	FT	11	1.04	.56	EV	20	1.30	.67	OX	1	0.00	.13
OS	14	1.15	.61	LT	8	0.90	.51	AV	7	0.85	.48				
DS	13	1.11	.59	PT	8	0.90	.51	OV	7	0.85	.48	TY	41	1.61	.80
US	12	1.08	.58	XT	7	0.85	.48	RV	5	0.70	.42	AY	12	1.08	.58
YS	11	1.04	.56	GT	4	0.60	.38	DV	3	0.48	.33	LY	10	1.00	.55
LS	6	0.78	.45	MT	2	0.30	.25	NV	3	0.48	.33	RY	9	0.95	.53
PS	6	0.78	.45	BT	1	0.00	.13	LV	2	0.30	.25	BY	7	0.85	.48
HS	4	0.60	.38	VT	1	0.00	.13	PV	1	0.00	.13	NY	5	0.70	.42
MS	4	0.60	.38					SV	1	0.00	.13	EY	4	0.60	.38
FS	3	0.48	.33	OU	37	1.57	.79	UV	1	0.00	.13	MY	2	0.30	.25
GS	3	0.48	.33	QU	15	1.18	.62					OY	2	0.30	.25
BS	1	0.00	.13	AU	13	1.11	.59					CY	1	0.00	.13
CS	1	0.00	.13	SU	11	1.04	.56	TW	36	1.56	.78	DY	1	0.00	.13
KS	1	0.00	.13	HU	8	0.90	.51	OW	8	0.90	.51	FY	1	0.00	.13
WS	1	0.00	.13	NU	7	0.85	.48	EW	7	0.85	.48	HY	1	0.00	.13
XS	1	0.00	.13	DU	5	0.70	.42	DW	4	0.60	.38	PY	1	0.00	.13
				RU	5	0.70	.42	RW	4	0.60	.38	SY	1	0.00	.13
NT	82	1.91	.93	TU	5	0.70	.42	SW	4	0.60	.38	WY	1	0.00	.13
ST	63	1.80	.88	CU	4	0.60	.38	AW	3	0.48	.33				
AT	47	1.67	.83	EU	3	0.48	.33	NW	3	0.48	.33				
RT	42	1.62	.81	FU	3	0.48	.33	LW	2	0.30	.25	IZ	2	0.30	.25
ET	37	1.57	.79	PU	3	0.48	.33	CW	1	0.00	.13	EZ	1	0.00	.13
HT	28	1.45	.74	BU	2	0.30	.25	FW	1	0.00	.13	TZ	1	0.00	.13
IT	27	1.43	.73	GU	2	0.30	.25	GW	1	0.00	.13		5,000		

Table A-8. The 18 digraphs composing 25 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters.

(1) ACCORDING TO THEIR FINAL LETTERS						(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES					
F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
ED........60	1.78	.88	IN.........75	1.88	.92	ED........60	1.78	.88	IN.........75	1.88	.92
ND........52	1.72	.85	ON........77	1.89	.92	ND........52	1.72	.85	AN........64	1.81	.89
NE........57	1.76	.87	TO........50	1.70	.84	RE........98	1.99	.96	TO........50	1.70	.84
RE........98	1.99	.96				TE........71	1.85	.91			
SE........49	1.69	.84	ER........87	1.94	.94	NE........57	1.76	.87	ER........87	1.94	.94
TE........71	1.85	.91	OR........64	1.81	.89	VE........57	1.76	.87	OR........64	1.81	.89
VE........57	1.76	.87				SE........49	1.69	.84			
			ES........54	1.73	.86				ES........54	1.73	.86
TH........78	1.89	.92				TH........78	1.89	.92			
			NT........82	1.91	.93				NT........82	1.91	.93
AN........64	1.81	.89	ST........63	1.80	.88	EN...... 111	2.05	.99	ST........63	1.80	.88
EN...... 111	2.05	.99	1,249			ON........77	1.89	.92	1,249		

Table A-9. The 53 digraphs composing 50 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters.

(1) ACCORDING TO THEIR FINAL LETTERS											
F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
DA........32	1.51	.76	NE........57	1.76	.87	AN........64	1.81	.89	AS........41	1.61	.80
EA........35	1.54	.78	RE........98	1.99	.96	EN...... 111	2.05	.99	ES........54	1.73	.86
LA........28	1.45	.74	SE........49	1.69	.84	IN.........75	1.88	.92	IS..........35	1.54	.78
MA.......36	1.56	.78	TE........71	1.85	.91	ON........77	1.89	.92	RS........31	1.49	.75
RA........39	1.59	.80	VE........57	1.76	.87						
TA........28	1.45	.74							AT........47	1.67	.83
			TH........78	1.89	.92	CO........41	1.61	.80	ET........37	1.57	.79
EC........32	1.51	.76				FO........40	1.60	.80	HT........28	1.45	.74
			FI..........39	1.59	.80	IO.........41	1.61	.80	NT........82	1.91	.93
			HI.........33	1.52	.77	RO........28	1.45	.74	RT........42	1.62	.81
ED........60	1.78	.88	NI.........30	1.48	.75	TO........50	1.70	.84	ST........63	1.80	.88
ND........52	1.72	.85	RI.........30	1.48	.75						
			SI..........34	1.53	.77				OU........37	1.57	.79
			TI.........45	1.65	.82						
CE........32	1.51	.76				AR........44	1.64	.82	TW.......36	1.56	.78
DE........33	1.52	.77				ER........87	1.94	.94			
EE........42	1.62	.81	AL........32	1.51	.76	OR........64	1.81	.89	TY........41	1.61	.80
LE........37	1.57	.79	EL........29	1.46	.74	UR........31	1.49	.75	2,495		

Table A-9—*Continued*

(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
RA 39	1.59	.80	EE 42	1.62	.81	EN...... 111	2.05	.99	ES 54	1.73	.86
MA 36	1.56	.78	LE 37	1.57	.79	ON........77	1.89	.92	AS 41	1.61	.80
EA 35	1.54	.78	DE 33	1.52	.77	IN 75	1.88	.92	IS..........35	1.54	.78
DA 32	1.51	.76	CE 32	1.51	.76	AN........64	1.81	.89	RS 31	1.49	.75
LA 28	1.45	.74									
TA 28	1.45	.74							NT........82	1.91	.93
			TH........78	1.89	.92	TO 50	1.70	.84	ST 63	1.80	.88
EC 32	1.51	.76				CO 41	1.61	.80	AT 47	1.67	.83
						IO 41	1.61	.80	RT 42	1.62	.81
			TI 45	1.65	.82	FO 40	1.60	.80	ET 37	1.57	.79
ED 60	1.78	.88	FI..........39	1.59	.80	RO 28	1.45	.74	HT........28	1.45	.74
ND........52	1.72	.85	SI..........34	1.53	.77						
			HI 33	1.52	.77				OU........37	1.57	.79
RE 98	1.99	.96	NI 30	1.48	.75						
TE 71	1.85	.91	RI 30	1.48	.75	ER 87	1.94	.94	TW 36	1.56	.78
NE........57	1.76	.87				OR........64	1.81	.89			
VE 57	1.76	.87	AL 32	1.51	.76	AR 44	1.64	.82	TY 41	1.61	.80
SE 49	1.69	.84	EL 29	1.46	.74	UR........31	1.49	.75	2,495		

Table A-10. The 117 digraphs composing 75 percent of the digraphs of Table A-1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters.

(1) ACCORDING TO THEIR FINAL LETTERS

F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)	F	L_{10} (F)	L_{224} (2F)
CA........20	1.30	.67	TE........71	1.85	.91	AN........64	1.81	.89	IS..........35	1.54	.78
DA........32	1.51	.76	VE........57	1.76	.87	EN...... 111	2.05	.99	NS........24	1.38	.71
EA........35	1.54	.78	WE.......22	1.34	.69	IN.........75	1.88	.92	OS........14	1.15	.61
HA........20	1.30	.67				ON........77	1.89	.92	RS........31	1.49	.75
LA........28	1.45	.74	EF........18	1.26	.66	UN........21	1.32	.68	SS.........19	1.28	.67
MA.......36	1.56	.78	OF........25	1.40	.72				TS........19	1.28	.67
NA........26	1.41	.72				CO........41	1.61	.80			
PA........14	1.15	.61	IG.........19	1.28	.67	DO........16	1.20	.63			
RA........39	1.59	.80	NG........27	1.43	.73	FO........40	1.60	.80	AT........47	1.67	.83
SA........24	1.38	.71				HO........20	1.30	.67	CT........14	1.15	.61
TA........28	1.45	.74	CH........14	1.15	.61	IO.........41	1.61	.80	DT........15	1.18	.62
			GH........20	1.30	.67	LO........13	1.11	.59	ET........37	1.57	.79
AC........14	1.15	.61	SH........26	1.41	.72	NO........18	1.26	.66	HT........28	1.45	.74
EC........32	1.51	.76	TH........78	1.89	.92	PO........17	1.23	.64	IT.........27	1.43	.73
IC.........22	1.34	.69				RO........28	1.45	.74	NT........82	1.91	.93
NC........19	1.28	.67	AI.........17	1.23	.64	SO........15	1.18	.62	OT........19	1.28	.67
			DI.........27	1.43	.73	TO........50	1.70	.84	RT........42	1.62	.81
AD........27	1.43	.73	EI.........27	1.43	.73	WO.......19	1.28	.67	ST........63	1.80	.88
ED........60	1.78	.88	FI..........39	1.59	.80				TT........19	1.28	.67
ND........52	1.72	.85	HI.........33	1.52	.77	EP........20	1.30	.67	YT........15	1.18	.62
RD........17	1.23	.64	LI.........20	1.30	.67	OP........25	1.40	.72			
			NI.........30	1.48	.75						
BE........18	1.26	.66	RI.........30	1.48	.75	AR........44	1.64	.82	AU........13	1.11	.59
CE........32	1.51	.76	SI..........34	1.53	.77	ER........87	1.94	.94	OU........37	1.57	.79
DE........33	1.52	.77	TI.........45	1.65	.82	HR........17	1.23	.64	QU........15	1.18	.62
EE........42	1.62	.81				IR.........27	1.43	.73			
GE........14	1.15	.61	AL........32	1.51	.76	OR........64	1.81	.89	EV........20	1.30	.67
HE........20	1.30	.67	EL........29	1.46	.74	PR........18	1.26	.66	IV.........25	1.40	.72
IE.........13	1.11	.59	IL.........23	1.36	.70	TR........17	1.23	.64			
LE........37	1.57	.79	LL.........27	1.43	.73	UR........31	1.49	.75	TW.......36	1.56	.78
ME.......26	1.41	.72	OL........19	1.28	.67						
NE........57	1.76	.87							IX.........15	1.18	.62
PE........23	1.36	.70	AM.......14	1.15	.61	AS........41	1.61	.80			
RE........98	1.99	.96	EM.......14	1.15	.61	DS........13	1.11	.59	TY........41	1.61	.80
SE........49	1.69	.84	OM.......25	1.40	.72	ES........54	1.73	.86	3,745		

Table A-10—*Continued*

(2) ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
RA	39	1.59	.80	BE	18	1.26	.66	EN	111	2.05	.99	RS	31	1.49	.75
MA	36	1.56	.78	GE	14	1.15	.61	ON	77	1.89	.92	NS	24	1.38	.71
EA	35	1.54	.78	IE	13	1.11	.59	IN	75	1.88	.92	SS	19	1.28	.67
DA	32	1.51	.76					AN	64	1.81	.89	TS	19	1.28	.67
LA	28	1.45	.74	OF	25	1.40	.72	UN	21	1.32	.68	OS	14	1.15	.61
TA	28	1.45	.74	EF	18	1.26	.66					DS	13	1.11	.59
NA	26	1.41	.72					TO	50	1.70	.84				
SA	24	1.38	.71	NG	27	1.43	.73	CO	41	1.61	.80				
CA	20	1.30	.67	IG	19	1.28	.67	IO	41	1.61	.80	NT	82	1.91	.93
HA	20	1.30	.67					FO	40	1.60	.80	ST	63	1.80	.88
PA	14	1.15	.61	TH	78	1.89	.92	RO	28	1.45	.74	AT	47	1.67	.83
				SH	26	1.41	.72	HO	20	1.30	.67	RT	42	1.62	.81
EC	32	1.51	.76	GH	20	1.30	.67	WO	19	1.28	.67	ET	37	1.57	.79
IC	22	1.34	.69	CH	14	1.15	.61	NO	18	1.26	.66	HT	28	1.45	.74
NC	19	1.28	.67					PO	17	1.23	64	IT	27	1.43	.73
AC	14	1.15	.61	TI	45	1.65	.82	DO	16	1.20	.63	OT	19	1.28	.67
				FI	39	1.59	.80	SO	15	1.18	.62	TT	19	1.28	.67
ED	60	1.78	.88	SI	34	1.53	.77	LO	13	1.11	.59	DT	15	1.18	.62
ND	52	1.72	.85	HI	33	1.52	.77					YT	15	1.18	.62
AD	27	1.43	.73	NI	30	1.48	.75	OP	25	1.40	.72	CT	14	1.15	.61
RD	17	1.23	.64	RI	30	1.48	.75	EP	20	1.30	.67				
				DI	27	1.43	.73					OU	37	1.57	.79
RE	98	1.99	.96	EI	27	1.43	.73					QU	15	1.18	.62
TE	71	1.85	.91	LI	20	1.30	.67	ER	87	1.94	.94	AU	13	1.11	.59
NE	57	1.76	.87	AI	17	1.23	.64	OR	64	1.81	.89				
VE	57	1.76	.87					AR	44	1.64	.82				
SE	49	1.69	.84	AL	32	1.51	.76	UR	31	1.49	.75	IV	25	1.40	.72
EE	42	1.62	.81	EL	29	1.46	.74	IR	27	1.43	.73	EV	20	1.30	.67
LE	37	1.57	.79	LL	27	1.43	.73	PR	18	1.26	.66				
DE	33	1.52	.77	IL	23	1.36	.70	HR	17	1.23	.64	TW	36	1.56	.78
CE	32	1.51	.76	OL	19	1.28	.67	TR	17	1.23	.64				
ME	26	1.41	.72									IX	15	1.18	.62
PE	23	1.36	.70	OM	25	1.40	.72	ES	54	1.73	.86				
WE	22	1.34	.69	AM	14	1.15	.61	AS	41	1.61	.80	TY	41	1.61	.80
HE	20	1.30	.67	EM	14	1.15	.61	IS	35	1.54	.78		3,745		

APPENDIX B

FREQUENCY DISTRIBUTIONS OF ENGLISH TRIGRAPHS

Frequency distributions of English trigraphs appearing in 50,000 letters of government plaintext telegrams.

Table B-1. The 56 trigraphs appearing 100 or more times, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
ENT	569	2.76	.99	TOP	174	2.24	.82	EIG	135	2.13	.79
ION	260	2.41	.88	NTH	171	2.23	.82	FIV	135	2.13	.79
AND	228	2.36	.86	TWE	170	2.23	.82	MEN	131	2.12	.78
ING	226	2.35	.86	TWO	163	2.21	.81	SEV	131	2.12	.78
IVE	225	2.35	.86	ATI	160	2.20	.81	ERS	126	2.10	.78
TIO	221	2.34	.85	THR	158	2.20	.81	UND	125	2.10	.78
FOR	218	2.34	.85	NTY	157	2.20	.81	NET	118	2.07	.77
OUR	211	2.32	.85	HRE	153	2.18	.80	PER	115	2.06	.76
THI	211	2.32	.85	WEN	153	2.18	.80	STA	115	2.06	.76
ONE	210	2.32	.85	FOU	152	2.18	.80	TER	115	2.06	.76
NIN	207	2.32	.85	ORT	146	2.16	.80	EQU	114	2.06	.76
STO	202	2.31	.84	REE	146	2.16	.80	RED	113	2.05	.76
EEN	196	2.29	.84	SIX	146	2.16	.80	TED	112	2.05	.76
GHT	196	2.29	.84	ASH	143	2.16	.80	ERI	109	2.04	.76
INE	192	2.28	.83	DAS	140	2.15	.79	HIR	106	2.03	.75
VEN	190	2.28	.83	IGH	140	2.15	.79	IRT	105	2.02	.75
EVE	177	2.25	.82	ERE	138	2.14	.79	DER	101	2.00	.74
EST	176	2.25	.82	COM	136	2.13	.79	DRE	100	2.00	.74
TEE	174	2.24	.82	ATE	135	2.13	.79				

Table B-2. The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by their first letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
AND	228	2.36	.86	GHT	196	2.29	.84	REE	146	2.16	.80
ATI	160	2.20	.81					RED	113	2.05	.76
ASH	143	2.16	.80	HRE	153	2.18	.80				
ATE	135	2.13	.79	HIR	106	2.03	.75	STO	202	2.31	.84
								SIX	146	2.16	.80
COM	136	2.13	.79	ION	260	2.41	.88	SEV	131	2.12	.78
				ING	226	2.35	.86	STA	115	2.06	.76
DAS	140	2.15	.79	IVE	225	2.35	.86				
DER	101	2.00	.74	INE	192	2.28	.83				
DRE	100	2.00	.74	IGH	140	2.15	.79	TIO	221	2.34	.85
				IRT	105	2.02	.75	THI	211	2.32	.85
ENT	569	2.76	.99					TEE	174	2.24	.82
EEN	196	2.29	.84	MEN	131	2.12	.78	TOP	174	2.24	.82
EVE	177	2.25	.82					TWE	170	2.23	.82
EST	176	2.25	.82	NIN	207	2.32	.85	TWO	162	2.21	.81
ERE	138	2.14	.79	NTH	171	2.23	.82	THR	158	2.20	.81
EIG	135	2.13	.79	NTY	157	2.20	.81	TER	115	2.06	.76
ERS	126	2.10	.78	NET	118	2.07	.77	TED	112	2.05	.76
EQU	114	2.06	.76								
ERI	109	2.04	.76	OUR	211	2.32	.85	UND	125	2.10	.78
				ONE	210	2.32	.85				
FOR	218	2.34	.85	ORT	146	2.16	.80	VEN	190	2.28	.83
FOU	152	2.18	.80								
FIV	135	2.13	.79	PER	115	2.06	.76	WEN	153	2.18	.80

Table B-3. The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by their second letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
DAS	140	2.15	.79	SIX	146	2.16	.80	ERS	126	2.10	.78
				EIG	135	2.13	.79	ERI	109	2.04	.76
EEN	196	2.29	.84	FIV	135	2.13	.79	IRT	105	2.02	.75
VEN	190	2.28	.83	HIR	106	2.03	.75	DRE	100	2.00	.74
TEE	174	2.24	.82								
WEN	153	2.18	.80	ENT	569	2.76	.99				
REE	146	2.16	.80	AND	228	2.36	.86	EST	176	2.25	.82
MEN	131	2.12	.78	ING	226	2.35	.86	ASH	143	2.16	.80
SEV	131	2.12	.78	ONE	210	2.32	.85				
NET	118	2.07	.77	INE	192	2.28	.83				
PER	115	2.06	.76	UND	125	2.10	.78	STO	202	2.31	.84
TER	115	2.06	.76					NTH	171	2.23	.82
RED	113	2.05	.76					ATI	160	2.20	.81
TED	112	2.05	.76	ION	260	2.41	.88	NTY	157	2.20	.81
DER	101	2.00	.74	FOR	218	2.34	.85	ATE	135	2.13	.79
				TOP	174	2.24	.82	STA	115	2.06	.76
IGH	140	2.15	.79	FOU	152	2.18	.80				
				COM	136	2.13	.79	OUR	211	2.32	.85
THI	211	2.32	.85								
GHT	196	2.29	.84	EQU	114	2.06	.76	IVE	225	2.35	.86
THR	158	2.20	.81					EVE	177	2.25	.82
				HRE	153	2.18	.80				
TIO	221	2.34	.85	ORT	146	2.16	.80	TWE	170	2.23	.82
NIN	207	2.32	.85	ERE	138	2.14	.79	TWO	163	2.21	.81

Table B-4. The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by their third letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
STA	115	2.06	.76	THI	211	2.32	.85	TER	115	2.06	.76
				ATI	160	2.20	.81	HIR	106	2.03	.75
AND	228	2.36	.86	ERI	109	2.04	.76	DER	101	2.00	.74
UND	125	2.10	.78								
RED	113	2.05	.76	COM	136	2.13	.79	DAS	140	2.15	.79
TED	112	2.05	.76					ERS	126	2.10	.78
				ION	260	2.41	.88				
IVE	225	2.35	.86	NIN	207	2.32	.85	ENT	569	2.76	.99
ONE	210	2.32	.85	EEN	196	2.29	.84	GHT	196	2.29	.84
INE	192	2.28	.83	VEN	190	2.28	.83	EST	176	2.25	.82
EVE	177	2.25	.82	WEN	153	2.18	.80	ORT	146	2.16	.80
TEE	174	2.24	.82	MEN	131	2.12	.78	NET	118	2.07	.77
TWE	170	2.23	.82					IRT	105	2.02	.75
HRE	153	2.18	.80	TIO	221	2.34	.85				
REE	146	2.16	.80	STO	202	2.31	.84	FOU	152	2.18	.80
ERE	138	2.14	.79	TWO	163	2.21	.81	EQU	114	2.06	.76
ATE	135	2.13	.79								
DRE	100	2.00	.74					FIV	135	2.13	.79
				TOP	174	2.24	.82	SEV	131	2.12	.78
ING	226	2.35	.86								
EIG	135	2.13	.79								
				FOR	218	2.34	.85	SIX	146	2.16	.80
NTH	171	2.23	.82	OUR	211	2.32	.85				
ASH	143	2.16	.80	THR	158	2.20	.81				
IGH	140	2.15	.79	PER	115	2.06	.76	NTY	157	2.20	.81

APPENDIX C

FREQUENCY DISTRIBUTIONS OF ENGLISH TETRAGRAPHS

Frequency distributions of English tetragraphs appearing in 50,000 letters of government plaintext telegrams.

Table C-1. The 54 tetragraphs appearing 50 or more times, arranged by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
TION	218	2.34	.99	THIR	104	2.02	.87	ASHT	64	1.81	.79
EVEN	168	2.23	.95	EENT	102	2.01	.87	HUND	64	1.81	.79
TEEN	163	2.21	.94	REQU	98	1.99	.86	DRED	63	1.80	.79
ENTY	161	2.21	.94	HIRT	97	1.99	.86	RIOD	63	1.80	.79
STOP	154	2.19	.93	COMM	93	1.97	.85	ENTS	62	1.79	.78
NINE	153	2.18	.93	QUES	87	1.94	.84	FFIC	62	1.79	.78
WENT	153	2.18	.93	UEST	87	1.94	.84	IVED	62	1.79	.78
TWEN	152	2.18	.93	EQUE	86	1.93	.84	FROM	59	1.77	.78
THRE	149	2.17	.93	NDRE	77	1.89	.82	IRTY	59	1.77	.78
FOUR	144	2.16	.92	LLAR	71	1.85	.81	RTEE	59	1.77	.78
IGHT	140	2.15	.92	OMMA	71	1.85	.81	UNDR	59	1.77	.78
FIVE	135	2.13	.91	OLLA	70	1.85	.81	NAUG	56	1.75	.77
HREE	134	2.13	.91	VENT	70	1.85	.81	OURT	56	1.75	.77
DASH	132	2.12	.91	DOLL	68	1.83	.80	UGHT	56	1.75	.77
EIGH	132	2.12	.91	LARS	68	1.83	.80	STAT	54	1.73	.76
SEVE	121	2.08	.89	THIS	68	1.83	.80	AUGH	52	1.72	.76
ENTH	114	2.06	.89	PERI	67	1.83	.80	CENT	52	1.72	.76
MENT	111	2.05	.88	ERIO	66	1.82	.80	FICE	50	1.70	.75

Table C-2. The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their first letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
ASHT.........	64	1.81	.79	HREE........	134	2.13	.91	REQU.........	98	1.99	.86
AUGH	52	1.72	.76	HIRT..........	97	1.99	.86	RIOD..........	63	1.80	.79
				HUND........	64	1.81	.79	RTEE.........	59	1.77	.78
COMM	93	1.97	.85								
CENT.........	52	1.72	.76	IGHT	140	2.15	.92	STOP	154	2.19	.93
				IVED..........	62	1.79	.78	SEVE	121	2.08	.89
DASH........	132	2.12	.91	IRTY..........	59	1.77	.78	STAT	54	1.73	.76
DOLL.........	68	1.83	.80								
DRED.........	63	1.80	.79	LLAR	71	1.85	.81	TION	218	2.34	.99
				LARS	68	1.83	.80	TEEN........	163	2.21	.94
EVEN........	168	2.23	.95					TWEN.......	152	2.18	.93
ENTY........	161	2.21	.94	MENT.......	111	2.05	.88	THRE........	149	2.17	.93
EIGH	132	2.12	.91					THIR.........	104	2.02	.87
ENTH	114	2.06	.89	NINE	153	2.18	.93	THIS..........	68	1.83	.80
EENT........	102	2.01	.87	NDRE	77	1.89	.82				
EQUE.........	86	1.93	.84	NAUG	56	1.75	.77	UEST.........	87	1.94	.84
ERIO..........	66	1.82	.80					UNDR	59	1.77	.78
ENTS.........	62	1.79	.78	OMMA	71	1.85	.81	UGHT	56	1.75	.77
				OLLA	70	1.85	.81				
FOUR........	144	2.16	.92	OURT.........	56	1.75	.77				
FIVE	135	2.13	.91					VENT.........	70	1.85	.81
FFIC	62	1.79	.78	PERI	67	1.83	.80				
FROM	59	1.77	.78								
FICE	50	1.70	.75	QUES.........	87	1.94	.84	WENT.......	153	2.18	.93

Table C-3. The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their second letters, and then according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities.

F	L_{10} (F)	L_{244} (F)	F	L_{10} (F)	L_{244} (F)	F	L_{10} (F)	L_{244} (F)
DASH........132	2.12	.91	TION 218	2.34	.99	HREE........134	2.13	.91
LARS 68	1.83	.80	NINE 153	2.18	.93	ERIO.......... 66	1.82	.80
NAUG 56	1.75	.77	FIVE 135	2.13	.91	DRED......... 63	1.80	.79
			EIGH 132	2.12	.91	FROM 59	1.77	.78
NDRE 77	1.89	.82	HIRT.......... 97	1.99	.86	IRTY.......... 59	1.77	.78
			RIOD.......... 63	1.80	.79			
TEEN........163	2.21	.94	FICE 50	1.70	.75			
WENT.......153	2.18	.93				ASHT......... 64	1.81	.79
SEVE 121	2.08	.89	LLAR 71	1.85	.81			
MENT.......111	2.05	.88	OLLA 70	1.85	.81			
EENT........102	2.01	.87				STOP 154	2.19	.93
REQU......... 98	1.99	.86				RTEE......... 59	1.77	.78
UEST 87	1.94	.84	OMMA 71	1.85	.81	STAT 54	1.73	.76
VENT......... 70	1.85	.81						
PERI 67	1.83	.80	ENTY........161	2.21	.94			
CENT......... 52	1.72	.76	ENTH 114	2.06	.89	QUES......... 87	1.94	.84
			ENTS......... 62	1.79	.78	HUND 64	1.81	.79
FFIC 62	1.79	.78	UNDR 59	1.77	.78	OURT......... 56	1.75	.77
						AUGH 52	1.72	.76
IGHT 140	2.15	.92	FOUR........144	2.16	.92			
UGHT 56	1.75	.77	COMM 93	1.97	.85			
			DOLL......... 68	1.83	.80	EVEN........168	2.23	.95
THRE........149	2.17	.93				IVED.......... 62	1.79	.78
THIR.........104	2.02	.87						
THIS.......... 68	1.83	.80	EQUE......... 86	1.93	.84	TWEN.......152	2.18	.93

Table C-4. The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their third letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
LLAR	71	1.85	.81	THIR	104	2.02	.87	REQU	98	1.99	.86
STAT	54	1.73	.76	THIS	68	1.83	.80				
				ERIO	66	1.82	.80	THRE	149	2.17	.93
FICE	50	1.70	.75	FFIC	62	1.79	.78	HIRT	97	1.99	.86
								NDRE	77	1.89	.82
UNDR	59	1.77	.78	OLLA	70	1.85	.81	LARS	68	1.83	.80
				DOLL	68	1.83	.80	PERI	67	1.83	.80
EVEN	168	2.23	.95					OURT	56	1.75	.77
TEEN	163	2.21	.94								
TWEN	152	2.18	.93	COMM	93	1.97	.85	DASH	132	2.12	.91
HREE	134	2.13	.91	OMMA	71	1.85	.81	UEST	87	1.94	.84
QUES	87	1.94	.84								
DRED	63	1.80	.79	NINE	153	2.18	.93	ENTY	161	2.21	.94
IVED	62	1.79	.78	WENT	153	2.18	.93	ENTH	114	2.06	.89
RTEE	59	1.77	.78	MENT	111	2.05	.88	ENTS	62	1.79	.78
				EENT	102	2.01	.87	IRTY	59	1.77	.78
				VENT	70	1.85	.81				
				HUND	64	1.81	.79	FOUR	144	2.16	.92
EIGH	132	2.12	.91	CENT	52	1.72	.76	EQUE	86	1.93	.84
AUGH	52	1.72	.76					NAUG	56	1.75	.77
				TION	218	2.34	.99				
IGHT	140	2.15	.92	STOP	154	2.19	.93				
ASHT	64	1.81	.79	RIOD	63	1.80	.79	FIVE	135	2.13	.91
UGHT	56	1.75	.77	FROM	59	1.77	.78	SEVE	121	2.08	.89

Table C-5. The tetragraphs appearing 50 or more times, arranged in alphabetic order by their fourth letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities.

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
OMMA	71	1.85	.81	DASH	132	2.12	.91	QUES	87	1.94	.84
OLLA	70	1.85	.81	EIGH	132	2.12	.91	LARS	68	1.83	.80
				ENTH	114	2.06	.89	THIS	68	1.83	.80
				AUGH	52	1.72	.76	ENTS	62	1.79	.78
FFIC	62	1.79	.78								
				PERI	67	1.83	.80				
								WENT	153	2.18	.93
HUND	64	1.81	.79	DOLL	68	1.83	.80	IGHT	140	2.15	.92
DRED	63	1.80	.79					MENT	111	2.05	.88
RIOD	63	1.80	.79	COMM	93	1.97	.85	EENT	102	2.01	.87
IVED	62	1.79	.78	FROM	59	1.77	.78	HIRT	97	1.99	.86
								UEST	87	1.94	.84
				TION	218	2.34	.99	VENT	70	1.85	.81
NINE	153	2.18	.93	EVEN	168	2.23	.95	ASHT	64	1.81	.79
THRE	149	2.17	.93	TEEN	163	2.21	.94	OURT	56	1.75	.77
FIVE	135	2.13	.91	TWEN	152	2.18	.93	UGHT	56	1.75	.77
HREE	134	2.13	.91					STAT	54	1.73	.76
SEVE	121	2.08	.89	ERIO	66	1.82	.80	CENT	52	1.72	.76
EQUE	86	1.93	.84								
NDRE	77	1.89	.82	STOP	154	2.19	.93				
RTEE	59	1.77	.78					REQU	98	1.99	.86
FICE	50	1.70	.75	FOUR	144	2.16	.92				
				THIR	104	2.02	.87				
				LLAR	71	1.85	.81	ENTY	161	2.21	.94
NAUG	56	1.75	.77	UNDR	59	1.77	.78	IRTY	59	1.77	.78

APPENDIX D

WORD AND PATTERN TABLES

Table D-1. List of words used in military text arranged alphabetically according to word length.

TWO LETTER WORDS

AM
AN
AS
AT
BE
BN
BY
CO
CP
CQ
DO
EM
GO
HE
HQ
IF
IN
IS
IT
ME
MM
MP
MY
NO
OF
OK
ON
OR
QM
SO
TO
US
WD
WE
WO

THREE LETTER WORDS

ACT
ADD
ADJ
AGE
AGO
AID
AIM
AIR
ALL
AND
ANY
APT
ARC
ARE
ARM
ASK
BAD
BAG
BAR
BID
BIG
BOX
BUT
BUY
CAM
CAN
CAR
CAV
COL
CPL
CUT
CWT
DAY
DID
DIE
DRY
DUE
EAT
ECM
END
EYE
FAR
FEW
FIT
FIX
FOR
GAL
GAS
GEN
GET
GHQ
GOT
GUN
HAD
HAM
HAS
HER
HIM
HIS
HOW
ILL
ITS
JAM
JET
JOB
KEG
LAW
LAY
LET
LOT
LOW
MAJ
MAN
MAT
MAY
MEN
MIX
MOS
NET
NEW
NOT
NOW
OFF
OLD
ONE
OUR
OUT
OWE
OWN
PAR
PAY
PEN
PER
PIN
PUT
PVT
QMC
RED
RID
ROB
RUN
SAM
SAW
SAY
SEA
SEE
SET
SGT
SHE
SIX
SPY
SUM
SUN
TAN
TAX
TEN
THE
TIN
TON
TOO
TOP
TOW
TRY
TUB
TWO
USE
VAT
WAR
WAS
WAY
WET
WGT
WON
YET
YOU

Table D-1—*Continued*

FOUR LETTER WORDS

AIDE
ALFA
ALLY
ALSO
AREA
ARMY
ASIA
AWAY
BACK
BASE
BEEN
BLUE
BODY
BOMB
BOOK
BOTH
BULB
BULK
CALL
CELL
CITY
CODE

COOK
DARK
DASH
DATE
DAYS
DIRT
DOWN
DRAW
DUMP
EACH
EAST
EASY
EDGE
EYES
FALL
FARM
FAST
FEEL
FEET
FELL
FILE
FIRE

FIRM
FIVE
FLAG
FLEE
FLOT
FORM
FOUR
FROM
FULL
FUSE
FUZE
GOLF
GUNS
HALF
HALT
HAND
HARD
HAVE
HEAD
HERD
HERE
HIGH

HILL
HITS
HOLD
HOOK
INTO
ITEM
JOIN
JULY
JUNE
JUST
KEEP
KILO
KIND
KING
LAND
LAST
LATE
LEAD
LEAK
LEFT
LESS
LIEU

LIMA
LINE
LIST
LOAD
LONG
LOOK
LOSS
LOST
LOVE
MADE
MAIM
MAIN
MANY
MASK
MASS
MEAT
MEET
MESS
MIKE
MILE
MINE
MOPP

MORE
MOVE
MULE
NAVY
NEAR
NEXT
NINE
NOON
NOTE
OMIT
ONCE
ONLY
OPEN
ORAL
OVER
PAPA
PARK
PASS
PIPE
PLAN
POST
PUMP

PUSH
RAID
RAIL
RAIN
RANK
REAR
RIOT
ROAD
ROUT
RULE
RUSH
SAID
SAME
SANK
SEEN
SHIP
SHOT
SIDE
SITE
SOME
SOON
STOP

SUNK
TAKE
TALK
TANK
TARE
TASK
TEAM
TENT
TEXT
THAN
THAT
THEM
THEN
THEY
THIS
TIME
TONS
TOOK
TOOL
TOWN
TYPE
UNIT

VARY
VERY
WEAK
WEEK
WELL
WERE
WEST
WHAT
WHEN
WILL
WIRE
WITH
XRAY
YOKE
YOUR
ZERO
ZONE
ZULU

FIVE LETTER WORDS

ABOUT
AFTER
AGAIN
AGENT
ALARM
ALERT
ALIGN
ALINE
ALLOW
ALONG
ALPHA
AMONG
ANNEX
APPLY
APRIL
AREAS
ARMOR
ASSET
AWAIT
AWARD
BANKS

BARGE
BEACH
BEGIN
BEING
BLACK
BLIND
BOATS
BOMBS
BOOTH
BRAVO
BREAK
BRIBE
BROKE
BURST
CANAL
CASES
CAUSE
CEASE
CHECK
CHIEF
CLEAR

CLERK
CLOSE
COAST
COLON
COMMA
CORPS
COUNT
COVER
CREEK
CREST
CROSS
CURVE
DAILY
DECKS
DEFER
DELAY
DELTA
DEPOT
DEPTH
DOCKS
DRAWN

DRESS
DRILL
DRIVE
EAGER
EARLY
EIGHT
ENEMY
ENTER
EQUAL
EQUIP
ERASE
ERROR
ETHER
EVERY
FATAL
FEARS
FERRY
FIELD
FIFTH
FIFTY
FIGHT

FIRES
FIRST
FLANK
FLARE
FLATS
FLEET
FOGGY
FORCE
FORTY
FRESH
FRONT
GATES
GAUGE
GIVEN
GOING
GROUP
GUARD
GUEST
HEAVY
HONOR
HORSE

HOTEL
HOURS
HOUSE
INDIA
ISSUE
JAPAN
JOINT
LARGE
LATER
LEAST
LEAVE
LEVEL
LIGHT
LIMIT
LOCAL
MAJOR
MARCH
METER
MILES
MOTOR
NAVAL

NIGHT
NINTH
NORTH
ORDER
OSCAR
OTHER
PACKS
PAIRS
PARTY
PLACE
PLAIN
PLANS
POINT
PRESS
PRIOR
PROOF
PROVE
QUICK
QUIET
RADIO
RAFTS

RAIDS
RALLY
RANGE
RAPID
REACH
READY
REFER
REPEL
RIDGE
RIGHT
RIGID
RIVER
ROGER
ROMEO
ROUTE
SCALE
SEIZE
SEVEN
SHELL
SHIFT
SHIPS

SHORE
SIEGE
SIGHT
SIXTH
SIXTY
SLOPE
SMALL
SMOKE
SOUTH
SPEED
SPELL
SPLIT
SQUAD
STAFF
STAKE
START
STEEL
SUGAR
TAKEN
TANGO
TANKS

Table D-1—*Continued*

TENTH
THEIR
THERE
THESE
THIRD
THREE
TITLE
TODAY
TOTAL
TRACT
TRAIN
TROOP
TRUCE
TRUCK
UNDER
UNION
UNITS
USUAL
VALOR
VISIT
VITAL
VOCAL
VOICE
WAGON
WEIGH
WHEEL
WHERE
WHICH
WIDTH
WIPED
WOODS
YARDS

SIX LETTER WORDS

ACCEPT
ACCESS
ACROSS
ACTION
ACTIVE
ADJUST
ADVICE
ADVISE
AFFAIR
ALASKA
ALLEGE
ALLIED
ALLIES
ALWAYS
ANIMAL
ANNUAL
ANYWAY
APPEAR
ARABIA
ARMIES
ARMORY
ARREST
ARRIVE
ASSETS
ASSIST
ASSURE
ATTACH
ATTACK
ATTAIN
AUGUST
BANNER
BARBED
BARGES
BATTEN
BATTLE
BEETLE
BEFORE
BETTER
BEYOND
BILLET
BITTER
BODIES
BOMBED
BOMBER
BOTTOM
BRANCH
BREACH
BREEZE
BRIDGE
BROKEN
BUFFER
BUREAU
CANADA
CANCEL
CANNOT
CANVAS
CASUAL
CAUSED
CENTER
CHANGE
CHARGE
CHEESE
CHURCH
CIPHER
CIRCLE
COFFEE
COLORS
COLUMN
COMBAT
COMMIT
COMMON
CONVEY
CONVOY
COURSE
CREDIT
CRISIS
CRITIC
DAMAGE
DEBARK
DECIDE
DECODE
DECREE
DEFEAT
DEFECT
DEFEND
DEGREE
DEPART
DEPEND
DEPLOY
DESERT
DETACH
DETAIL
DEVICE
DEVISE
DIRECT
DIVERT
DIVIDE
DOCTOR
DOLLAR
DOWNED
DRAGON
DRYRUN
DUGOUT
DURING
EFFECT
EFFORT
EIGHTH
EIGHTY
EITHER
ELEVEN
EMBARK
EMPLOY
ENCODE
ENGAGE
ENGINE
ENROLL
ENTIRE
ERASER
ESCORT
EUROPE
EXCEPT
EXCESS
EXCITE
EXPECT
EXPELS
EXPEND
EXTEND
EXTENT
FIERCE
FILING
FINISH
FIRING
FLIGHT
FLYING
FOLLOW
FORCES
FORMAL
FORMED
FOUGHT
FOURTH
FRIDAY
FUTURE
GARAGE
GREASE
GROUND
GUNNER
HALTED
HAMMER
HAPPEN
HARBOR
HELPER
HIGHER
HOURLY
INDEED
INFORM
INLAND
INTEND
INTENT
INVENT
ISLAND
ISSUES
JULIET
KEEPER
KILLED
LADDER
LANDED
LAUNCH
LEADER
LEAGUE
LESSON
LETTER
LINING
LIQUID
LITTER
LITTLE
LOCATE
LOSSES
MANAGE
MANNER
MANUAL
MEAGER
MEDIUM
MEMBER
METHOD
METRIC
MINING
MINUTE
MIRROR
MOBILE
MONDAY
MORALE
MORTAR
MOVING
MURDER
MUZZLE
NAPALM
NAUGHT
NEARER
NINETY
NORMAL
NOTING
NOUGHT
NOVICE
NOZZLE
NUMBER
OCCUPY
OFFEND
OFFICE
OPPOSE
ORDERS
ORIENT
OTHERS
OUTPUT
PANAMA
PARADE
PARLEY
PASSED
PASSES
PATROL
PERIOD
PICKET
PINCER
PISTOL
PLACES
PLANES
POINTS
POISON
POLICE
POSTAL
PREFER
PROMPT
PROPER
PURSUE
QUEBEC
RADIAL
RAIDED
RATION
RAVINE
RECORD
REDUCE
REFILL
REFUGE
REFUSE
REJECT
RELIEF
REMAIN
REMEDY
REPAIR
REPORT
RESCUE
RESIST
RESULT
RESUME
RETIRE
RETURN
REVIEW
RIDING
ROCKET
ROUTED
ROUTES
RUBBER
RUNNER
SALARY
SCHEME
SCHOOL
SCORED
SCREEN
SEAMAN
SEAMEN
SEARCH
SECOND
SECTOR
SECURE
SELECT
SERIAL
SETTLE
SEVERE
SHELLS
SIERRA
SIGNAL
SINGLE
SLIGHT
SPHERE
SPOOLS
SPOONS
STATES
STATUS
STRAFE
STREET
STRESS
STRIPS
SUBMIT
SUDDEN
SUFFER
SUMMER
SUMMIT
SUMMON
SUNDAY
SUNKEN
SUNSET
SUPPLY
SURVEY
SWITCH
SYSTEM
TABLES
TANKER
TARGET
TATTOO
TERROR
THIRTY
THOUGH
THREAT
TRAINS
TRENCH
TROOPS
TURRET
TWELVE
TWENTY
UNABLE
UNITED
UNLESS
VALLEY
VERBAL
VERIFY
VESSEL
VICTIM
VICTOR
VISITS
VISUAL
WEIGHT
WIRING
WITHIN
WOODED
YANKEE
ZIGZAG

Table D-1—*Continued*

SEVEN LETTER WORDS

ABANDON
ABSENCE
ADDRESS
ADVANCE
AGAINST
ALMANAC
AMERICA
AMMETER
ANALYZE
ANOTHER
ANTENNA
APPOINT
APPROVE
ARMORED
ARRANGE
ARRIVAL
ASIATIC
ASSAULT
ATTACKS
ATTEMPT
AVERAGE
AVIATOR
AWKWARD
BAGGAGE
BALLOON
BARRAGE
BATTERY
BATTLES
BEARING
BECAUSE
BEDDING
BETWEEN
BICYCLE
BINDING
BIVOUAC
BOMBARD
BOMBERS
BOMBING
BOYCOTT
BRIBERY
BRIGADE
CALIBER
CALIBRE
CAPTAIN
CAPTIVE
CARRIER

CAVALRY
CENTRAL
CHANGES
CHANNEL
CHARLIE
CHASSIS
CIRCUIT
COASTAL
COLLECT
COLLEGE
COLONEL
COMMAND
COMMEND
COMMENT
COMMUTE
COMPANY
COMPASS
CONCEAL
CONDEMN
CONDUCT
CONFINE
CONTACT
CONTAIN
CONTROL
CORRECT
COUNCIL
COURIER
COVERED
CROSSED
CRUISER
CURRENT
CYCLONE
DAMAGED
DECIDED
DECLARE
DECODED
DEFENSE
DELAYED
DELIVER
DERRICK
DESTROY
DETRAIN
DETRUCK
DEVELOP
DIAGRAM
DISCUSS

DISEASE
DISMISS
DISTILL
DROPPED
EASTERN
ECHELON
ELEMENT
ELEVATE
EMBASSY
ENCODED
ENEMIES
ENFORCE
ENGAGED
ENTENTE
ENTRAIN
ENTRUCK
ENVELOP
EVENING
EXCLUDE
EXPLAIN
EXPRESS
EXTRACT
EXTREME
FALLING
FARTHER
FEDERAL
FIFTEEN
FIGHTER
FILLING
FINDING
FISHING
FITTING
FOGHORN
FORCING
FORGING
FORWARD
FOXTROT
FUELOIL
FURNISH
FURTHER
GASSING
GENERAL
GETTING
GLASSES
GRADUAL
GRENADE

GUARDED
HALTING
HASBEEN
HEADING
HEAVIER
HIGHEST
HOLDING
HORIZON
HOSTILE
HUNDRED
ICEBERG
ILLEGAL
ILLNESS
INCLUDE
INFLICT
INITIAL
INQUIRE
INQUIRY
INSPIRE
INSTALL
INSTANT
INVADED
ISLANDS
ISSUING
JAMMING
JANUARY
JUMPOFF
KITCHEN
KILLING
LANDING
LEADING
LECTURE
LIAISON
LIBRARY
LICENSE
LIFTING
LOADING
LOGICAL
LOOKOUT
MACHINE
MANDATE
MANNING
MAPPING
MARCHED
MARSHAL
MARTIAL

MAXIMUM
MEDICAL
MESSAGE
MESSING
MILITIA
MINIMUM
MISFIRE
MISSILE
MISSING
MISSION
MORNING
NATURAL
NEAREST
NIGHTLY
NOTHING
NUCLEAR
NUMBERS
OBSERVE
OCTOBER
OFFENSE
OFFICER
OMITTED
OPERATE
OPINION
ORDERED
OUTPOST
OUTSIDE
PACIFIC
PACKAGE
PASSAGE
PASSIVE
PATROLS
PAYROLL
PLACING
PLATOON
POUNDER
PRAIRIE
PRECEDE
PREPARE
PRESENT
PRESSED
PRIMARY
PROCEED
PROGRAM
PROMOTE
PROPOSE

PROTECT
PROTEST
PROVOST
PURPOSE
PURSUIT
PUSHING
QUARTER
QUICKLY
RADIATE
RAIDING
RAILWAY
RAINING
RAPIDLY
REACHED
RECEIPT
RECEIVE
RECOVER
RECRUIT
REDUCED
REFUGEE
REGULAR
RELEASE
RELIEVE
REPAIRS
REPLACE
REQUEST
REQUIRE
RESERVE
RESPECT
RESPOND
RETIRED
RETREAT
REVENUE
REVERSE
REVOLVE
ROUTINE
RUNNING
SAILORS
SATISFY
SECRECY
SECTION
SECTORS
SERVICE
SESSION
SETBACK
SEVENTH

SEVENTY
SEVERAL
SHELLED
SHORTLY
SIGNIFY
SIMILAR
SIMPLEX
SINKING
SIXTEEN
SLOPING
SMOKING
SOLDIER
STARTER
STATION
STOPPED
STORAGE
SUCCESS
SUGGEST
SUMMARY
SUNRISE
SUPPORT
SUPPOSE
SURPLUS
SUSPEND
TACTICS
TALKING
TARGETS
TERRAIN
THATTHE
THROUGH
TOBACCO
TONIGHT
TONNAGE
TORPEDO
TRACTOR
TRAFFIC
TRAWLER
TRIGGER
TUESDAY
TWELFTH
UNIFORM
UNKNOWN
UNUSUAL
USELESS
UTILITY
UTILIZE

Table D-1—*Continued*

VACANCY
VARYING
VESSELS
VICTORY
VILLAGE
VISIBLE
VISITOR
WARFARE
WARSHIP
WEATHER
WESTERN
WHETHER
WHISKEY
WINDAGE
WITHOUT
WITHTHE
WITNESS
WOUNDED
WRECKED
WRITTEN

EIGHT LETTER WORDS

ACTIVITY
ACTUALLY
ADJACENT
ADJUTANT
ADVANCED
ADVANCES
ADVISING
ADVISORY
AIRBORNE
AIRCRAFT
AIRFIELD
AIRPLANE
ALTITUDE
AMERICAN
ANALYSIS
ANNOUNCE
ANTITANK
APPARENT
APPEARED
APPROACH
APPROVAL
ARMAMENT
ARRESTED
ASSEMBLE
ASSEMBLY
ASSIGNED
ASSOONAS
ATLANTIC
ATTACKED
ATTEMPTS
AVIATION
BARRACKS
BARRAGES
BATTERED
BATTLING
BESIEGED
BILLETED
BOUNDARY
BREAKING
BUILDING
BULLETIN
BUSINESS
CALAMITY
CAMPAIGN
CANISTER
CAPACITY
CAPTURED
CARELESS
CARRIAGE
CARRIERS
CARRYING
CASUALTY
CAUSEWAY
CEMETERY
CENTERED
CHAPLAIN
CHEMICAL
CIRCULAR
CITATION
CIVILIAN
CLERICAL
CODEBOOK
COMMANDS
COMMENCE
COMMERCE
COMPLETE
COMPOSED
COMPUTER
CONCLUDE
CONCRETE
CONFLICT
CONGRESS
CONTINUE
CONTRACT
CORPORAL
CORRIDOR
COVERING
CRITICAL
CRITIQUE
CROSSING
CRUISERS
DAMAGING
DARKNESS
DAYLIGHT
DECEMBER
DECIPHER
DECISION
DECISIVE
DECLARED
DECREASE
DEDICATE
DEFEATED
DEFECTOR
DEFENDED
DEFENDER
DEFENSES
DEFERRED
DEFINITE
DELAYING
DEMANDED
DEPARTED
DEPLOYED
DEPORTED
DESCRIBE
DESERTED
DESERTER
DESPATCH
DETACHED
DETECTOR
DETONATE
DEVELOPE
DICTATED
DICTATOR
DIMINISH
DIRECTOR
DISARMED
DISASTER
DISLODGE
DISPATCH
DISPERSE
DISTANCE
DISTRESS
DISTRICT
DIVIDING
DIVISION
DOCTRINE
DOMINANT
DRESSING
DRIFTING
EASTERLY
EASTWARD
ECONOMIC
EFFECTED
EIGHTEEN
ELEMENTS
ELEVENTH
ELIGIBLE
EMPLOYEE
EMPLOYER
ENCIPHER
ENCIRCLE
ENFILADE
ENGAGING
ENGINEER
ENLISTED
ENORMOUS
ENROLLED
ENTERING
ENTRENCH
ENVELOPE
EQUALIZE
ESCORTED
ESTIMATE
EUROPEAN
EVACUATE
EXCAVATE
EXCHANGE
EXERCISE
EXPANDED
EXPEDITE
EXPELLED
EXPENDED
EXPENSES
EXTENDED
EXTERIOR
FACTIONS
FATALITY
FEBRUARY
FERRYING
FIGHTERS
FIGHTING
FINISHED
FLANKING
FLEXIBLE
FOOTHOLD
FORENOON
FORTRESS
FOURTEEN
FRONTAGE
FUSELAGE
GARRISON
GROUNDED
GROUPING
GUARDING
HAVEBEEN
HINDERED
HOSPITAL
HOWITZER
IDENTIFY
IGNITION
IMPROPER
IMPROVED
INCIDENT
INDICATE
INDIRECT
INFANTRY
INFECTED
INITIATE
INSECURE
INSIGNIA
INSTRUCT
INTEREST
INTERIOR
INTERNAL
INTRENCH
INVADING
INVASION
INVENTED
JETPLANE
JUNCTION
LANGUAGE
LAUNCHED
LAUNCHER
LATITUDE
LETTERED
LIMITING
LOCATION
LUMINOUS
MAINTAIN
MANDATED
MANEUVER
MARCHING
MARITIME
MATERIAL
MATERIEL
MECHANIC
MEDICINE
MEMORIAL
MERCIFUL
MESSAGES
MIDNIGHT
MILITARY
MISFIRES
MISSIONS
MOBILIZE
MONOPOLY
MOUNTAIN
MOVEMENT
NATIONAL
NAUTICAL
NINETEEN
NORTHERN
NOVEMBER
OBSERVED
OBSERVER
OBSOLETE
OBSTACLE
OCCUPIED
OFFENDED
OFFICERS
OFFICIAL
OPERATOR
OPPOSING
OPPOSITE
ORDINATE
ORDNANCE
OUTBOARD
OUTGUARD
OUTPOSTS
PAINTING
PARALLAX
PARALLEL
PASSPORT
PLANNING
POLITICS
PONTOONS
POSITION
POSITIVE
POSSIBLE
POSTPONE
PREPARED
PRESERVE
PRESSING
PRESSURE
PRINTING
PRIORITY
PRISONER
PROBABLE
PROBABLY
PROGRESS
PROHIBIT
PROTESTS
PROTOCOL
PURPOSES
QUARTERS
RAILHEAD
RAILROAD
RALLYING
RECEIVER
RECORDER
REDCROSS
REENLIST
REGIMENT
REGISTER

Table D-1—*Continued*

REJECTED
REJECTOR
REMEDIES
REMEMBER
REPAIRED
REPEATED
REPEATER
REPELLED
REPLACED
REPORTED
REPULSED
REQUIRED
RESEARCH
RESERVES
RESPECTS
RESTORED
RETIRING
RETURNED
REVIEWED
REVOLVER
RIGOROUS
SABOTAGE
SANITARY
SATURDAY
SCHEDULE
SEABORNE
SEALEVEL
SELECTED
SENTENCE
SENTINEL
SEPARATE
SERGEANT
SHELLING
SHIPPING
SIGHTING
SKIRMISH
SOLDIERS
SOUTHERNS
SPECIFIC
SPOTTING
SQUADRON
STANDARD
STATIONS
STRATEGY
SUFFERED
SUITABLE
SUPERIOR
SUPPLIES
URPRISE
SURROUND
SURVIVED
SUSPENSE
SWEEPING
SWIMMING
TACTICAL
TAXATION
TELEGRAM
TERRIBLE
TERRIFIC
THATHAVE
THIRTEEN
THOUSAND
THURSDAY
TOMORROW
TOTALING
TRAILERS
TRAINING
TRANSFER
TRAVERSE
TRAWLERS
VEHICLES
VICINITY
VIGOROUS
WARSHIPS
WESTERLY
WESTWARD
WINDWARD
WIRELESS
WITHDRAW
WITHDREW

NINE LETTER WORDS

ACCESSORY
ACCOMPANY
ACCORDING
ADDRESSED
ADDRESSES
ADMISSION
ADVANCING
ADVANTAGE
AFTERNOON
AGREEMENT
AIRPLANES
ALLOTMENT
ALLOWANCE
ALTERNATE
AMBULANCE
AMUSEMENT
ANNOUNCED
ANONYMOUS
APPARATUS
APPOINTED
ARBITRARY
ARTILLERY
ASCENSION
ASSAULTED
ASSISTANT
ASSOCIATE
ASSURANCE
ATTACKING
ATTEMPTED
ATTENTION
AUTOMATIC
AVAILABLE
BALLISTIC
BAROMETER
BATTALION
BATTERIES
BEACHHEAD
BEGINNING
BLOCKADED
BOMBARDED
BRIGADIER
BUILDINGS
CABLEGRAM
CAMPAIGNS
CANCELLED
CARTRIDGE
CENTERING
CHALLENGE
CHARACTER
CHAUFFEUR
CHRONICAL
CIGARETTE
CIRCULATE
CIVILIANS
CLEARANCE
COALITION
COLLAPSED
COLLISION
COMBATANT
COMMANDED
COMMANDER
COMMITTEE
COMPANIES
COMPELLED
COMPLETED
CONDEMNED
CONDENSED
CONDITION
CONFERRED
CONFIDENT
CONFLICTS
CONQUERED
CONTINUAL
CONTINUED
CONTINUES
COOPERATE
CORRECTED
CRITICISE
CRITICISM
DEBARKING
DECREASED
DEFECTIVE
DEFENSIVE
DEFICIENT
DEPARTURE
DEPENDENT
DESCRIBED
DESIGNATE
DESTITUTE
DESTROYED
DESTROYER
DETENTION
DETERMINE
DETONATED
DETRAINED
DEVELOPED
DIETITIAN
DIFFERENT
DIFFICULT
DIMENSION
DIRECTION
DIRIGIBLE
DISAPPEAR
DISCUSSED
DISINFECT
DISMISSAL
DISPERSED
DISTRICTS
DIVISIONS
DOMINANCE
DOMINATED
ECHELONED
EFFECTIVE
EFFICIENT
ELABORATE
ELEVATION
ELSEWHERE
EMBASSIES
EMERGENCY
EMPLOYING
ENDURANCE
ENGINEERS
ENLISTING
ENTRAINED
EQUIPMENT
ESTABLISH
ESTIMATED
ESTIMATES
EXCESSIVE
EXCLUSION
EXCLUSIVE
EXECUTIVE
EXERCISES
EXHIBITED
EXPANSION
EXPANSIVE
EXPENSIVE
EXPLOSION
EXPLOSIVE
EXTENDING
EXTENSION
EXTENSIVE
FIFTEENTH
FIREALARM
FORMATION
FORTIFIED
FRONTLINE
GROUPMENT
GYROMETER
HOSTILITY
HURRICANE
IDENTICAL
IMMEDIATE
IMPORTANT
IMPRESSED
INCENTIVE
INCIDENCE
INCIDENTS
INCLINING
INCLUDING
INCLUSIVE
INCREASED
INDEMNITY
INDICATED
INFLATION
INFLICTED
INFLUENCE
INHABITED
INSTANTLY
INTEGRITY
INTENSIVE
INTENTION
INTERCEPT
INTERDICT
INTERFERE
INTERMENT
INTERPOSE
INTERRUPT
INTERVENE
INTERVIEW
INVENTION
IRREGULAR
KILOMETER
LAUNCHING
LIABILITY
LOGISTICS
LONGITUDE
MAINTAINS
MECHANISM
MEMORANDA
MESSENGER
MOTORIZED
MOVEMENTS
MUNITIONS
NAVALBASE
NECESSARY
NECESSITY
NEGLIGENT

Table D-1—*Continued*

NEWSPAPER
NORTHEAST
NORTHERLY
NORTHWARD
NORTHWEST
NUMBERING
OBJECTION
OBJECTIVE
OBTAINING
OCCUPYING
OFFENSIVE
OFFICIALS
OPERATING
OPERATION
OSCILLATE
OUTSKIRTS
PARACHUTE
PARAGRAPH
PARTITION
PASSENGER
PATRIOTIC
PENETRATE
PERMANENT
PERSONNEL
PLACEMENT
POLITICAL
POPULATED
POSITIONS
PRACTICAL
PRECEDING
PREFERRED
PREMATURE
PREPARING
PRESIDENT
PRINCIPAL
PRINCIPLE
PRISONERS
PROCEDURE
PROCEEDED
PROJECTOR
PROMOTION
PROPOSALS
PROTECTED
PROTECTOR
PROTESTED
PROVISION
PROXIMITY
RADIATION
RADIOGRAM
READINESS
REARGUARD
REBELLION
RECEIVING
RECOGNIZE
RECOMMEND
REENFORCE
REFERENCE
REFILLING
REGARDING
REINFORCE
REINSTATE
REMAINDER
REMAINING
REPRESENT
REPRISALS
REQUESTED
REQUIRING
RESOURCES
RESTRAINT
RETENTION
RETURNING
REVIEWING
SCREENING
SEAPLANES
SECRETARY
SEMICOLON
SEMIRIGID
SEPTEMBER
SERIOUSLY
SERVICING
SEVENTEEN
SHELLFIRE
SITUATION
SIXTEENTH
SOUTHEAST
SOUTHWARD
SOUTHWEST
SPEARHEAD
STANDARDS
STATEMENT
STRAGGLER
STRATEGIC
SUBMITTED
SUCCEEDED
SURRENDER
SUSPECTED
SUSPENDED
SUSPICION
TECHNICAL
TECHNIQUE
TELEPHONE
TENTATIVE
TERRITORY
THEREFORE
TRANSPORT
TWENTIETH
UNTENABLE
VARIATION
WATERTANK
WEDNESDAY
WITNESSES
YESTERDAY

TEN LETTER WORDS

ACCEPTABLE
ACCEPTANCE
ACCIDENTAL
ACCORDANCE
ACTIVITIES
ADDITIONAL
AIRCONTROL
AIRSUPPORT
ALLEGIANCE
ALLOCATION
AMBASSADOR
AMMUNITION
ANTICIPATE
APPARENTLY
APPEARANCE
APPROACHED
ARMOREDCAR
ARTIFICIAL
ASPOSSIBLE
ASSEMBLIES
ASSESSMENT
ASSIGNMENT
ASSISTANCE
ATOMICBOMB
ATTACHMENT
ATTAINMENT
ATTEMPTING
AUDIBILITY
AUTOMOBILE
BALLISTICS
BATTLESHIP
BEENNEEDED
BRIDGEHEAD
CAMOUFLAGE
CAPABILITY
CASUALTIES
CENSORSHIP
CENTRALIZE
CIRCUITOUS
COASTGUARD
COLLECTING
COLLECTION
COLLISIONS
COMMANDANT
COMMANDEER
COMMANDING
COMMISSARY
COMMISSION
COMMITMENT
COMMUNIQUE
COMPENSATE
COMPLETELY
COMPRESSED
CONCERNING
CONCESSION
CONCLUSION
CONDITIONS
CONFERENCE
CONFESSION
CONFIDENCE
CONNECTING
CONNECTION
CONSPIRACY
CONSTITUTE
CONTINGENT
CONTINUOUS
CONTRABAND
CONVENIENT
COORDINATE
CORRECTION
CREDENTIAL
CROSSROADS
DEBOUCHING
DECIPHERED
DECORATION
DEDICATION
DEFICIENCY
DEFINITION
DEMOBILIZE
DEPARTMENT
DEPENDABLE
DEPLOYMENT
DEPRESSION
DESIGNATED
DESPATCHED
DESPATCHES
DESTROYERS
DETACHMENT
DETERMINED
DETONATION
DETRAINING
DETRUCKING
DIFFERENCE
DIPLOMATIC
DIRECTIONS
DISCIPLINE
DISCUSSION
DISPATCHED
DISPATCHER
DISPATCHES
DISPERSION
DISTRESSED
DISTRIBUTE
DOMINATION
EFFICIENCY
EIGHTEENTH
ELEMENTARY
EMPLOYMENT
ENCIPHERED
ENCIRCLING
ENEMYTANKS
ENGAGEMENT
ENLISTMENT
ENROLLMENT
ENTERPRISE
ENTRENCHED
ENTRUCKING
EQUIVALENT
ESTIMATION
EVACUATING
EVACUATION
EVALUATION
EXCAVATION
EXCITEMENT
EXHIBITION
EXPEDITING
EXPEDITION
EXPENDABLE
EXPERIENCE
EXPERIMENT

Table D-1—*Continued*

EXPLOSIONS
EXTINGUISH
FACILITIES
FLASHLIGHT
FORMATIONS
FOUNDATION
FOURTEENTH
FRONTLINES
GEOGRAPHIC
GONIOMETER
GOVERNMENT
GYROSCOPIC
HELICOPTER
HYDROMETER
HYGROMETER
ILLITERATE
ILLUMINATE
ILLUSTRATE
IMPASSABLE
IMPOSSIBLE
IMPRESSION
IMPRESSIVE
INCENDIARY
INDICATING
INDICATION
INDIVIDUAL
INFLICTING
INSECURITY
INSPECTION
INSTRUCTED
INSTRUCTOR
INSTRUMENT
INTERNMENT
INVITATION
IRRIGATION
KILOMETERS
LABORATORY
LIEUTENANT
LIMITATION
LOCOMOTIVE
MACHINEGUN
MAINTAINED
MANAGEMENT
MECHANIZED
MEMORANDUM
MILLIMETER
MOTORCYCLE
NATURALIZE
NAVIGATION
NEGLIGENCE
NEWSPAPERS
NINETEENTH
OBJECTIVES
OCCUPATION
ONEHUNDRED
OPERATIONS
OPPOSITION
OVERCOMING
PATROLLING
PERMISSION
PERSISTENT
PHOSPHORUS
POPULATION
POSSESSION
POSTOFFICE
PRECEDENCE
PREFERENCE
PRESCRIBED
PROHIBITED
PROPORTION
PROTECTION
PROVISIONS
QUARANTINE
RECEPTACLE
RECREATION
RECRUITING
REENFORCED
REENLISTED
REGIMENTAL
REGULATION
REINFORCED
RESISTANCE
RESPECTFUL
RESTRICTED
REVOLUTION
SANITATION
SEPARATION
SIGNALLING
SIMILARITY
STATISTICS
SUBMARINES
SUBMISSION
SUBSTITUTE
SUCCESSFUL
SUCCESSIVE
SUFFICIENT
SUPPORTING
SUSPENSION
SUSPICIONS
SUSPICIOUS
THIRTEENTH
THREATENED
TRAJECTORY
TRANSPORTS
TRANSVERSE
TROOPSHIPS
TWENTYFIVE
UNDERSTAND
UNDERSTOOD
UNEXPENDED
UNSUITABLE
VICTORIOUS
VISIBILITY
WILLATTACK
WITHDRAWAL

ELEVEN LETTER WORDS

ACCESSORIES
ACKNOWLEDGE
AERONAUTICS
ALTERNATING
APPLICATION
APPOINTMENT
APPROACHING
APPROPRIATE
APPROXIMATE
ARBITRATION
ARMOREDCARS
ARRANGEMENT
ASSESSMENTS
ASSIGNMENTS
ASSOCIATION
BATTLEFIELD
BATTLESHIPS
BELLIGERENT
BOMBARDMENT
CATASTROPHE
CERTIFICATE
CIRCULATION
COEFFICIENT
COINCIDENCE
COMMUNICATE
COMMUNIQUES
COMPARTMENT
COMPETITION
COMPOSITION
COMPUTATION
CONCEALMENT
CONCENTRATE
CONFINEMENT
CONSTITUTED
CONSUMPTION
CONTINENTAL
CONTROVERSY
COOPERATION
CORPORATION
CORRECTNESS
CREDENTIALS
CUSTOMHOUSE
DEBARKATION
DEMONSTRATE
DESCRIPTION
DESCRIPTIVE
DESIGNATION
DESTRUCTION
DETERIORATE
DEVELOPMENT
DISAPPEARED
DISCONTINUE
DISCREPANCY
DISINFECTED
DISPOSITION
DISTINCTION
DISTINGUISH
DYNAMOMETER
ECHELONMENT
EFFECTIVELY
ELECTRICITY
EMBARKATION
EMPLACEMENT
ENCOUNTERED
ENEMYPLANES
ENFORCEMENT
ENGAGEMENTS
ENGINEERING
ESTABLISHED
ESTIMATEDAT
EXAMINATION
EXPLANATION
EXTENSIVELY
EXTERMINATE
FINGERPRINT
FIRECONTROL
HEAVYBOMBER
HEAVYLOSSES
HOSTILITIES
IMMEDIATELY
IMMIGRATION
IMPEDIMENTA
IMPROVEMENT
INCOMPETENT
INDEPENDENT
INFLAMMABLE
INFORMATION
INSPIRATION
INSTITUTION
INSTRUCTION
INSTRUMENTS
INTELLIGENT
INTERCEPTED
INTERESTING
INTERFERING
INTERPRETER
INTERRUPTED
INTERVENING
INVESTIGATE
LEGISLATION
LIGHTBOMBER
MAINTENANCE
MANUFACTURE
MEASUREMENT
NATIONALISM
NATIONALITY
NAVALATTACK
NAVALBATTLE
NAVALFORCES
NECESSITATE

Table D-1—*Continued*

OBSERVATION
OVERWHELMED
PARENTHESES
PARENTHESIS
PENETRATION
PERFORMANCE
PHILIPPINES
PHOTOGRAPHY
PREARRANGED
PRELIMINARY
PREPARATION
PROGRESSIVE
RADIOACTIVE
RANGEFINDER
REAPPOINTED
RECOGNITION
RECOMMENDED
RECONNOITER
REPLACEMENT
REQUIREMENT
REQUISITION
RESERVATION
RESIGNATION
RESPONSIBLE
RESTRICTION
RETALIATION
RETROACTIVE
SCHOOLHOUSE
SEVENTEENTH
SEVENTYFIVE
SIGNIFICANT
SMOKESCREEN
STRATEGICAL
SUBSISTENCE
SUITABILITY
SUPERIORITY
SURRENDERED
SYNCHRONIZE
TEMPERATURE
THERMOMETER
TOPOGRAPHIC
TRADITIONAL
TRANSFERRED
WITHDRAWING

TWELVE LETTER WORDS

ADVANTAGEOUS
AGRICULTURAL
ANNOUNCEMENT
ANTIAIRCRAFT
ANTICIPATION
BREAKTHROUGH
CANCELLATION
CARELESSNESS
COMMENCEMENT
COMMENDATION
COMMISSIONED
COMMISSIONER
COMPENSATION
COMPLETENESS
CONCENTRATED
CONCILIATION
CONFIDENTIAL
CONFIRMATION
CONFISCATION
CONFORMATION
CONSCRIPTION
CONSIDERABLE
CONSTITUTING
CONSTITUTION
CONSTRUCTION
CONTINUATION
CONVALESCENT
CONVERSATION
COORDINATION
DECENTRALIZE
DECIPHERMENT
DEMONSTRATED
DEPARTMENTAL
DIFFICULTIES
DISORGANIZED
DISPLACEMENT
DISSEMINATED
DISTRIBUTING
DISTRIBUTION
EMPLACEMENTS
ENCIPHERMENT
ENTANGLEMENT
ENTERPRISING
FIGHTERPLANE
GENERALALARM
GENERALSTAFF
GEOGRAPHICAL
HEADQUARTERS
HEAVYBOMBERS
HYDROGRAPHIC
ILLUMINATING
ILLUMINATION
ILLUSTRATION
INAUGURATION
INCOMPETENCE
INEFFICIENCY
INSTRUCTIONS
INTELLIGENCE
INTERCEPTION
INTERDICTION
INTERFERENCE
INTERMEDIATE
INTERRUPTION
INTERVENTION
INTRODUCTION
INTRODUCTORY
IRREGULARITY
LIGHTBOMBERS
MARKSMANSHIP
MEASUREMENTS
MEDIUMBOMBER
MOBILIZATION
NONCOMBATANT
NORTHWESTERN
OBSTRUCTIONS
ORGANIZATION
PREPARATIONS
PREPAREDNESS
PRESERVATION
PRESIDENTIAL
PROCLAMATION
PSYCHROMETER
RADIOSTATION
RECREATIONAL
REENLISTMENT
REGISTRATION
REPLACEMENTS
RESPECTFULLY
ROADJUNCTION
SATISFACTORY
SEARCHLIGHTS
SHARPSHOOTER
SIGNIFICANCE
SIMULTANEOUS
SOUTHWESTERN
SUBSTITUTION
SUCCESSFULLY
TRANSFERRING
TRANSMISSION
TRANSPACIFIC
UNIDENTIFIED
UNITEDSTATES
UNSUCCESSFUL
VERIFICATION
VETERINARIAN

THIRTEEN LETTER WORDS

ACCOMMODATION
APPROXIMATELY
CHRONOLOGICAL
CIRCUMSTANCES
COMMUNICATION
CONCENTRATING
CONCENTRATION
CONGRESSIONAL
CONSIDERATION
CORRESPONDING
COUNTERATTACK
DECENTRALIZED
DEMONSTRATION
DEPENDABILITY
DETERMINATION
DISAPPEARANCE
DISCREPANCIES
DISSEMINATION
DISTINGUISHED
ENTERTAINMENT
ESTABLISHMENT
EXTERMINATION
EXTRAORDINARY
FIGHTERPLANES
IMPRACTICABLE
INDETERMINATE
INSTALLATIONS
INSTANTANEOUS

Table D-1—*Continued*

INTERNATIONAL
INVESTIGATION
MEDIUMBOMBERS
MISCELLANEOUS
PRELIMINARIES
QUALIFICATION
QUARTERMASTER
REAPPOINTMENT
REENFORCEMENT
REIMBURSEMENT
REINFORCEMENT
REINSTATEMENT
REVOLUTIONARY
SPECIFICATION
TRANSATLANTIC

FOURTEEN LETTER WORDS

ADMINISTRATION
ADMINISTRATIVE
CENTRALIZATION
CHARACTERISTIC
CIRCUMSTANTIAL
CLASSIFICATION
CORRESPONDENCE
DEMOBILIZATION
DISCONTINUANCE
DISTINGUISHING
IDENTIFICATION
INTERPRETATION
INVESTIGATIONS
IRREGULARITIES
METEOROLOGICAL
NATURALIZATION
RECOMMENDATION
RECONNAISSANCE
RECONNOITERING
RECONSTRUCTION
REORGANIZATION
REPRESENTATIVE
RESPONSIBILITY
SATISFACTORILY
TRANSPORTATION

Table D-2. List of words used in military text arranged alphabetically in reverse order according to word length.

TWO LETTER WORDS

WD
BE
HE
ME

WE
IF
OF
OK

AM
EM
MM
QM

AN
BN
IN
ON

CO
DO
GO
NO

SO
TO
WO
CP

MP
CQ
HQ
OR

AS
IS
US
AT

IT
BY
MY

THREE LETTER WORDS

SEA
JOB
ROB
TUB
QMC
ARC
BAD
HAD
ADD
RED
AID
BID
DID
RID
OLD

AND
END
SEE
AGE
SHE
THE
DIE
ONE
ARE
USE
DUE
OWE
EYE
OFF
BAG

KEG
BIG
MAJ
ADJ
ASK
GAL
ALL
ILL
COL
CPL
CAM
HAM
JAM
SAM
ECM

AIM
HIM
ARM
SUM
CAN
MAN
TAN
TEN
MEN
PEN
TEN
PIN
TIN
TON
WON

GUN
RUN
SUN
OWN
AGO
TOO
TWO
TOP
GHQ
BAR
CAR
FAR
PAR
WAR
HER

PER
AIR
FOR
OUR
GAS
HAS
WAS
HIS
MOS
ITS
EAT
MAT
VAT
ACT
GET

JET
LET
NET
SET
WET
YET
SGT
WGT
FIT
GOT
LOT
NOT
APT
BUT
CUT

OUT
PUT
PVT
CWT
YOU
CAV
LAW
SAW
FEW
NEW
HOW
LOW
NOW
TOW
TAX

FIX
MIX
SIX
BOX
DAY
LAY
MAY
PAY
SAY
WAY
ANY
SPY
DRY
TRY
BUY

FOUR LETTER WORDS

AREA
ALFA
ASIA
LIMA
PAPA
BULB
BOMB
HEAD
LEAD
LOAD
ROAD
RAID
SAID
HOLD
HAND
LAND
KIND
HARD
HERD
ONCE
MADE
AIDE

SIDE
CODE
FLEE
EDGE
TAKE
MIKE
YOKE
FILE
MILE
MULE
RULE
SAME
TIME
SOME
LINE
MINE
NINE
ZONE
JUNE
PIPE
TYPE
TARE

HERE
WERE
FIRE
WIRE
MORE
BASE
FUSE
DATE
LATE
SITE
NOTE
BLUE
HAVE
FIVE
LOVE
MOVE
FUZE
HALF
GOLF
FLAG
KING
LONG

EACH
HIGH
DASH
PUSH
RUSH
WITH
BOTH
LEAK
WEAK
BACK
WEEK
TALK
BULK
RANK
SANK
TANK
SUNK
BOOK
COOK
HOOK
LOOK
TOOK

DARK
PARK
MASK
TASK
ORAL
FEEL
RAIL
CALL
FALL
CELL
FELL
WELL
HILL
WILL
FULL
TOOL
TEAM
THEM
ITEM
MAIM
FROM
FARM

FIRM
FORM
THAN
PLAN
BEEN
SEEN
THEN
WHEN
OPEN
MAIN
RAIN
JOIN
NOON
SOON
DOWN
TOWN
KILO
ZERO
ALSO
INTO
KEEP

SHIP
DUMP
PUMP
STOP
MOPP
NEAR
REAR
OVER
FOUR
YOUR
EYES
THIS
TONS
GUNS
MASS
PASS
LESS
MESS
LOSS
HITS
DAYS

MEAT
THAT
WHAT
FEET
MEET
LEFT
OMIT
UNIT
HALT
TENT
SHOT
RIOT
FLOT
DIRT
EAST
FAST
LAST
WEST
LIST
LOST
POST

JUST
ROUT
NEXT
TEXT
LIEU
ZULU
DRAW
XRAY
AWAY
BODY
THEY
ALLY
ONLY
JULY
ARMY
MANY
VARY
VERY
EASY
CITY
NAVY

Table D-2—***Continued***

FIVE LETTER WORDS

ALPHA
INDIA
COMMA
DELTA
SQUAD
SPEED
WIPED
RIGID
RAPID
FIELD
BLIND
GUARD
AWARD
THIRD
BRIBE
PLACE
VOICE
FORCE
TRUCE
THREE
RIDGE
SIEGE
RANGE
BARGE
LARGE

GAUGE
STAKE
SMOKE
BROKE
SCALE
TITLE
ALINE
SLOPE
FLARE
THERE
WHERE
SHORE
CEASE
ERASE
THESE
CLOSE
HORSE
CAUSE
HOUSE
ROUTE
ISSUE
LEAVE
DRIVE
PROVE
CURVE

SEIZE
CHIEF
STAFF
PROOF
BEING
GOING
ALONG
AMONG
BEACH
REACH
WHICH
MARCH
WEIGH
FRESH
WIDTH
FIFTH
TENTH
NINTH
BOOTH
DEPTH
NORTH
SOUTH
SIXTH
BREAK
BLACK

CHECK
QUICK
TRUCK
CREEK
FLANK
CLERK
LOCAL
VOCAL
CANAL
FATAL
VITAL
TOTAL
EQUAL
USUAL
NAVAL
WHEEL
STEEL
REPEL
HOTEL
LEVEL
APRIL
SMALL
SHELL
SPELL
DRILL

ALARM
JAPAN
TAKEN
SEVEN
GIVEN
ALIGN
AGAIN
PLAIN
TRAIN
BEGIN
WAGON
UNION
COLON
DRAWN
ROMEO
TANGO
RADIO
BRAVO
EQUIP
TROOP
GROUP
OSCAR
CLEAR
SUGAR
UNDER

ORDER
DEFER
REFER
EAGER
ROGER
ETHER
OTHER
LATER
METER
AFTER
ENTER
RIVER
COVER
THEIR
PRIOR
MAJOR
VALOR
ARMOR
HONOR
ERROR
MOTOR
AREAS
BOMBS
RAIDS

WOODS
YARDS
MILES
FIRES
CASES
GATES
PACKS
DECKS
DOCKS
BANKS
TANKS
PLANS
SHIPS
CORPS
FEARS
PAIRS
HOURS
DRESS
PRESS
CROSS
FLATS
BOATS
RAFTS
UNITS

TRACT
FLEET
QUIET
ASSET
SHIFT
EIGHT
FIGHT
LIGHT
NIGHT
RIGHT
SIGHT
AWAIT
SPLIT
LIMIT
VISIT
AGENT
JOINT
POINT
FRONT
COUNT
DEPOT
START
ALERT
LEAST

COAST
CREST
GUEST
FIRST
BURST
ABOUT
ALLOW
ANNEX
TODAY
DELAY
READY
FOGGY
DAILY
RALLY
APPLY
EARLY
ENEMY
EVERY
FERRY
FIFTY
PARTY
FORTY
SIXTY
HEAVY

SIX LETTER WORDS

CANADA
ARABIA
ALASKA
PANAMA
SIERRA
QUEBEC
METRIC
CRITIC
BOMBED
BARBED
RAIDED
LANDED
WOODED
INDEED
ALLIED
KILLED
FORMED
DOWNED

SCORED
PASSED
CAUSED
UNITED
HALTED
ROUTED
LIQUID
INLAND
ISLAND
DEFEND
OFFEND
DEPEND
EXPEND
INTEND
EXTEND
SECOND
BEYOND
GROUND

METHOD
PERIOD
RECORD
OFFICE
POLICE
ADVICE
DEVICE
NOVICE
FIERCE
REDUCE
PARADE
DECIDE
DIVIDE
DECODE
ENCODE
COFFEE
YANKEE
DECREE

DEGREE
STRAFE
ENGAGE
DAMAGE
MANAGE
GARAGE
BRIDGE
ALLEGE
CHANGE
CHARGE
REFUGE
MORALE
UNABLE
CIRCLE
SINGLE
MOBILE
BEETLE
BATTLE

SETTLE
LITTLE
NOZZLE
MUZZLE
SCHEME
RESUME
ENGINE
RAVINE
EUROPE
SPHERE
SEVERE
RETIRE
ENTIRE
BEFORE
SECURE
ASSURE
FUTURE
GREASE

CHEESE
ADVISE
DEVISE
OPPOSE
COURSE
REFUSE
LOCATE
EXCITE
MINUTE
RESCUE
LEAGUE
PURSUE
ARRIVE
ACTIVE
TWELVE
BREEZE
RELIEF
ZIGZAG

RIDING
FILING
LINING
MINING
FIRING
WIRING
DURING
NOTING
MOVING
FLYING
BREACH
DETACH
ATTACH
BRANCH
TRENCH
LAUNCH
SEARCH
CHURCH

SWITCH
THOUGH
FINISH
EIGHTH
FOURTH
ATTACK
DEBARK
EMBARK
VERBAL
RADIAL
SERIAL
ANIMAL
FORMAL
NORMAL
SIGNAL
POSTAL
MANUAL
ANNUAL

CASUAL
VISUAL
CANCEL
VESSEL
DETAIL
REFILL
ENROLL
SCHOOL
PATROL
PISTOL
SYSTEM
VICTIM
NAPALM
BOTTOM
INFORM
MEDIUM
SEAMAN
SUDDEN

Table D-2—*Continued*

SCREEN
SUNKEN
BROKEN
SEAMEN
HAPPEN
BATTEN
ELEVEN
REMAIN
ATTAIN
WITHIN
COLUMN
DRAGON
RATION
ACTION
COMMON
SUMMON
POISON
LESSON
RETURN
DRYRUN

TATTOO
APPEAR
DOLLAR
MORTAR
RUBBER
MEMBER
BOMBER
NUMBER
PINCER
LEADER
LADDER
MURDER
PREFER
BUFFER
SUFFER
MEAGER
HIGHER
CIPHER
EITHER
TANKER

HAMMER
SUMMER
BANNER
MANNER
GUNNER
RUNNER
KEEPER
HELPER
PROPER
NEARER
ERASER
CENTER
BETTER
LETTER
BITTER
LITTER
AFFAIR
REPAIR
HARBOR

TERROR
MIRROR
SECTOR
VICTOR
DOCTOR
CANVAS
PLACES
FORCES
BARGES
BODIES
ALLIES
ARMIES
TABLES
PLANES
PASSES
LOSSES
STATES
ROUTES
ISSUES

CRISIS
EXPELS
SHELLS
SPOOLS
TRAINS
SPOONS
STRIPS
TROOPS
ORDERS
OTHERS
COLORS
ACCESS
EXCESS
UNLESS
STRESS
ACROSS
ASSETS
VISITS
POINTS

STATUS
ALWAYS
COMBAT
DEFEAT
THREAT
DEFECT
EFFECT
REJECT
SELECT
EXPECT
DIRECT
STREET
TARGET
JULIET
PICKET
ROCKET
BILLET
TURRET
SUNSET

WEIGHT
FLIGHT
SLIGHT
NAUGHT
FOUGHT
NOUGHT
CREDIT
SUBMIT
COMMIT
SUMMIT
RESULT
ORIENT
INTENT
EXTENT
INVENT
CANNOT
ACCEPT
EXCEPT
PROMPT

DEPART
DESERT
DIVERT
ESCORT
EFFORT
REPORT
ARREST
RESIST
ASSIST
AUGUST
ADJUST
DUGOUT
OUTPUT
BUREAU
REVIEW
FOLLOW
FRIDAY
MONDAY
SUNDAY

ANYWAY
REMEDY
VALLEY
PARLEY
CONVEY
SURVEY
VERIFY
SUPPLY
HOURLY
DEPLOY
EMPLOY
CONVOY
OCCUPY
SALARY
ARMORY
NINETY
EIGHTY
TWENTY
THIRTY

SEVEN LETTER WORDS

AMERICA
MILITIA
ANTENNA
ALMANAC
BIVOUAC
TRAFFIC
PACIFIC
ASIATIC
REDUCED
INVADED
DECIDED
DECODED
ENCODED
WOUNDED
GUARDED
PROCEED
ENGAGED
DAMAGED
REACHED
MARCHED
WRECKED
SHELLED
DROPPED
STOPPED

HUNDRED
ORDERED
COVERED
RETIRED
ARMORED
PRESSED
CROSSED
OMITTED
DELAYED
COMMAND
COMMEND
SUSPEND
RESPOND
BOMBARD
AWKWARD
FORWARD
REPLACE
SERVICE
ADVANCE
ABSENCE
ENFORCE
BRIGADE
GRENADE
PRECEDE

OUTSIDE
INCLUDE
EXCLUDE
REFUGEE
WINDAGE
BAGGAGE
PACKAGE
VILLAGE
TONNAGE
AVERAGE
STORAGE
BARRAGE
PASSAGE
MESSAGE
COLLEGE
ARRANGE
WITHTHE
THATTHE
CHARLIE
PRAIRIE
VISIBLE
BICYCLE
MISSILE
HOSTILE

EXTREME
CONFINE
MACHINE
ROUTINE
CYCLONE
WARFARE
DECLARE
PREPARE
CALIBRE
MISFIRE
INSPIRE
REQUIRE
INQUIRE
LECTURE
RELEASE
DISEASE
SUNRISE
LICENSE
DEFENSE
OFFENSE
PROPOSE
SUPPOSE
PURPOSE
REVERSE

BECAUSE
MANDATE
RADIATE
OPERATE
ELEVATE
ENTENTE
PROMOTE
COMMUTE
REVENUE
RELIEVE
RECEIVE
PASSIVE
CAPTIVE
REVOLVE
APPROVE
OBSERVE
RESERVE
UTILIZE
ANALYZE
JUMPOFF
BOMBING
PLACING
FORCING
HEADING

LEADING
LOADING
BEDDING
RAIDING
HOLDING
LANDING
BINDING
FINDING
FORGING
FISHING
PUSHING
NOTHING
TALKING
SINKING
SMOKING
FALLING
FILLING
KILLING
JAMMING
EVENING
RAINING
MANNING
RUNNING
MORNING

SLOPING
MAPPING
BEARING
GASSING
MESSING
MISSING
LIFTING
HALTING
GETTING
FITTING
ISSUING
VARYING
ICEBERG
THROUGH
FURNISH
TWELFTH
SEVENTH
SETBACK
DERRICK
DETRUCK
ENTRUCK
MEDICAL
LOGICAL
CONCEAL

Table D-2—*Continued*

ILLEGAL
MARSHAL
INITIAL
MARTIAL
FEDERAL
GENERAL
SEVERAL
CENTRAL
NATURAL
COASTAL
GRADUAL
UNUSUAL
ARRIVAL
CHANNEL
COLONEL
COUNCIL
FUELOIL
INSTALL
DISTILL
PAYROLL
CONTROL
DIAGRAM
PROGRAM
UNIFORM
MINIMUM

MAXIMUM
HASBEEN
FIFTEEN
SIXTEEN
BETWEEN
KITCHEN
WRITTEN
EXPLAIN
TERRAIN
DETRAIN
ENTRAIN
CONTAIN
CAPTAIN
CONDEMN
ABANDON
OPINION
SESSION
MISSION
STATION
SECTION
ECHELON
BALLOON
PLATOON
LIAISON
HORIZON

EASTERN
WESTERN
FOGHORN
UNKNOWN
TOBACCO
TORPEDO
WARSHIP
DEVELOP
ENVELOP
NUCLEAR
SIMILAR
REGULAR
CALIBER
OCTOBER
OFFICER
POUNDER
TRIGGER
WEATHER
WHETHER
ANOTHER
FARTHER
FURTHER
SOLDIER
CARRIER
COURIER

HEAVIER
TRAWLER
CRUISER
AMMETER
FIGHTER
STARTER
QUARTER
DELIVER
RECOVER
AVIATOR
TRACTOR
VISITOR
TACTICS
ISLANDS
CHANGES
ENEMIES
BATTLES
GLASSES
CHASSIS
ATTACKS
VESSELS
PATROLS
BOMBERS
NUMBERS
REPAIRS

SAILORS
SECTORS
COMPASS
SUCCESS
USELESS
ILLNESS
WITNESS
ADDRESS
EXPRESS
DISMISS
DISCUSS
TARGETS
SURPLUS
RETREAT
EXTRACT
CONTACT
COLLECT
RESPECT
CORRECT
PROTECT
INFLICT
CONDUCT
TONIGHT
CIRCUIT
RECRUIT

PURSUIT
ASSAULT
INSTANT
ELEMENT
COMMENT
CURRENT
PRESENT
APPOINT
FOXTROT
RECEIPT
ATTEMPT
SUPPORT
SUGGEST
HIGHEST
NEAREST
PROTEST
REQUEST
AGAINST
OUTPOST
PROVOST
BOYCOTT
WITHOUT
LOOKOUT
SIMPLEX
TUESDAY

RAILWAY
SECRECY
VACANCY
WHISKEY
SIGNIFY
SATISFY
RAPIDLY
QUICKLY
NIGHTLY
SHORTLY
COMPANY
DESTROY
PRIMARY
SUMMARY
LIBRARY
JANUARY
BRIBERY
BATTERY
INQUIRY
CAVALRY
VICTORY
EMBASSY
UTILITY
SEVENTY

EIGHT LETTER WORDS

INSIGNIA
SPECIFIC
TERRIFIC
ECONOMIC
MECHANIC
ATLANTIC
RAILHEAD
RAILROAD
REPLACED
ADVANCED
DEMANDED
EXPANDED
DEFENDED
OFFENDED
EXPENDED
EXTENDED
GROUNDED
BESIEGED
DETACHED

LAUNCHED
FINISHED
OCCUPIED
ATTACKED
REPELLED
EXPELLED
ENROLLED
DISARMED
ASSIGNED
RETURNED
APPEARED
DECLARED
PREPARED
HINDERED
SUFFERED
CENTERED
BATTERED
LETTERED
REPAIRED

REQUIRED
RESTORED
DEFERRED
CAPTURED
REPULSED
COMPOSED
MANDATED
DEFEATED
REPEATED
DICTATED
EFFECTED
INFECTED
REJECTED
SELECTED
BILLETED
INVENTED
DEPARTED
DESERTED
ESCORTED

DEPORTED
REPORTED
ARRESTED
ENLISTED
SURVIVED
IMPROVED
OBSERVED
REVIEWED
DEPLOYED
AIRFIELD
FOOTHOLD
THOUSAND
SURROUND
STANDARD
OUTBOARD
OUTGUARD
WINDWARD
EASTWARD
WESTWARD

DESCRIBE
ORDNANCE
DISTANCE
COMMENCE
SENTENCE
ANNOUNCE
COMMERCE
ENFILADE
CONCLUDE
LATITUDE
ALTITUDE
EMPLOYEE
CARRIAGE
FUSELAGE
FRONTAGE
SABOTAGE
LANGUAGE
DISLODGE
EXCHANGE

PROBABLE
SUITABLE
ELIGIBLE
TERRIBLE
POSSIBLE
FLEXIBLE
ASSEMBLE
OBSTACLE
ENCIRCLE
SCHEDULE
MARITIME
AIRPLANE
JETPLANE
MEDICINE
DOCTRINE
POSTPONE
SEABORNE
AIRBORNE
DEVELOPE

ENVELOPE
INSECURE
PRESSURE
DECREASE
EXERCISE
SURPRISE
SUSPENSE
DISPERSE
TRAVERSE
DEDICATE
INDICATE
INITIATE
ESTIMATE
ORDINATE
DETONATE
SEPARATE
EVACUATE
EXCAVATE
OBSOLETE

Table D-2—*Continued*

COMPLETE
CONCRETE
EXPEDITE
DEFINITE
OPPOSITE
CONTINUE
CRITIQUE
THATHAVE
DECISIVE
POSITIVE
PRESERVE
EQUALIZE
MOBILIZE
INVADING
DIVIDING
BUILDING
GUARDING
ENGAGING
DAMAGING
MARCHING
BREAKING
FLANKING
TOTALING
SHELLING
BATTLING
SWIMMING
TRAINING
PLANNING
SWEEPING
SHIPPING
GROUPING
ENTERING
COVERING
RETIRING
ADVISING

OPPOSING
DRESSING
PRESSING
CROSSING
DRIFTING
FIGHTING
SIGHTING
LIMITING
PAINTING
PRINTING
SPOTTING
DELAYING
RALLYING
CARRYING
FERRYING
APPROACH
ENTRENCH
INTRENCH
RESEARCH
DESPATCH
DISPATCH
SKIRMISH
DIMINISH
ELEVENTH
ANTITANK
CODEBOOK
CHEMICAL
CLERICAL
TACTICAL
CRITICAL
NAUTICAL
OFFICIAL
MATERIAL
MEMORIAL
NATIONAL

INTERNAL
CORPORAL
HOSPITAL
APPROVAL
MATERIEL
PARALLEL
SENTINEL
SEALEVEL
PROTOCOL
MERCIFUL
TELEGRAM
AMERICAN
EUROPEAN
CIVILIAN
HAVEBEEN
NINETEEN
EIGHTEEN
THIRTEEN
FOURTEEN
CAMPAIGN
CHAPLAIN
MAINTAIN
MOUNTAIN
BULLETIN
INVASION
DECISION
DIVISION
LOCATION
AVIATION
CITATION
TAXATION
JUNCTION
IGNITION
POSITION
FORENOON

SQUADRON
GARRISON
NORTHERN
SOUTHERN
CIRCULAR
DECEMBER
REMEMBER
NOVEMBER
DEFENDER
RECORDER
ENGINEER
TRANSFER
LAUNCHER
DECIPHER
ENCIPHER
PRISONER
IMPROPER
REPEATER
DESERTER
DISASTER
REGISTER
CANISTER
COMPUTER
RECEIVER
REVOLVER
OBSERVER
MANEUVER
EMPLOYER
HOWITZER
CORRIDOR
SUPERIOR
INTERIOR
EXTERIOR
OPERATOR

DICTATOR
DEFECTOR
DEJECTOR
DIRECTOR
DETECTOR
ASSOONAS
POLITICS
COMMANDS
ADVANCES
BARRAGES
MESSAGES
REMEDIES
SUPPLIES
VEHICLES
MISFIRES
DEFENSES
EXPENSES
PURPOSES
RESERVES
ANALYSIS
BARRACKS
MISSIONS
STATIONS
FACTIONS
PONTOONS
WARSHIPS
OFFICERS
SOLDIERS
CARRIERS
TRAILERS
TRAWLERS
CRUISERS
FIGHTERS
QUARTERS

CARELESS
WIRELESS
BUSINESS
DARKNESS
CONGRESS
PROGRESS
FORTRESS
DISTRESS
REDCROSS
RESPECTS
ELEMENTS
ATTEMPTS
PROTESTS
OUTPOSTS
ENORMOUS
LUMINOUS
RIGOROUS
VIGOROUS
CONTRACT
INDIRECT
CONFLICT
DISTRICT
INSTRUCT
AIRCRAFT
DAYLIGHT
MIDNIGHT
PROHIBIT
SERGEANT
DOMINANT
ADJUTANT
ADJACENT
INCIDENT
ARMAMENT
MOVEMENT

REGIMENT
APPARENT
PASSPORT
INTEREST
REENLIST
WITHDRAW
WITHDREW
TOMORROW
PARALLAX
SATURDAY
THURSDAY
CAUSEWAY
IDENTIFY
STRATEGY
PROBABLY
ASSEMBLY
ACTUALLY
MONOPOLY
EASTERLY
WESTERLY
BOUNDARY
MILITARY
SANITARY
FEBRUARY
CEMETERY
ADVISORY
INFANTRY
CAPACITY
FATALITY
CALAMITY
VICINITY
PRIORITY
ACTIVITY
CASUALTY

NINE LETTER WORDS

MEMORANDA
STRATEGIC
AUTOMATIC
PATRIOTIC
BALLISTIC

BEACHHEAD
SPEARHEAD
DESCRIBED
ANNOUNCED
BLOCKADED

SUCCEEDED
PROCEEDED
COMMANDED
SUSPENDED
BOMBARDED

FORTIFIED
CANCELLED
COMPELLED
DETRAINED
ENTRAINED

CONDEMNED
ECHELONED
DEVELOPED
CONQUERED
PREFERRED

CONFERRED
DECREASED
INCREASED
CONDENSED
COLLAPSED

Table D-2—*Continued*

DISPERSED
ADDRESSED
IMPRESSED
DISCUSSED
INDICATED
POPULATED
ESTIMATED
DOMINATED
DETONATED
SUSPECTED
CORRECTED
PROTECTED
INFLICTED
COMPLETED
INHABITED
EXHIBITED
ASSAULTED
APPOINTED
ATTEMPTED
PROTESTED
REQUESTED
SUBMITTED
CONTINUED
DESTROYED
MOTORIZED
SEMIRIGID
RECOMMEND
REARGUARD
NORTHWARD
SOUTHWARD
AMBULANCE
DOMINANCE
CLEARANCE
ENDURANCE
ASSURANCE
ALLOWANCE
INCIDENCE
REFERENCE
INFLUENCE
REENFORCE
REINFORCE
LONGITUDE
COMMITTEE
ADVANTAGE
CARTRIDGE
CHALLENGE
AVAILABLE

UNTENABLE
DIRIGIBLE
PRINCIPLE
HURRICANE
INTERVENE
FRONTLINE
DETERMINE
TELEPHONE
INTERFERE
ELSEWHERE
SHELLFIRE
THEREFORE
PROCEDURE
PREMATURE
DEPARTURE
NAVALBASE
CRITICISE
INTERPOSE
ASSOCIATE
IMMEDIATE
OSCILLATE
CIRCULATE
DESIGNATE
ALTERNATE
COOPERATE
ELABORATE
PENETRATE
REINSTATE
CIGARETTE
PARACHUTE
DESTITUTE
TECHNIQUE
EXPANSIVE
DEFENSIVE
OFFENSIVE
EXPENSIVE
INTENSIVE
EXTENSIVE
EXPLOSIVE
EXCESSIVE
INCLUSIVE
EXCLUSIVE
TENTATIVE
DEFECTIVE
EFFECTIVE
OBJECTIVE
INCENTIVE

EXECUTIVE
RECOGNIZE
SERVICING
ADVANCING
PRECEDING
EXTENDING
REGARDING
ACCORDING
INCLUDING
LAUNCHING
ATTACKING
DEBARKING
REFILLING
SCREENING
REMAINING
OBTAINING
INCLINING
BEGINNING
RETURNING
PREPARING
NUMBERING
CENTERING
REQUIRING
OPERATING
ENLISTING
RECEIVING
REVIEWING
EMPLOYING
OCCUPYING
PARAGRAPH
ESTABLISH
TWENTIETH
FIFTEENTH
SIXTEENTH
WATERTANK
TECHNICAL
CHRONICAL
PRACTICAL
POLITICAL
IDENTICAL
PRINCIPAL
DISMISSAL
CONTINUAL
PERSONNEL
CABLEGRAM
RADIOGRAM
FIREALARM

CRITICISM
MECHANISM
DIETITIAN
SEVENTEEN
SUSPICION
BATTALION
REBELLION
COLLISION
PROVISION
EXPANSION
ASCENSION
DIMENSION
EXTENSION
EXPLOSION
ADMISSION
EXCLUSION
RADIATION
VARIATION
INFLATION
FORMATION
OPERATION
SITUATION
ELEVATION
OBJECTION
DIRECTION
CONDITION
COALITION
PARTITION
DETENTION
RETENTION
INTENTION
ATTENTION
INVENTION
PROMOTION
SEMICOLON
AFTERNOON
DISAPPEAR
IRREGULAR
SEPTEMBER
COMMANDER
SURRENDER
REMAINDER
PASSENGER
MESSENGER
BRIGADIER
STRAGGLER
NEWSPAPER

CHARACTER
KILOMETER
BAROMETER
GYROMETER
DESTROYER
PROJECTOR
PROTECTOR
CHAUFFEUR
LOGISTICS
STANDARDS
RESOURCES
COMPANIES
BATTERIES
EMBASSIES
SEAPLANES
AIRPLANES
EXERCISES
WITNESSES
ADDRESSES
ESTIMATES
CONTINUES
BUILDINGS
OFFICIALS
REPRISALS
PROPOSALS
CIVILIANS
CAMPAIGNS
MAINTAINS
DIVISIONS
MUNITIONS
POSITIONS
ENGINEERS
PRISONERS
READINESS
CONFLICTS
DISTRICTS
INCIDENTS
MOVEMENTS
OUTSKIRTS
ANONYMOUS
APPARATUS
DISINFECT
INTERDICT
DIFFICULT
COMBATANT
IMPORTANT

ASSISTANT
CONFIDENT
PRESIDENT
DEPENDENT
NEGLIGENT
DEFICIENT
EFFICIENT
PLACEMENT
AGREEMENT
AMUSEMENT
STATEMENT
EQUIPMENT
GROUPMENT
INTERMENT
ALLOTMENT
PERMANENT
DIFFERENT
REPRESENT
RESTRAINT
INTERCEPT
INTERRUPT
TRANSPORT
NORTHEAST
SOUTHEAST
NORTHWEST
SOUTHWEST
INTERVIEW
YESTERDAY
WEDNESDAY
EMERGENCY
NORTHERLY
SERIOUSLY
INSTANTLY
ACCOMPANY
ARBITRARY
NECESSARY
SECRETARY
ARTILLERY
ACCESSORY
TERRITORY
LIABILITY
HOSTILITY
PROXIMITY
INDEMNITY
INTEGRITY
NECESSITY

Table D-2—*Continued*

TEN LETTER WORDS

ATOMICBOMB
GEOGRAPHIC
GYROSCOPIC
DIPLOMATIC
BRIDGEHEAD
PRESCRIBED
REENFORCED
REINFORCED
BEENNEEDED
UNEXPENDED
APPROACHED
ENTRENCHED
DESPATCHED
DISPATCHED
THREATENED
MAINTAINED
DETERMINED
ONEHUNDRED
DECIPHERED
ENCIPHERED
COMPRESSED
DISTRESSED
DESIGNATED
RESTRICTED
INSTRUCTED
PROHIBITED
REENLISTED
MECHANIZED
CONTRABAND
UNDERSTAND
UNDERSTOOD
COASTGUARD
POSTOFFICE
ACCORDANCE
ALLEGIANCE
APPEARANCE
ACCEPTANCE
RESISTANCE
ASSISTANCE
PRECEDENCE
CONFIDENCE
NEGLIGENCE
EXPERIENCE
PREFERENCE
DIFFERENCE

CONFERENCE
CAMOUFLAGE
DEPENDABLE
EXPENDABLE
IMPASSABLE
UNSUITABLE
ACCEPTABLE
IMPOSSIBLE
ASPOSSIBLE
RECEPTACLE
MOTORCYCLE
AUTOMOBILE
DISCIPLINE
QUARANTINE
ENTERPRISE
TRANSVERSE
COORDINATE
ILLUMINATE
ANTICIPATE
ILLITERATE
ILLUSTRATE
COMPENSATE
DISTRIBUTE
SUBSTITUTE
CONSTITUTE
COMMUNIQUE
TWENTYFIVE
SUCCESSIVE
IMPRESSIVE
LOCOMOTIVE
CENTRALIZE
NATURALIZE
DEMOBILIZE
COMMANDING
DEBOUCHING
DETRUCKING
ENTRUCKING
ENCIRCLING
SIGNALLING
PATROLLING
OVERCOMING
DETRAINING
CONCERNING
INDICATING
EVACUATING

COLLECTING
CONNECTING
INFLICTING
EXPEDITING
RECRUITING
ATTEMPTING
SUPPORTING
EXTINGUISH
NINETEENTH
EIGHTEENTH
THIRTEENTH
FOURTEENTH
WILLATTACK
ARTIFICIAL
CREDENTIAL
ADDITIONAL
ACCIDENTAL
REGIMENTAL
INDIVIDUAL
WITHDRAWAL
AIRCONTROL
SUCCESSFUL
RESPECTFUL
MEMORANDUM
SUSPENSION
DISPERSION
CONCESSION
CONFESSION
DEPRESSION
IMPRESSION
POSSESSION
SUBMISSION
COMMISSION
PERMISSION
DISCUSSION
CONCLUSION
DEDICATION
INDICATION
ALLOCATION
FOUNDATION
RECREATION
IRRIGATION
NAVIGATION
REGULATION
POPULATION

ESTIMATION
DOMINATION
DETONATION
OCCUPATION
SEPARATION
DECORATION
LIMITATION
SANITATION
INVITATION
EVACUATION
EVALUATION
EXCAVATION
COLLECTION
CONNECTION
INSPECTION
CORRECTION
PROTECTION
EXHIBITION
EXPEDITION
DEFINITION
AMMUNITION
OPPOSITION
PROPORTION
REVOLUTION
MACHINEGUN
BATTLESHIP
CENSORSHIP
ARMOREDCAR
COMMANDEER
DISPATCHER
MILLIMETER
GONIOMETER
HYDROMETER
HYGROMETER
HELICOPTER
AMBASSADOR
INSTRUCTOR
BALLISTICS
STATISTICS
CROSSROADS
DESPATCHES
DISPATCHES
ASSEMBLIES
FACILITIES
ACTIVITIES

CASUALTIES
FRONTLINES
SUBMARINES
OBJECTIVES
ENEMYTANKS
SUSPICIONS
COLLISIONS
PROVISIONS
EXPLOSIONS
FORMATIONS
OPERATIONS
DIRECTIONS
CONDITIONS
TROOPSHIPS
NEWSPAPERS
KILOMETERS
DESTROYERS
TRANSPORTS
SUSPICIOUS
VICTORIOUS
CIRCUITOUS
CONTINUOUS
PHOSPHORUS
FLASHLIGHT
COMMANDANT
LIEUTENANT
CONTINGENT
SUFFICIENT
CONVENIENT
EQUIVALENT
ENGAGEMENT
MANAGEMENT
EXCITEMENT
DETACHMENT
ATTACHMENT
EXPERIMENT
ENROLLMENT
ASSIGNMENT
ATTAINMENT
INTERNMENT
GOVERNMENT
ASSESSMENT
COMMITMENT
DEPARTMENT
ENLISTMENT

Table D-2—*Continued*

INSTRUMENT
DEPLOYMENT
EMPLOYMENT
PERSISTENT

AIRSUPPORT
CONSPIRACY
DEFICIENCY
EFFICIENCY

COMPLETELY
APPARENTLY
INCENDIARY
COMMISSARY

ELEMENTARY
LABORATORY
TRAJECTORY
CAPABILITY

AUDIBILITY
VISIBILITY
SIMILARITY
INSECURITY

ELEVEN LETTER WORDS

IMPEDIMENTA
TOPOGRAPHIC
RECOMMENDED
PREARRANGED
ESTABLISHED
OVERWHELMED
DISAPPEARED
SURRENDERED
ENCOUNTERED
TRANSFERRED
DISINFECTED
REAPPOINTED
INTERCEPTED
INTERRUPTED
CONSTITUTED
BATTLEFIELD
PERFORMANCE
MAINTENANCE
COINCIDENCE
SUBSISTENCE
ACKNOWLEDGE
CATASTROPHE
INFLAMMABLE
RESPONSIBLE
NAVALBATTLE
TEMPERATURE
MANUFACTURE
SCHOOLHOUSE
CUSTOMHOUSE
CERTIFICATE
COMMUNICATE

INVESTIGATE
APPROPRIATE
APPROXIMATE
EXTERMINATE
DETERIORATE
CONCENTRATE
DEMONSTRATE
NECESSITATE
DISCONTINUE
SEVENTYFIVE
PROGRESSIVE
RADIOACTIVE
RETROACTIVE
DESCRIPTIVE
SYNCHRONIZE
APPROACHING
INTERVENING
ENGINEERING
INTERFERING
ALTERNATING
INTERESTING
WITHDRAWING
DISTINGUISH
SEVENTEENTH
NAVALATTACK
STRATEGICAL
TRADITIONAL
CONTINENTAL
FIRECONTROL
NATIONALISM
SMOKESCREEN

APPLICATION
ASSOCIATION
RETALIATION
DEBARKATION
EMBARKATION
LEGISLATION
CIRCULATION
INFORMATION
EXPLANATION
DESIGNATION
RESIGNATION
EXAMINATION
PREPARATION
COOPERATION
IMMIGRATION
INSPIRATION
CORPORATION
PENETRATION
ARBITRATION
COMPUTATION
OBSERVATION
RESERVATION
RESTRICTION
DISTINCTION
DESTRUCTION
INSTRUCTION
RECOGNITION
REQUISITION
COMPOSITION
DISPOSITION
COMPETITION

DESCRIPTION
CONSUMPTION
INSTITUTION
LIGHTBOMBER
HEAVYBOMBER
RANGEFINDER
DYNAMOMETER
THERMOMETER
INTERPRETER
RECONNOITER
AERONAUTICS
NAVALFORCES
ACCESSORIES
HOSTILITIES
ENEMYPLANES
PHILIPPINES
PARENTHESES
HEAVYLOSSES
COMMUNIQUES
PARENTHESIS
CREDENTIALS
BATTLESHIPS
ARMOREDCARS
CORRECTNESS
ENGAGEMENTS
ASSIGNMENTS
ASSESSMENTS
INSTRUMENTS
ESTIMATEDAT
SIGNIFICANT
INDEPENDENT

INTELLIGENT
COEFFICIENT
BOMBARDMENT
REPLACEMENT
EMPLACEMENT
ENFORCEMENT
ARRANGEMENT
CONFINEMENT
REQUIREMENT
MEASUREMENT
IMPROVEMENT
CONCEALMENT
ECHELONMENT
DEVELOPMENT
APPOINTMENT
COMPARTMENT
BELLIGERENT
INCOMPETENT
FINGERPRINT
DISCREPANCY
PHOTOGRAPHY
IMMEDIATELY
EXTENSIVELY
EFFECTIVELY
PRELIMINARY
CONTROVERSY
ELECTRICITY
NATIONALITY
SUITABILITY
SUPERIORITY

TWELVE LETTER WORDS

TRANSPACIFIC
HYDROGRAPHIC
UNIDENTIFIED
COMMISSIONED
DISSEMINATED
CONCENTRATED
DEMONSTRATED

DISORGANIZED
SIGNIFICANCE
INTELLIGENCE
INTERFERENCE
INCOMPETENCE
CONSIDERABLE
FIGHTERPLANE

INTERMEDIATE
DECENTRALIZE
GENERALSTAFF
TRANSFERRING
ENTERPRISING
ILLUMINATING
DISTRIBUTING

CONSTITUTING
BREAKTHROUGH
GEOGRAPHICAL
CONFIDENTIAL
PRESIDENTIAL
RECREATIONAL
AGRICULTURAL

Table D-2—*Continued*

DEPARTMENTAL
UNSUCCESSFUL
GENERALALARM
VETERINARIAN
TRANSMISSION
VERIFICATION
CONFISCATION
COMMENDATION
CONCILIATION
CANCELLATION
PROCLAMATION
CONFIRMATION
CONFORMATION
COORDINATION
ILLUMINATION
ANTICIPATION
REGISTRATION
ILLUSTRATION
INAUGURATION
COMPENSATION

CONVERSATION
RADIOSTATION
CONTINUATION
PRESERVATION
MOBILIZATION
ORGANIZATION
INTERDICTION
ROADJUNCTION
INTRODUCTION
CONSTRUCTION
INTERVENTION
INTERCEPTION
CONSCRIPTION
INTERRUPTION
DISTRIBUTION
SUBSTITUTION
CONSTITUTION
NORTHWESTERN
SOUTHWESTERN

MARKSMANSHIP
MEDIUMBOMBER
COMMISSIONER
PSYCHROMETER
SHARPSHOOTER
DIFFICULTIES
UNITEDSTATES
PREPARATIONS
OBSTRUCTIONS
INSTRUCTIONS
LIGHTBOMBERS
HEAVYBOMBERS
HEADQUARTERS
PREPAREDNESS
COMPLETENESS
CARELESSNESS
SEARCHLIGHTS
REPLACEMENTS
EMPLACEMENTS

MEASUREMENTS
ADVANTAGEOUS
SIMULTANEOUS
ANTIAIRCRAFT
NONCOMBATANT
CONVALESCENT
DISPLACEMENT
COMMENCEMENT
ANNOUNCEMENT
ENTANGLEMENT
DECIPHERMENT
ENCIPHERMENT
REENLISTMENT
INEFFICIENCY
SUCCESSFULLY
RESPECTFULLY
SATISFACTORY
INTRODUCTORY
IRREGULARITY

THIRTEEN LETTER WORDS

TRANSATLANTIC
DISTINGUISHED
DECENTRALIZED
DISAPPEARANCE
IMPRACTICABLE
INDETERMINATE
CORRESPONDING
CONCENTRATING
COUNTERATTACK
CHRONOLOGICAL
CONGRESSIONAL

INTERNATIONAL
SPECIFICATION
QUALIFICATION
COMMUNICATION
ACCOMMODATION
INVESTIGATION
DISSEMINATION
DETERMINATION
EXTERMINATION
CONSIDERATION
CONCENTRATION

DEMONSTRATION
QUARTERMASTER
CIRCUMSTANCES
DISCREPANCIES
PRELIMINARIES
FIGHTERPLANES
INSTALLATIONS
MEDIUMBOMBERS
MISCELLANEOUS
INSTANTANEOUS
REENFORCEMENT

REINFORCEMENT
REIMBURSEMENT
REINSTATEMENT
ESTABLISHMENT
ENTERTAINMENT
REAPPOINTMENT
APPROXIMATELY
EXTRAORDINARY
REVOLUTIONARY
DEPENDABILITY

FOURTEEN LETTER WORDS

CHARACTERISTIC
RECONNAISSANCE
DISCONTINUANCE
CORRESPONDENCE
ADMINISTRATIVE
REPRESENTATIVE
DISTINGUISHING

RECONNOITERING
METEOROLOGICAL
CIRCUMSTANTIAL
CLASSIFICATION
IDENTIFICATION
RECOMMENDATION

ADMINISTRATION
INTERPRETATION
TRANSPORTATION
CENTRALIZATION
NATURALIZATION
DEMOBILIZATION

REORGANIZATION
RECONSTRUCTION
IRREGULARITIES
INVESTIGATIONS
SATISFACTORILY
RESPONSIBILITY

Table D-3. List of words used in military text arranged alphabetically according to word pattern.

AA	A	CC	EPT
AA	A	CC	ORDING
AA	O	CC	UPY
AA	A	DD	
AA	BE	DD	ING
AA	LA	DD	ER
AA	SU	DD	EN
AA	B	EE	N
AA	CR	EE	K
AA	F	EE	L
AA	F	EE	T
AA	FL	EE	
AA	FL	EE	T
AA	FOURT	EE	N
AA	HASB	EE	N
AA	K	EE	P
AA	M	EE	T
AA	PROC	EE	D
AA	R	EE	NLIST
AA	S	EE	
AA	S	EE	N
AA	SCR	EE	N
AA	SIXT	EE	N
AA	SP	EE	D
AA	ST	EE	L
AA	SW	EE	PING
AA	THR	EE	
AA	W	EE	K
AA	WH	EE	L
AA	YANK	EE	
AA	BU	FF	ER
AA	E	FF	ORT
AA	JUMPO	FF	
AA	O	FF	
AA	O	FF	END
AA	O	FF	ICE
AA	O	FF	ICER
AA	STA	FF	
AA	SU	FF	ER
AA	TRA	FF	IC
AA	FO	GG	Y
AA	A	LL	
AA	A	LL	IED
AA	A	LL	IES
AA	A	LL	OW
AA	A	LL	Y
AA	BI	LL	ET
AA	BU	LL	ETIN
AA	CA	LL	
AA	CE	LL	
AA	CO	LL	APSED
AA	DO	LL	AR
AA	DRI	LL	
AA	ENRO	LL	
AA	FA	LL	
AA	FA	LL	ING
AA	FE	LL	
AA	FU	LL	
AA	HI	LL	
AA	I	LL	
AA	INSTA	LL	
AA	KI	LL	ED
AA	OSCI	LL	ATE
AA	PATRO	LL	ING
AA	PAYRO	LL	
AA	RA	LL	Y
AA	REFI	LL	
AA	SHE	LL	
AA	SHE	LL	ING
AA	SMA	LL	
AA	SPE	LL	
AA	VA	LL	EY
AA	VI	LL	AGE
AA	WE	LL	
AA	WI	LL	
AA	CO	MM	A
AA	CO	MM	AND
AA	CO	MM	ANDER
AA	CO	MM	END
AA	CO	MM	ENT
AA	CO	MM	IT
AA	CO	MM	UTE
AA	HA	MM	ER
AA	JA	MM	ING
AA	SU	MM	ARY
AA	SU	MM	ER
AA	SU	MM	IT
AA	SU	MM	ON
AA	A	NN	EX
AA	BA	NN	ER
AA	CA	NN	OT
AA	CHA	NN	EL
AA	GU	NN	ER
AA	MA	NN	ER
AA	TO	NN	AGE
AA	B	OO	K

Table D-3—*Continued*

AA	B	OO	TH
AA	C	OO	K
AA	C	OO	RDINATE
AA	H	OO	K
AA	L	OO	K
AA	PLAT	OO	N
AA	PR	OO	F
AA	SCH	OO	L
AA	T	OO	
AA	T	OO	K
AA	T	OO	L
AA	TR	OO	PS
AA	W	OO	DS
AA	A	PP	LY
AA	A	PP	OINT
AA	A	PP	OINTED
AA	A	PP	ROVE
AA	HA	PP	EN
AA	MA	PP	ING
AA	SU	PP	LY
AA	SU	PP	ORT
AA	SU	PP	ORTING
AA	A	RR	EST
AA	A	RR	IVE
AA	CA	RR	Y
AA	CU	RR	ENT
AA	DE	RR	ICK
AA	FE	RR	Y
AA	GA	RR	ISON
AA	HU	RR	ICANE
AA	SIE	RR	A
AA	TE	RR	AIN
AA	A	SS	ET
AA	A	SS	IGNED
AA	A	SS	URE
AA	ACRO	SS	
AA	COMPA	SS	
AA	CONGRE	SS	
AA	CRO	SS	
AA	CRO	SS	ING
AA	DARKNE	SS	
AA	DRE	SS	
AA	DRE	SS	ING
AA	EMBA	SS	Y
AA	I	SS	UE
AA	LE	SS	
AA	LE	SS	EN
AA	LO	SS	
AA	MA	SS	
AA	ME	SS	
AA	ME	SS	ING
AA	PA	SS	
AA	PA	SS	ED
AA	PA	SS	IVE
AA	PO	SS	IBLE
AA	PRE	SS	
AA	UNLE	SS	
AA	WITNE	SS	
AA	BA	TT	EN
AA	BA	TT	ERY
AA	BA	TT	LE
AA	BA	TT	LESHIP
AA	BI	TT	ER
AA	LI	TT	ER
AA	OMI	TT	ED
AA	SPO	TT	ING
AA	SUBMI	TT	ED
AA	WRI	TT	EN
AA	MU	ZZ	LE
AA	NO	ZZ	LE
AABA	AGR	EEME NT	
AABA	K	EEPE R	
AABA	CH	EESE	
AABA	BR	EEZE	
AABA	MA	NNIN G	
AABA	PLA	NNIN G	
AABA	RU	NNIN G	
AABA	L	OOKO UT	
AABA	E	RROR	
AABA	MI	RROR	
AABA	TE	RROR	
AABA	GLA	SSES	
AABA	LO	SSES	
AABA	PA	SSES	
AABA	A	SSIS T	
AABA	CHA	SSIS	
AABAACB	A	SSESSME NT	
AABAACBDEA	A	SSESSMENTS	
AABAB	PROC	EEDED	
AABB	CO	FFEE	
AABB	BA	LLOO N	
AABBAACAC	B	EENNEEDED	
AABBCBC	SU	CCEEDED	
AABCA	B	EETLE	
AABCA	A	NNOUN CE	
AABCA	F	OOTHO LD	

Table D-3—*Continued*

AABCA	CA	RRIER
AABCA	A	SSETS
AABCA	I	SSUES
AABCADEC	CO	MMITMENT
AABCADEC	A	TTENTION
AABCADEFEA	A	NNOUNCEMEN T
AABCB	SCR	EENIN G
AABCB	DI	FFERE NT
AABCB	SU	FFERE D
AABCB	O	FFICI AL
AABCB	SU	FFICI ENT
AABCB	A	LLEGE
AABCB	CO	LLEGE
AABCB	BI	LLETE D
AABCB	A	MMETE R
AABCB	W	OODED
AABCB	TE	RRIFI C
AABCB	BA	TTERE D
AABCBDEB	DI	FFERENCE
AABCC	A	CCESS
AABCC	A	CCESS ORY
AABCC	CO	MMISS ARY
AABCCB	WI	LLATTA CK
AABCCDD	CO	MMITTEE
AABCCDEFBC	A	CCESSORIES
AABCDA	I	LLEGAL
AABCDA	A	TTEMPT
AABCDAB	A	TTEMPTE D
AABCDB	O	FFENSE
AABCDB	CHA	LLENGE
AABCDB	BA	LLISTI C
AABCDB	A	RRESTE D
AABCDB	PA	SSENGE R
AABCDB	BA	TTERIE S
AABCDBA	SU	RRENDER
AABCDBABD	SU	RRENDERED
AABCDBC	CO	MMANDAN T
AABCDBD	O	FFENDED
AABCDBEC	BA	LLISTICS
AABCDD	A	DDRESS
AABCDD	I	LLNESS
AABCDDCA	A	DDRESSED
AABCDDCD	A	DDRESSES
AABCDEB	CO	MMUNIQU E
AABCDEB	TR	OOPSHIP
AABCDEB	A	SSEMBLE
AABCDEBC	TR	OOPSHIPS
AABCDEC	CO	MMANDIN G
AABCDECB	BA	TTLEFIEL D
AABCDED	CO	MMANDED
AABCDEDFC	A	MMUNITION
AABCDEE	CO	MMANDEE R
AABCDEFA	R	EENLISTE D
AABCDEFA	I	RREGULAR
AABCDEFB	O	FFENSIVE
AABCDEFBA	A	SSEMBLIES
AABCDEFC	A	LLOTMENT
AABCDEFC	C	OOPERATE
AABCDEFD	I	LLUSTRAT E
AABCDEFD	A	SSIGNMEN T
AABCDEFDGA	A	SSIGNMENTS
AABCDEFGA	C	OOPERATIO N
AABCDEFGABF	R	EENLISTMENT
AABCDEFGD	BA	TTLESHIPS
AABCDEFGDAE	C	OORDINATION
AABCDEFGDE	A	PPOINTMENT
ABA		AGA IN
ABA		AGA INST
ABA		ALA RM
ABA	C	ALA MITY
ABA	S	ALA RY
ABA	D	AMA GE
ABA		ANA LYZE
ABA	M	ANA GE
ABA	C	ANA L
ABA	J	APA N
ABA	N	APA LM
ABA	P	ARA CHUTE
ABA	P	ARA DE
ABA	SEP	ARA TION
ABA	F	ATA L
ABA	C	AVA LRY
ABA	EXC	AVA TION
ABA	N	AVA L
ABA	N	AVA LFORCES
ABA		AWA IT
ABA		AWA RD
ABA		AWA Y
ABA	PRO	BAB LE
ABA	PRO	BAB LY
ABA	BI	CYC LE
ABA		CYC LONE
ABA	BLOCKA	DED
ABA	GROUN	DED
ABA	GUAR	DED
ABA	INVA	DED

Table D-3—*Continued*

ABA	LAN	DED		ABA	L	IAI	SON
ABA	RAI	DED		ABA	PROH	IBI	T
ABA	WOUN	DED		ABA	SERV	ICI	NG
ABA		DID		ABA	RA	IDI	NG
ABA	IC	EBE	RG	ABA	R	IDI	NG
ABA	PR	ECE	DING	ABA	R	IGI	D
ABA	R	ECE	IPT	ABA	F	ILI	NG
ABA	CR	EDE	NTIAL	ABA	M	ILI	TARY
ABA	F	EDE	RAL	ABA	MOB	ILI	ZE
ABA	D	EFE	AT	ABA	L	IMI	T
ABA	D	EFE	CT	ABA	PROX	IMI	TY
ABA	D	EFE	CTOR	ABA	S	IMI	LAR
ABA	D	EFE	R	ABA	F	INI	SH
ABA	SI	EGE		ABA	F	IRI	NG
ABA	R	EJE	CT	ABA	RET	IRI	NG
ABA		ELE	VATION	ABA	W	IRI	NG
ABA	S	ELE	CT	ABA	ADV	ISI	NG
ABA	T	ELE	GRAM	ABA	DEC	ISI	ON
ABA	DISPLAC	EME	NT	ABA	V	ISI	BLE
ABA	PLAC	EME	NT	ABA	D	ISI	NFECT
ABA	R	EME	DY	ABA	V	ISI	T
ABA	SCH	EME		ABA	V	ISI	TOR
ABA		ENE	MY	ABA	CR	ITI	QUE
ABA	G	ENE	RAL	ABA	POL	ITI	CS
ABA	R	EPE	L	ABA	POS	ITI	VE
ABA	CONQU	ERE	D	ABA	UT	ILI	ZE
ABA	COV	ERE	D	ABA		MEM	ORIAL
ABA	H	ERE		ABA	DOMI	NAN	CE
ABA	SPH	ERE		ABA	DOMI	NAN	T
ABA	TH	ERE		ABA	ORD	NAN	CE
ABA	W	ERE		ABA	MOR	NIN	G
ABA	WH	ERE		ABA		NIN	E
ABA	D	ESE	RT	ABA		NIN	ETY
ABA	PR	ESE	NT	ABA		NIN	TH
ABA	TH	ESE		ABA	C	OLO	N
ABA	COMPL	ETE		ABA	C	OLO	RS
ABA	KILOM	ETE	R	ABA	SEMIC	OLO	N
ABA	M	ETE	R	ABA	AUT	OMO	BILE
ABA	D	EVE	LOP	ABA	PR	OMO	TE
ABA		EVE	RY	ABA	H	ONO	R
ABA	S	EVE	N	ABA	VIG	ORO	US
ABA	S	EVE	NTH	ABA	M	OTO	R
ABA	S	EVE	NTY	ABA	M	OTO	RIZED
ABA	S	EVE	RAL	ABA	PR	OVO	ST
ABA		EYE		ABA		PIP	E
ABA		FIF	TH	ABA		POP	ULATED
ABA		FIF	TY	ABA	LIB	RAR	Y
ABA	EIG	HTH		ABA	CA	RTR	IDGE

Table D-3—*Continued*

ABA	D	RYR UN
ABA	DI	SAS TER
ABA	CA	SES
ABA	RE	SIS T
ABA		SUS PEND
ABA		SYS TEM
ABA	DIC	TAT OR
ABA	S	TAT ION
ABA	AL	TIT UDE
ABA	LA	TIT UDE
ABA		TIT LE
ABA		TOT AL
ABA		TOT ALING
ABA	A	UGU ST
ABA		USU AL
ABA	F	UTU RE
ABA	SUR	VIV ED
ABAA	HAV	EBEE N
ABAA		SESS ION
ABAACC		TATTOO
ABAB	DETRA	ININ G
ABAB	L	ININ G
ABAB	M	ININ G
ABAB	OBTA	ININ G
ABAB	RA	ININ G
ABAB	REMA	ININ G
ABAB	TRA	ININ G
ABAB	CR	ISIS
ABAB		PAPA
ABAB	WI	THTH E
ABAB	PAR	TITI ON
ABAC	QU	EBEC
ABACA	C	ANADA
ABACA	P	ANAMA
ABACA	PR	ECEDE
ABACA		ELEME NT
ABACA		ELEME NTARY
ABACA		ELEVE N
ABACA	C	EMETE RY
ABACA	S	EVERE
ABACA	AUD	IBILI TY
ABACA	EXH	IBITI ON
ABACA	V	ICINI TY
ABACA	FAC	ILITI ES
ABACA	M	ILITI A
ABACA	D	IMINI SH
ABACA	L	IMITI NG
ABACA		INITI AL
ABACA	D	IRIGI BLE
ABACA	SEM	IRIGI D
ABACA	REQU	ISITI ON
ABACA	C	IVILI AN
ABACA	D	IVISI ON
ABACA	L	OCOMO TIVE
ABACA	M	ONOPO LY
ABACA	PR	OTOCO L
ABACA	CONS	TITUT E
ABACA		UNUSU AL
ABACADA	V	ISIBILI TY
ABACADB	DEF	INITION
ABACADBA	PR	ECEDENCE
ABACADC		INITIAT E
ABACADD	COMPL	ETENESS
ABACADDA	N	AVALATTA CK
ABACADEC	D	IVISIONS
ABACB	V	ACANC Y
ABACB	COMB	ATANT
ABACB	C	ATAST ROPHE
ABACB	D	ETECT OR
ABACB	V	ISITS
ABACB		MEMBE R
ABACBDEC	D	ETENTION
ABACBDEC	R	ETENTION
ABACBDEFGFAG		NONCOMBATANT
ABACC	R	EBELL ION
ABACC	N	ECESS ARY
ABACC	N	ECESS ITY
ABACC	CAR	ELESS
ABACC	WIR	ELESS
ABACCA	P	ARALLA X
ABACCA	R	EPELLE D
ABACCA	T	OMORRO W
ABACCDACC	CAR	ELESSNESS
ABACCDC	P	ARALLEL
ABACCDEFEA	N	ECESSITATE
ABACDA		ALASKA
ABACDA		ARABIA
ABACDA	N	AVALBA SE
ABACDA	R	ECEIVE
ABACDA	D	ECEMBE R
ABACDA	D	EFENSE
ABACDA	R	EJECTE D
ABACDA	R	ELEASE
ABACDA	S	ELECTE D
ABACDA	R	EMEDIE S

Table D-3—*Continued*

ABACDA		EMERGE NCY
ABACDA		ENEMIE S
ABACDA	R	EPEATE D
ABACDA	R	EVENUE
ABACDA	U	NKNOWN
ABACDA	PR	OMOTIO N
ABACDAAC	S	EVENTEEN
ABACDAACD	S	EVENTEENT H
ABACDAC	D	ESERTER
ABACDAD	D	EFENSES
ABACDAED		AVAILABL E
ABACDAEEC	N	AVALBATTL E
ABACDB	F	ATALIT Y
ABACDB	A	NONYMO US
ABACDB	C	OLONEL
ABACDBA	TH	EREFORE
ABACDC	R	ECEIVI NG
ABACDC		EVENIN G
ABACDC	DYNA	MOMETE R
ABACDCA	L	IMITATI ON
ABACDCCA		NINETEEN
ABACDCCAD		NINETEENT H
ABACDCEA	S	TATEMENT
ABACDCECFGHIE	M	ETEOROLOGICAL
ABACDD		FIFTEE N
ABACDD	FO	RTRESS
ABACDDEC		FIFTEENT H
ABACDEA		ELEVATE
ABACDEA	D	EVELOPE
ABACDEA	VER	IFICATI ON
ABACDEA	S	IMILARI TY
ABACDEAD		SUSPENSE
ABACDEAFGE		SUSPENSION
ABACDEB	EXPL	ANATION
ABACDEB	T	OPOGRAP HIC
ABACDEBFA	R	ECEPTACLE
ABACDEC		ABANDON
ABACDEC	D	AMAGING
ABACDEC	QU	ARANTIN E
ABACDECA	P	ENETRATE
ABACDECFBA	D	ETERIORATE
ABACDECFGB	P	ENETRATION
ABACDED	C	APABILI TY
ABACDED	M	OTORCYC LE
ABACDED		SUSPICI ON
ABACDEDEDC	G	ENERALALAR M
ABACDEDFBA		SUSPICIOUS
ABACDEDFGA		SUSPICIONS
ABACDEFA	D	EFECTIVE
ABACDEFA	D	EFENSIVE
ABACDEFA	T	ELEPHONE
ABACDEFA	D	ETERMINE
ABACDEFA	D	EVELOPME NT
ABACDEFA		EXERCISE
ABACDEFAF		EXERCISES
ABACDEFB		DEDICATE
ABACDEFB		ENEMYTAN KS
ABACDEFC		DEDICATI ON
ABACDEFCDFE	V	ETERINARIAN
ABACDEFCFD		ELECTRICIT Y
ABACDEFD		SUSPECTE D
ABACDEFDF		SUSPENDED
ABACDEFE		ANALYSIS
ABACDEFGA		EXECUTIVE
ABACDEFGB		POPULATIO N
ABACDEFGBA		ENEMYPLANE S
ABACDEFGBA	S	EVENTYFIVE
ABACDEFGBEHF	D	ETERMINATION
ABACDEFGDHH	G	ENERALSTAFF
ABACDEFGE		MEMORANDA
ABACDEFGHA		MEMORANDUM
ABACDEFGHIA	D	ECENTRALIZE
ABBA		AFFA IR
ABBA		APPA RENT
ABBA		APPA RENTLY
ABBA		ARRA NGE
ABBA	B	ARRA CKS
ABBA	B	ARRA GE
ABBA		ASSA ULT
ABBA	P	ASSA GE
ABBA	IMP	ASSA BLE
ABBA		ATTA CH
ABBA		ATTA CK
ABBA		ATTA IN
ABBA	B	ATTA LION
ABBA	IN	DEED
ABBA		EFFE CT
ABBA	COMP	ELLE D
ABBA	SH	ELLE D
ABBA	CONF	ERRE D
ABBA	COMPR	ESSE D
ABBA	IMPR	ESSE D
ABBA	PR	ESSE D
ABBA	V	ESSE L
ABBA	B	ETTE R
ABBA	CIGAR	ETTE

Table D-3—*Continued*

ABBA	L	ETTE R
ABBA	D	IFFI CULT
ABBA	F	ILLI NG
ABBA	K	ILLI NG
ABBA	REF	ILLI NG
ABBA	SW	IMMI NG
ABBA	SH	IPPI NG
ABBA	M	ISSI LE
ABBA	M	ISSI NG
ABBA	ADM	ISSI ON
ABBA	M	ISSI ON
ABBA	PERM	ISSI ON
ABBA	F	ITTI NG
ABBA	AFTER	NOON
ABBA		NOON
ABBA	F	OLLO W
ABBA	C	OMMO N
ABBA		OPPO SE
ABBA		OPPO SITE
ABBA	B	OTTO M
ABBAB	B	AGGAG E
ABBAB	WITN	ESSES
ABBACA		APPARA TUS
ABBACA	L	ETTERE D
ABBACB	V	ESSELS
ABBACDA		EFFECTE D
ABBACDA	M	ESSENGE R
ABBACDB	M	ISSIONS
ABBACDEA		IRRIGATI ON
ABBACDEDA		OPPOSITIO N
ABBACDEFA		EFFECTIVE
ABBACDEFA	D	IFFICULTI ES
ABBACDEFA		IMMIGRATI ON
ABBACDEFCD		ILLITERATE
ABBACDEFDB		ATTAINMENT
ABBACDEFEC		ARRANGEMEN T
ABBACDEFGB		ATTACHMENT
ABBCA		ANNUA L
ABBCA		APPEA R
ABBCA	DIS	APPEA R
ABBCA	C	ARRIA GE
ABBCA	S	ETTLE
ABBCA		ISSUI NG
ABBCA	FOUR	TEENT H
ABBCA	SIX	TEENT H
ABBCA	CHA	UFFEU R
ABBCA	S	URROU ND
ABBCADAEFC		APPEARANCE
ABBCADAEFC	DIS	APPEARANCE
ABBCADC		APPEARE D
ABBCBBDA	P	OSSESSIO N
ABBCBDA		ASSISTA NCE
ABBCBDAED		ASSISTANT
ABBCCDAB		ASSOONAS
ABBCDA		ALLOWA NCE
ABBCDA		APPROA CH
ABBCDA		ARRIVA L
ABBCDA		ASSURA NCE
ABBCDA	M	ESSAGE
ABBCDA		ILLUMI NATE
ABBCDAB	M	ESSAGES
ABBCDAB	C	ORRIDOR
ABBCDAEA	B	ELLIGERE NT
ABBCDAEFC		ALLOCATIO N
ABBCDAEFC		IMMEDIATE
ABBCDAEFGAE		ILLUMINATIN G
ABBCDAEFGAHE		ILLUMINATION
ABBCDAEFGAHE	D	ISSEMINATION
ABBCDBCEA		APPROPRIA TE
ABBCDCA		EFFICIE NT
ABBCDCA	C	OLLISIO N
ABBCDCAED		EFFICIENC Y
ABBCDCAED	C	OLLISIONS
ABBCDCEFA		ADDITIONA L
ABBCDDCA	C	OMMISSIO N
ABBCDDCA	C	OMMISSIO NER
ABBCDDCEAFGC		ACCOMMODATIO N
ABBCDEA		ACCOMPA NY
ABBCDEA		APPROVA L
ABBCDEA		ASSOCIA TE
ABBCDEA	SH	ELLFIRE
ABBCDEA	T	ERRIBLE
ABBCDEAFB		ACCORDANC E
ABBCDEAFB		REENFORCE
ABBCDEAFBC		ACCEPTANCE
ABBCDEAFBGBC		REENFORCEMEN T
ABBCDEAFD		APPLICATI ON
ABBCDEAFEC		ASSOCIATIO N
ABBCDEAFGC		ACCEPTABLE
ABBCDEAFGC		ALLEGIANCE
ABBCDEAFGHF	C	ORRESPONDIN G
ABBCDEFGA		ACCIDENTA L
ABBCDEFGA		APPROXIMA TE
ABBCDEFGA		OCCUPATIO N
ABBCDEFGBA		IRREGULARI TY
ABBCDEFGBAHAC		IRREGULARITIE S

Table D-3—*Continued*

ABBCDEFGEA		ILLUSTRATI	ON	ABCA	N	EARE	ST
ABBCDEFGHAD	C	OMMENDATION		ABCA	C	EASE	
ABCA	P	ACKA	GE	ABCA	GR	EASE	
ABCA	EV	ACUA	TING	ABCA	INCR	EASE	D
ABCA	EV	ACUA	TION	ABCA	L	EAVE	
ABCA	R	ADIA	L	ABCA		ECHE	LON
ABCA	R	ADIA	TE	ABCA	WR	ECKE	D
ABCA		ADJA	CENT	ABCA	INF	ECTE	D
ABCA	GR	ADUA	L	ABCA		EDGE	
ABCA		ADVA	NCE	ABCA	S	EIZE	
ABCA	DI	AGRA	M	ABCA	R	ELIE	F
ABCA		ALFA		ABCA	H	ELPE	R
ABCA	EV	ALUA	TION	ABCA	TW	ELVE	
ABCA		ALWA	YS	ABCA	NOV	EMBE	R
ABCA	C	AMPA	IGN	ABCA	ABS	ENCE	
ABCA	M	ANDA	TE	ABCA	LIC	ENSE	
ABCA	M	ANUA	L	ABCA	C	ENTE	R
ABCA	J	ANUA	RY	ABCA		ENTE	R
ABCA	C	ANVA	S	ABCA		ENVE	LOP
ABCA	CH	APLA	IN	ABCA	R	EQUE	ST
ABCA	C	APTA	IN	ABCA	FI	ERCE	
ABCA		AREA		ABCA	S	ERGE	ANT
ABCA	DEB	ARKA	TION	ABCA	MAT	ERIE	L
ABCA	EMB	ARKA	TION	ABCA	REV	ERSE	
ABCA		ASIA		ABCA	OBS	ERVE	
ABCA	CO	ASTA	L	ABCA	R	ESPE	CT
ABCA	C	ASUA	L	ABCA	W	ESTE	RLY
ABCA	C	ASUA	LTY	ABCA	W	ESTE	RN
ABCA		AVIA	TOR	ABCA		ETHE	R
ABCA		BARB	ED	ABCA	MAN	EUVE	R
ABCA		BOMB		ABCA	R	EVIE	W
ABCA		BOMB	ARD	ABCA		EXCE	PT
ABCA		BOMB	ER	ABCA		EXPE	CT
ABCA	LIGHT	BOMB	ER	ABCA		EXPE	ND
ABCA		BRIB	E	ABCA		EXTE	ND
ABCA		BULB		ABCA		GAUG	E
ABCA		CANC	EL	ABCA		GEOG	RAPHIC
ABCA		CHEC	K	ABCA	FOR	GING	
ABCA		CIRC	LE	ABCA	W	HICH	
ABCA		CIRC	ULATE	ABCA		HIGH	
ABCA		CONC	EAL	ABCA		HIGH	ER
ABCA		CONC	LUDE	ABCA		HIGH	EST
ABCA	HUN	DRED		ABCA	V	ICTI	M
ABCA	L	EADE	R	ABCA	M	IDNI	GHT
ABCA		EAGE	R	ABCA	DR	IFTI	NG
ABCA	M	EAGE	R	ABCA	L	IFTI	NG
ABCA	S	EAME	N	ABCA	S	IGNI	FY
ABCA	ST	EAME	R	ABCA	BU	ILDI	NG

Table D-3—*Continued*

ABCA		INDI	A
ABCA		INDI	CATE
ABCA		INDI	RECT
ABCA	DESCR	IPTI	ON
ABCA	L	IQUI	D
ABCA	A	IRFI	ELD
ABCA	M	ISFI	RE
ABCA	F	ISHI	NG
ABCA	W	ITHI	N
ABCA	FUE	LOIL	
ABCA		MAIM	
ABCA	LA	NDIN	G
ABCA	I	NFAN	TRY
ABCA	CO	NFIN	E
ABCA	U	NION	
ABCA	SU	NKEN	
ABCA	FLA	NKIN	G
ABCA	I	NLAN	D
ABCA	I	NTEN	D
ABCA	CO	NTIN	UAL
ABCA	CO	NTIN	UE
ABCA	I	NVEN	T
ABCA		OCTO	BER
ABCA	D	OCTO	R
ABCA	F	OGHO	RN
ABCA	P	OISO	N
ABCA	C	OMPO	SED
ABCA	C	ONVO	Y
ABCA	EN	ORMO	US
ABCA	EXPL	OSIO	N
ABCA		PUMP	
ABCA		PURP	OSE
ABCA	HA	RBOR	
ABCA	AI	RBOR	NE
ABCA	MU	RDER	
ABCA	O	RDER	
ABCA	O	RDER	S
ABCA		REAR	
ABCA		RECR	UIT
ABCA		REPR	ISAL
ABCA	COU	RIER	
ABCA	P	RIOR	
ABCA	SUPE	RIOR	
ABCA	A	RMOR	
ABCA	A	RMOR	Y
ABCA	P	ROGR	AM
ABCA	MO	RTAR	
ABCA	QUA	RTER	
ABCA	QUA	RTER	S
ABCA	FEB	RUAR	Y
ABCA	FO	RWAR	D
ABCA	CEN	SORS	HIP
ABCA		SUNS	ET
ABCA	IMPOR	TANT	
ABCA	S	TART	
ABCA	PRO	TECT	
ABCA		TENT	
ABCA		TENT	H
ABCA	PRO	TEST	
ABCA		TEXT	
ABCA		THAT	
ABCA	S	TRAT	EGIC
ABCA	S	TRAT	EGY
ABCA	D	UGOU	T
ABCA		UNSU	ITABLE
ABCA	P	URSU	E
ABCA	P	URSU	IT
ABCA	O	UTGU	ARD
ABCAA	D	ECREE	
ABCAA	D	EGREE	
ABCAA	B	ETWEE	N
ABCAA	DI	SCUSS	
ABCAA	A	SPOSS	IBLE
ABCAAB	P	ONTOON	
ABCAAB		THATTH	E
ABCAACDEB	P	REARRANGE	D
ABCAB	W	ARFAR	E
ABCAB	S	ECREC	Y
ABCAB	OBS	ERVER	
ABCAB	W	HETHE	R
ABCAB	B	INDIN	G
ABCAB	F	INDIN	G
ABCAB	S	INKIN	G
ABCAB	PA	INTIN	G
ABCAB	PR	INTIN	G
ABCAB	I	NTENT	
ABCAB	C	ORPOR	AL
ABCAB		RECRE	ATION
ABCAB	P	RIORI	TY
ABCAB	SUPE	RIORI	TY
ABCAB	DI	SEASE	
ABCAB	PRO	TECTE	D
ABCAB	PRO	TESTE	D
ABCAB	O	UTPUT	
ABCABA	INT	ERFERE	
ABCABB	D	ISMISS	

Table D-3—*Continued*

ABCABB	D	ISMISS AL
ABCABC		THATHA VE
ABCABCA		ENTENTE
ABCABDA	S	ENTENCE
ABCABDB		REPRESE NT
ABCABDBEFGFHIB		REPRESENTATIVE
ABCABDBEFGFHIED		REPRESENTATIONS
ABCABDC		RETREAT
ABCABDEFA	C	ORPORATIO N
ABCABDEFGHD		RECREATIONA L
ABCAC		ARMAM ENT
ABCAC	N	EARER
ABCAC		PROPO SE
ABCAC	P	RAIRI E
ABCAC	PRO	TESTS
ABCACA	D	IETITI AN
ABCACB	O	RDERED
ABCACBDEC		PROPORTIO N
ABCACDEFD		PROPOSALS
ABCADA		ALMANA C
ABCADA	R	ELIEVE
ABCADA	C	ENTERE D
ABCADA	B	ESIEGE D
ABCADA	R	EVIEWE D
ABCADAB	CO	NTINENT AL
ABCADAC	S	EALEVEL
ABCADAC		INDIVID UAL
ABCADAEC		IGNITION
ABCADAEFB		TENTATIVE
ABCADAEFC	S	IGNIFICAN T
ABCADAEFCE	S	IGNIFICANC E
ABCADAEFGHF		SUBSISTENCE
ABCADB		ATLANT IC
ABCADB		BRIBER Y
ABCADB		CIRCUI T
ABCADB	W	EDNESD AY
ABCADB	LOG	ISTICS
ABCADB	EXPL	OSIONS
ABCADB		PREPAR ING
ABCADB	IM	PROPER
ABCADB		PROPER
ABCADBA		INSIGNI A
ABCADBC		PREPARE
ABCADBCEFCGG		PREPAREDNESS
ABCADBD		PREPARA TION
ABCADBEFD		CIRCUITOU S
ABCADC	R	ADIATI ON
ABCADC	ST	ANDARD
ABCADC	V	ARIATI ON
ABCADC		ASIATI C
ABCADC		AVIATI ON
ABCADC	R	EVIEWI NG
ABCADC		EXTENT
ABCADC	I	NVENTE D
ABCADC		TACTIC S
ABCADC	S	TARTER
ABCADC		ZIGZAG
ABCADCA	CO	NVENIEN T
ABCADCB	CO	NDENSED
ABCADCB		TACTICA L
ABCADCEFBGABC		ENTERTAINMENT
ABCADCEFGED		CONCENTRATE
ABCADCEFGEHBC		CONCENTRATION
ABCADCEFGEHC		CONCENTRATIN G
ABCADD	D	EPRESS ION
ABCADD		EXCESS
ABCADD	D	ISTILL
ABCADD	P	OSTOFF ICE
ABCADD	B	OYCOTT
ABCADDA		AMBASSA DOR
ABCADDA		EXPELLE D
ABCADDECCFA		UNSUCCESSFU L
ABCADDEFA		EXCESSIVE
ABCADEA		ADVANTA GE
ABCADEA		ADVANTA GEOUS
ABCADEA	D	ECREASE
ABCADEA	S	EPTEMBE R
ABCADEA	R	EQUESTE D
ABCADEA	D	ISCIPLI NE
ABCADEAB	CO	NTINGENT
ABCADEAE		EXPENDED
ABCADEAE		EXPENSES
ABCADEAE		EXTENDED
ABCADEAFA		ELSEWHERE
ABCADEAFGA		EXPERIENCE
ABCADEB	C	ENTERIN G
ABCADEB		ENTERIN G
ABCADEB	R	ESPECTS
ABCADEB		INCIDEN T
ABCADEB	M	ISFIRES
ABCADEBCE		INCIDENCE
ABCADEC	M	ANDATED
ABCADEC	S	ECRETAR Y
ABCADEC	GYR	OSCOPIC
ABCADECA		REARGUAR D
ABCADECAFD	D	ISTINCTION

Table D-3—*Continued*

ABCADECFC		CONCERNIN G
ABCADEDA	CO	NFINEMEN T
ABCADEDAFB		INVITATION
ABCADEDBD		SUBSTITUT E
ABCADEDBDE		SUBSTITUTI ON
ABCADEDC	LI	EUTENANT
ABCADEDFGA		ENTERPRISE
ABCADEDFGDBC		CONCILIATION
ABCADEDFGFB		ENTERPRISIN G
ABCADEE	P	ROGRESS
ABCADEEBFGHC		CANCELLATION
ABCADEED		CANCELLE D
ABCADEEFBC		CONCESSION
ABCADEEFGD	P	ROGRESSIVE
ABCADEFA		ECHELONE D
ABCADEFA		ENVELOPE
ABCADEFA		EXPEDITE
ABCADEFA		EXPERIME NT
ABCADEFAB		INDICATIN G
ABCADEFAB	D	ISTINGUIS H
ABCADEFABGADE	D	ISTINGUISHING
ABCADEFAGB		INDICATION
ABCADEFB		ADVANCED
ABCADEFBA	EXT	RAORDINAR Y
ABCADEFC		BOMBARDM ENT
ABCADEFC		CIRCULAR
ABCADEFC	U	NTENABLE
ABCADEFCGHB		RETROACTIVE
ABCADEFD		ADVANCIN G
ABCADEFD		EXTENDIN G
ABCADEFD		EXTERIOR
ABCADEFE		CONCRETE
ABCADEFE		EXPEDITI NG
ABCADEFE		EXPEDITI ON
ABCADEFE		OBSOLETE
ABCADEFE	G	ONIOMETE R
ABCADEFE		PURPOSES
ABCADEFE		RECRUITI NG
ABCADEFEA	C	OMPOSITIO N
ABCADEFGA		EXPENSIVE
ABCADEFGA		EXTENSIVE
ABCADEFGAF		ECHELONMEN T
ABCADEFGB	C	ASUALTIES
ABCADEFGB		CIRCULATI ON
ABCADEFGBC		CONCLUSION
ABCADEFGC		INDICATED
ABCADEFGC	S	TRATEGICA L
ABCADEFGD		EXTENSION
ABCADEFGDC		CONCEALMEN T
ABCADEFGE		REPRISALS
ABCADEFGF		BOMBARDED
ABCADEFGHAB	C	ONFORMATION
ABCADEFGHCA		EXTERMINATE
ABCADEFGHCFIG		EXTERMINATION
ABCADEFGHEIGCF		REORGANIZATION
ABCADEFGHH	R	ESPECTFULL Y
ABCADEFGHIAJF		CIRCUMSTANCES
ABCADEFGHIB		RETROACTIVE
ABCADEFGHIE		GEOGRAPHICA L
ABCADEFGHIGBH		CIRCUMSTANTIA L
ABCBA		AWKWA RD
ABCBA		CAPAC ITY
ABCBA	COMP	LETEL Y
ABCBA	PA	CIFIC
ABCBA	SPE	CIFIC
ABCBA	HIN	DERED
ABCBA		DIVID E
ABCBA		GARAG E
ABCBA	C	ITATI ON
ABCBA		LEVEL
ABCBA	P	REFER
ABCBA		REFER
ABCBA	P	RESER VATION
ABCBA		RESER VATION
ABCBA		TAXAT ION
ABCBA	HOS	TILIT Y
ABCBA	U	TILIT Y
ABCBA	AC	TIVIT Y
ABCBAA	U	SELESS
ABCBAAB	P	REFERRE D
ABCBAB		DIVIDI NG
ABCBAB	AC	TIVITI ES
ABCBABDEB	P	REFERENCE
ABCBABDEB		REFERENCE
ABCBADA		MINIMUM
ABCBADB	P	RESERVE
ABCBADB		RESERVE
ABCBADB		REVERSE
ABCBADBC		RESERVES
ABCBADEB	SPE	CIFICATI ON
ABCBCDBA		REMEMBER
ABCBDA		DEFEND
ABCBDA		DEPEND
ABCBDA	MU	NITION S
ABCBDA		RESEAR CH
ABCBDA		STATES

Table D-3—*Continued*

ABCBDA		STATUS	ABCCDAEC		TERRITOR Y
ABCBDA	IN	TEREST	ABCCDAED		CORRECTE D
ABCBDAB		DEFENDE R	ABCCDAEFB		COLLECTIO N
ABCBDAB	E	NGAGING	ABCCDAEFB		CORRECTIO N
ABCBDABA		DEFENDED	ABCCDAEFBC		CONNECTION
ABCBDABD		DEPENDEN T	ABCCDAEFC		CONNECTIN G
ABCBDABDEA		STATISTICS	ABCCDAEFDGG		CORRECTNESS
ABCBDAEFGB		DEPENDABLE	ABCCDEA		GASSING
ABCBDAEFGHG		DEPENDABILI TY	ABCCDEA		GETTING
ABCBDCBA		PARAGRAP H	ABCCDEA	ST	RAGGLER
ABCBDDBA		DEFERRED	ABCCDEA	IN	TERRUPT
ABCBDEA	E	CONOMIC	ABCCDEAB	IN	TERRUPTE D
ABCBDEA		DAMAGED	ABCCDEAD		COMMENCE
ABCBDEA	PO	LITICAL	ABCCDEAD		COMMERCE
ABCBDEAEC		MANAGEMEN T	ABCCDEADCDE		COMMENCEMEN T
ABCBDEBA		DEFEATED	ABCCDEBFGHDA		DISSEMINATED
ABCBDEBA		DESERTED	ABCCDEFA		COMMUNIC ATE
ABCBDEBA		RECEIVER	ABCCDEFA		SUPPLIES
ABCBDEBA		REPEATER	ABCCDEFAGHFBE		COMMUNICATION
ABCBDEFA		REJECTOR	ABCCDEFBGHDGAD		CORRESPONDENCE
ABCBDEFA		STATIONS	ABCCDEFGA	R	EAPPOINTE D
ABCBDEFBA		DEVELOPED	ABCCDEFGHAFG	R	EAPPOINTMENT
ABCBDEFGA	R	ESISTANCE	ABCDA	S	ABOTA GE
ABCBDEFGBA		DETERMINED	ABCDA	R	AILWA Y
ABCBDEFGHFA		DISINFECTED	ABCDA		ALPHA
ABCBDEFGHIJBA		DECENTRALIZED	ABCDA		ANIMA L
ABCCA		LITTL E	ABCDA	S	ANITA RY
ABCCA		PASSP ORT	ABCDA	M	ARSHA L
ABCCA	S	TREET	ABCDA	M	ARTIA L
ABCCABDEC	C	ROSSROADS	ABCDA	E	ASTWA RD
ABCCBADED		MILLIMETE R	ABCDA	N	ATURA L
ABCCBCA	BE	GINNING	ABCDA	N	ATURA LIZE
ABCCBDA	INF	LAMMABL E	ABCDA	TE	CHNIC AL
ABCCDA		COLLEC T	ABCDA		COUNC IL
ABCCDA		CORREC T	ABCDA	R	EACHE D
ABCCDA	T	RIGGER	ABCDA	L	EAGUE
ABCCDA		RUBBER	ABCDA		EASTE RLY
ABCCDA		RUNNER	ABCDA		EASTE RN
ABCCDA		SPOOLS	ABCDA	W	EATHE R
ABCCDA		SPOONS	ABCDA	H	EAVIE R
ABCCDA		SUGGES T	ABCDA	INS	ECURE
ABCCDA		SUPPOS E	ABCDA	S	ECURE
ABCCDA		TURRET	ABCDA	R	EDUCE
ABCCDAA		SUCCESS	ABCDA	SCH	EDULE
ABCCDAAEB		SUCCESSFU L	ABCDA	B	EFORE
ABCCDAAEBFF		SUCCESSFULL Y	ABCDA	R	EFUGE
ABCCDAAEFD		SUCCESSIVE	ABCDA	R	EFUSE
ABCCDAB	P	RESSURE	ABCDA	R	EGIME NT

Table D-3—*Continued*

ABCDA	R	EGIME NTAL	ABCDA	WI	THOUT
ABCDA		EITHE R	ABCDA	EX	TRACT
ABCDA	FUS	ELAGE	ABCDA		TRACT
ABCDA	D	ELIVE R	ABCDA	INS	TRUCT
ABCDA	GR	ENADE	ABCDA	DES	TRUCT ION
ABCDA		ERASE	ABCDA		TWENT Y
ABCDA	OP	ERATE	ABCDA	B	UREAU
ABCDA	R	ESCUE	ABCDA		WESTW ARD
ABCDA	PR	ESIDE NT	ABCDAA	R	EFUGEE
ABCDA	R	ESUME	ABCDAA	C	ODEBOO K
ABCDA	D	EVICE	ABCDAA	BU	SINESS
ABCDA	D	EVISE	ABCDAA	DI	STRESS
ABCDA		GOING	ABCDAA		STRESS
ABCDA	T	HOUGH	ABCDAAD	F	ORENOON
ABCDA	F	IGHTI NG	ABCDAB	C	HURCH
ABCDA		INFLI CT	ABCDAB		DECIDE
ABCDA	EXT	INGUI SH	ABCDAB		DECODE
ABCDA		INQUI RE	ABCDAB	SP	EARHEA D
ABCDA		INQUI RY	ABCDAB	R	EDUCED
ABCDA		INSPI RE	ABCDAB		ENTREN CH
ABCDA		LOCAL	ABCDAB		ERASER
ABCDA	LAU	NCHIN G	ABCDAB		POSTPO NE
ABCDA	CO	NDEMN	ABCDAB		RETIRE
ABCDA	MACHI	NEGUN	ABCDAB	ES	TIMATI ON
ABCDA		NOTIN G	ABCDABA		DECIDED
ABCDA	EXPA	NSION	ABCDABAB		INCLININ G
ABCDA	CO	NTAIN	ABCDABC	M	AINTAIN
ABCDA	MOU	NTAIN	ABCDABC	M	AINTAIN ED
ABCDA	I	NTERN AL	ABCDABCEFD		PHOSPHORUS
ABCDA	FRO	NTLIN E	ABCDABEFA		ENTRENCHE D
ABCDA	I	NTREN CH	ABCDAC	L	ANGUAG E
ABCDA	C	ONTRO L	ABCDAC		ANYWAY
ABCDA	H	ORIZO N	ABCDAC	GOV	ERNMEN T
ABCDA		OUTBO ARD	ABCDAC	I	NSTANT
ABCDA		PROMP T	ABCDAC	I	NSTANT LY
ABCDA		RECOR D	ABCDAC	F	OXTROT
ABCDA		REPOR T	ABCDAC	DI	SPERSE
ABCDA		RETUR N	ABCDAC	RES	TRICTI ON
ABCDA	P	RIMAR Y	ABCDAC	PA	TRIOTI C
ABCDA		RIVER	ABCDACB	CO	NDEMNED
ABCDA		ROGER	ABCDACDAEFGB	I	NSTANTANEOUS
ABCDA	FA	RTHER	ABCDACEFDAF		COINCIDENCE
ABCDA	FU	RTHER	ABCDAD		MOVEME NT
ABCDA	NO	RTHER LY	ABCDAD	A	MUSEME NT
ABCDA		SATIS FY	ABCDAD		RIGORO US
ABCDA		SHIPS	ABCDADC	S	ANITATI ON
ABCDA	WAR	SHIPS	ABCDADEDAFB		INSTITUTION
ABCDA		THIRT Y	ABCDADEFEAGC		ANTIAIRCRAFT

Table D-3—*Continued*

ABCDAEA		EXTREME
ABCDAEA		MAXIMUM
ABCDAEAB	SU	ITABILIT Y
ABCDAEABD	UNI	TEDSTATES
ABCDAEAE	PAR	ENTHESES
ABCDAEB	F	IGHTING
ABCDAEB	S	IGHTING
ABCDAEB		RAILROA D
ABCDAEB		REPORTE D
ABCDAEB		RETURNE D
ABCDAEB		TRACTOR
ABCDAEB	INS	TRUCTOR
ABCDAEBA		RECORDER
ABCDAEBC	DE	TONATION
ABCDAEBFBDC	U	NIDENTIFIED
ABCDAEBFC		SATISFACT ORY
ABCDAEC		AVERAGE
ABCDAEC	D	ISTRICT
ABCDAEC		OUTPOST
ABCDAECA		TWENTIET H
ABCEAECAB	I	NTERNMENT
ABCDAECB	D	ISTRICTS
ABCDAECD	L	ABORATOR Y
ABCDAECE		OUTPOSTS
ABCDAECFD	EX	AMINATION
ABCDAED	T	RAVERSE
ABCDAEE		ACTUALL Y
ABCDAEE		EXPRESS
ABCDAEE		THIRTEE N
ABCDAEEFAB		THIRTEENTH
ABCDAEFA	OV	ERWHELME D
ABCDAEFAB		INFLICTIN G
ABCDAEFB	P	RESCRIBE D
ABCDAEFBE	O	NEHUNDRED
ABCDAEFC	R	ADIOACTI VE
ABCDAEFC	M	ANUFACTU RE
ABCDAEFC	PR	ESIDENTI AL
ABCDAEFC	D	ISTRIBUT E
ABCDAEFCA	D	ISTRIBUTI NG
ABCDAEFCA	D	ISTRIBUTI ON
ABCDAEFD	F	LASHLIGH T
ABCDAEFD	C	ONTROVER SY
ABCDAEFD	A	SCENSION
ABCDAEFD		WINDWARD
ABCDAEFDB		RESTRICTE D
ABCDAEFDE		RESTRICTI ON
ABCDAEFE	PAR	ENTHESIS
ABCDAEFE		RETURNIN G
ABCDAEFEGE	RE	SPONSIBILI TY
ABCDAEFF		REDCROSS
ABCDAEFGAHB		INSPIRATION
ABCDAEFGC		REGARDING
ABCDAEFGD		RESTRAINT
ABCDAEFGFE	TR	ANSPACIFIC
ABCDAEFGHC		TWENTYFIVE
ABCDAEFGHFBC		CONSCRIPTION
ABCDBA	PR	ACTICA L
ABCDBA	W	ATERTA NK
ABCDBA		ENGINE
ABCDBA	S	ENTINE L
ABCDBA	R	EVOLVE
ABCDBA	S	ITUATI ON
ABCDBAA		ENGINEE R
ABCDBAAEDBC		ENGINEERING
ABCDBAB		LIABILI TY
ABCDBAD	RE	TALIATI ON
ABCDBAEAD	D	ISPOSITIO N
ABCDBAEBE	U	NEXPENDED
ABCDBBA		ANTENNA
ABCDBBA	D	ISCUSSI ON
ABCDBBDEA	TRA	NSMISSION
ABCDBCAEB		INTENTION
ABCDBEA		INCENDI ARY
ABCDBEA	PR	OTECTIO N
ABCDBEA	IN	TERCEPT
ABCDBEAB	IN	TERCEPTE D
ABCDBEAE	C	ONTINUOU S
ABCDBEAFB		INVENTION
ABCDBEAFCDB	QU	ARTERMASTER
ABCDBEAFD		INCENTIVE
ABCDBEAFD		INTENSIVE
ABCDBECA	E	NCIRCLIN G
ABCDBEFAGABC		ENTANGLEMENT
ABCDBEFAGEB		TEMPERATURE
ABCDBEFBA		DECREASED
ABCDBEFCDAB	C	ONTINUATION
ABCDBEFGA		YESTERDAY
ABCDBEFGAB		ARMOREDCAR
ABCDBEFGBCHIA		DISTINGUISHED
ABCDBEFGHA	P	ERFORMANCE
ABCDCA		AIRCRA FT
ABCDCA		CRITIC
ABCDCA		CRITIC AL
ABCDCA	D	EFICIE NT
ABCDCA		ENGAGE
ABCDCA	P	OSITIO N

Table D-3—*Continued*

ABCDCA	PR	OVISIO N	ABCDEA	CO	ASTGUA RD
ABCDCA	FI	REALAR M	ABCDEA	M	ATERIA L
ABCDCAAC		PHILIPPI NES	ABCDEA	S	ATURDA Y
ABCDCAB		ANTITAN K	ABCDEA	C	AUSEWA Y
ABCDCABCA	I	NDEPENDEN T	ABCDEA	N	AUTICA L
ABCDCAC		CRITICI SE	ABCDEA	ME	CHANIC
ABCDCAC		CRITICI SM	ABCDEA		CHEMIC AL
ABCDCAD		OPINION	ABCDEA		CONDUC T
ABCDCAEAB		ENGAGEMEN T	ABCDEA		DISLOD GE
ABCDCAEB	P	OSITIONS	ABCDEA		DOWNED
ABCDCAED	D	EFICIENC Y	ABCDEA	B	ECAUSE
ABCDCAED	PR	OVISIONS	ABCDEA	D	ECIPHE R
ABCDCAEFD		CHARACTER	ABCDEA	D	ECLARE
ABCDCAEFDGHEGA		CHARACTERISTIC	ABCDEA	OBJ	ECTIVE
ABCDCBABC	IN	TERPRETER	ABCDEA	L	ECTURE
ABCDCBCEA	HO	STILITIES	ABCDEA	V	EHICLE S
ABCDCEA	BRI	DGEHEAD	ABCDEA		ENCODE
ABCDCEA	M	EDICINE	ABCDEA	COMP	ENSATE
ABCDCEA	D	EFINITE	ABCDEA		ENTIRE
ABCDCEA	S	EPARATE	ABCDEA	R	EPLACE
ABCDCEA		SURPRIS E	ABCDEA	R	EPULSE D
ABCDCEAFC	QU	ALIFICATI ON	ABCDEA	CONSID	ERABLE
ABCDCEAFE	P	ERSISTENT	ABCDEA	INT	ERPOSE
ABCDCEBA		ELIGIBLE	ABCDEA	S	ERVICE
ABCDCECA	D	ESTITUTE	ABCDEA		EUROPE
ABCDCECDA	CO	NSTITUTIN G	ABCDEA		EUROPE AN
ABCDCEFGAB		PHOTOGRAPH Y	ABCDEA		EXCITE
ABCDCEFGCA	DEM	OBILIZATIO N	ABCDEA	T	HROUGH
ABCDCEFGCA	M	OBILIZATIO N	ABCDEA		IDENTI CAL
ABCDDA	R	ECOMME ND	ABCDEA		IDENTI FY
ABCDDA	T	OBACCO	ABCDEA		INHABI TED
ABCDDA		SHELLS	ABCDEA	D	IRECTI ON
ABCDDAB	B	EACHHEA D	ABCDEA		MEDIUM
ABCDDAEACBE		INEFFICIENC Y	ABCDEA	SY	NCHRON IZE
ABCDDAEFAF	R	ECOMMENDED	ABCDEA	JU	NCTION
ABCDDAEFGHICE	R	ECOMMENDATION	ABCDEA	CO	NFIDEN T
ABCDDEA		DROPPED	ABCDEA		NOTHIN G
ABCDDEA	AI	RSUPPOR T	ABCDEA	E	NTRAIN
ABCDDEA	A	RTILLER Y	ABCDEA	L	OCATIO N
ABCDDEAEC		COEFFICIE NT	ABCDEA	REV	OLUTIO N
ABCDDECDFA		SCHOOLHOUS E	ABCDEA	DEC	ORATIO N
ABCDDEFCGHA	MI	SCELLANEOUS	ABCDEA	T	ORPEDO
ABCDDEFEACGE		CLASSIFICATI ON	ABCDEA		OVERCO MING
ABCDDEFGGEDBA	R	ECONNAISSANCE	ABCDEA	T	RAILER S
ABCDEA		AERONA UTICS	ABCDEA	T	RAWLER
ABCDEA	R	AILHEA D	ABCDEA	DI	RECTOR
ABCDEA		AIRPLA NE	ABCDEA		REPAIR
ABCDEA		AMBULA NCE	ABCDEA	NO	RTHWAR D

Table D-3—*Continued*

ABCDEA	C	RUISER
ABCDEA	I	SLANDS
ABCDEA		STRIPS
ABCDEA		SUNRIS E
ABCDEA		TARGET
ABCDEA	NOR	THEAST
ABCDEA		THREAT
ABCDEA	NOR	THWEST
ABCDEA		TWELFT H
ABCDEA	L	UMINOU S
ABCDEAA		EIGHTEE N
ABCDEAAE		SUBMISSI ON
ABCDEAAFED		EIGHTEENTH
ABCDEAB		INVADIN G
ABCDEAB	F	LEXIBLE
ABCDEAB		NATIONA L
ABCDEAB		REPAIRE D
ABCDEAB		REQUIRE
ABCDEAB		RESTORE D
ABCDEAB	OU	TSKIRTS
ABCDEABA		DEMANDED
ABCDEABD		IMPEDIME NTA
ABCDEABE	AT	OMICBOMB
ABCDEABFB		REQUIREME NT
ABCDEABFD		NATIONALI SM
ABCDEABFDC		NATIONALIT Y
ABCDEABFE		MARKSMANS HIP
ABCDEABFFGHD		SHARPSHOOTER
ABCDEAC		AUTOMAT IC
ABCDEAC	AI	RCONTRO L
ABCDEAD		CONTACT
ABCDEAD	V	ICTORIO US
ABCDEAD	C	RUISERS
ABCDEADFD		THREATENE D
ABCDEAE		ENCODED
ABCDEAE	P	ERMANEN T
ABCDEAE		FORTIFI ED
ABCDEAE		REQUIRI NG
ABCDEAEFGC		TRADITIONA L
ABCDEAFA	R	EPLACEME NT
ABCDEAFAGE		EXCITEMENT
ABCDEAFAGHEAID		IDENTIFICATION
ABCDEAFB		CLERICAL
ABCDEAFB		INVASION
ABCDEAFBC		RESOURCES
ABCDEAFC	DES	IGNATION
ABCDEAFC	RES	IGNATION
ABCDEAFC	CO	NFIDENTI AL
ABCDEAFD	D	IMENSION
ABCDEAFE		ADJUTANT
ABCDEAFE		INTERIOR
ABCDEAFE	I	NFLUENCE
ABCDEAFF	R	EADINESS
ABCDEAFGA	D	ECIPHERME NT
ABCDEAFGAFB		MEDIUMBOMBE R
ABCDEAFGD		LEGISLATI ON
ABCDEAFGE	CO	MPARTMENT
ABCDEAFGEE		SMOKESCREE N
ABCDEBA		DELAYED
ABCDEBA	D	ETONATE
ABCDEBA		INDEMNI TY
ABCDEBA	D	ISPERSI ON
ABCDEBA		RECOVER
ABCDEBA		SURPLUS
ABCDEBAB		ARBITRAR Y
ABCDEBAED		ARBITRATI ON
ABCDEBFA	B	RIGADIER
ABCDEBFAGA		ENCOUNTERE D
ABCDEBFCAGBF		INTERNATIONA L
ABCDEBFDGA		NAVIGATION
ABCDEBFGAF	H	EADQUARTER S
ABCDEBFGHA	R	ESPONSIBLE
ABCDEBFGHBCGIA		NATURALIZATION
ABCDECA	E	NLISTIN G
ABCDECA		PRINCIP AL
ABCDECA		PRINCIP LE
ABCDECA		SKIRMIS H
ABCDECAB	I	NTERMENT
ABCDECAC	I	NTERVENE
ABCDECACFE	M	AINTENANCE
ABCDECAFCDA		TRANSATLANT IC
ABCDECBA		NEGLIGEN T
ABCDECBA		REVOLVER
ABCDECBA	P	ROTECTOR
ABCDECBAFB		NEGLIGENCE
ABCDECCFA		DISCUSSED
ABCDECDCAFC	I	NTERFERENCE
ABCDECFA		ENCIRCLE
ABCDECFA		EVACUATE
ABCDECFBA		SEAPLANES
ABCDECFEA		STANDARDS
ABCDEDA	N	EWSPAPE R
ABCDEDA		MARITIM E
ABCDEDA	CO	NTRABAN D
ABCDEDA	C	OALITIO N
ABCDEDA	BA	ROMETER

Table D-3—*Continued*

ABCDEDA	GY	ROMETER
ABCDEDA	HYD	ROMETER
ABCDEDA	HYG	ROMETER
ABCDEDA	PSYCH	ROMETER
ABCDEDAB	C	ONDITION
ABCDEDAC	REC	OGNITION
ABCDEDAFC	N	EWSPAPERS
ABCDEDFA		DICTATED
ABCDEDFA		EXCAVATE
ABCDEDFA		EXHIBITE D
ABCDEDFAC		ANTICIPAT E
ABCDEDFAC		CLEARANCE
ABCDEDFACDGB		ANTICIPATION
ABCDEDFCAB		INTERESTIN G
ABCDEDFCGAHB		INAUGURATION
ABCDEDFDA		ARTIFICIA L
ABCDEDFDEAB	C	ONSTITUTION
ABCDEDFDGHAIF		CHRONOLOGICAL
ABCDEDFGA	PR	OCLAMATIO N
ABCDEDFGA	P	RELIMINAR Y
ABCDEDFGABHED		INDETERMINATE
ABCDEDFGADB	P	RELIMINARIE S
ABCDEDFGHAGD		ADMINISTRATI VE
ABCDEDFGHAGDIE		ADMINISTRATION
ABCDEEA		ENROLLE D
ABCDEEA	P	ERSONNE L
ABCDEEA		IMPOSSI BLE
ABCDEEACB	S	IGNALLING
ABCDEEAFDBC		INTELLIGENT
ABCDEEAFDBGD		INTELLIGENCE
ABCDEEDFGBA		RECONNOITER
ABCDEEDFGBAFE		RECONNOITERIN G
ABCDEEFAB		ENROLLMEN T
ABCDEEFAB	C	ONFESSION
ABCDEEFAE		EMBASSIES
ABCDEEFDGFA		DISAPPEARED
ABCDEEFGCAHB		INTERRUPTION
ABCDEFA	C	ABLEGRA M
ABCDEFA		AMERICA N
ABCDEFA	C	AMOUFLA GE
ABCDEFA		CHRONIC AL
ABCDEFA		CONFLIC T
ABCDEFA	DIS	CREPANC Y
ABCDEFA	S	EABORNE
ABCDEFA		EMPLOYE R
ABCDEFA		ENCIPHE R
ABCDEFA		ENFORCE
ABCDEFA		ENLISTE D
ABCDEFA	D	EPLOYME NT
ABCDEFA		EQUIPME NT
ABCDEFA	FIGHT	ERPLANE
ABCDEFA		ESCORTE D
ABCDEFA	D	ESCRIBE
ABCDEFA	J	ETPLANE
ABCDEFA		EXCLUDE
ABCDEFA		INCLUSI VE
ABCDEFA		LOGICAL
ABCDEFA	F	ORMATIO N
ABCDEFA	T	RANSFER
ABCDEFA		REGULAR
ABCDEFA	P	RISONER
ABCDEFA		SAILORS
ABCDEFA		SECTORS
ABCDEFA		SERIOUS LY
ABCDEFA	E	STABLIS H
ABCDEFA		TONIGHT
ABCDEFAA		EMPLOYEE
ABCDEFAAF	T	RANSFERRE D
ABCDEFAAGC	T	RANSFERRIN G
ABCDEFAB		INCLUDIN G
ABCDEFAB		RADIOGRA M
ABCDEFAB	P	REMATURE
ABCDEFABA		EMPLACEME NT
ABCDEFAC		INTEGRIT Y
ABCDEFAC	P	RISONERS
ABCDEFACB	IN	TRODUCTOR Y
ABCDEFACD		ALTERNATE
ABCDEFACGF		ALTERNATIN G
ABCDEFAD		CONTRACT
ABCDEFAD	D	ESTROYER
ABCDEFAD		INTERVIE W
ABCDEFAD		OPERATOR
ABCDEFAD	FI	RECONTRO L
ABCDEFAD	P	ROCEDURE
ABCDEFADB	D	ESTROYERS
ABCDEFADF	T	RANSVERSE
ABCDEFAE	D	ISCONTIN UE
ABCDEFAEGHEC	D	ISCONTINUANC E
ABCDEFAF		EXPANDED
ABCDEFAF	I	MPROVEME NT
ABCDEFAFCD	R	ADIOSTATIO N
ABCDEFAGA		ENCIPHERE D
ABCDEFAGAB		ENFORCEMEN T
ABCDEFAGB	D	ETACHMENT
ABCDEFAGB		INFLATION
ABCDEFAGB		REINFORCE

Table D-3—*Continued*

ABCDEFAGB		TRAJECTOR Y	ABCDEFECACD		THERMOMETER
ABCDEFAGBDB		REIMBURSEME NT	ABCDEFECAE		CONFERENCE
ABCEDFAGBHBD		REINFORCEMEN T	ABCDEFEDCGCAHB		INTERPRETATION
ABCDEFAGC		INTERDICT	ABCDEFEFA	C	OMPETITIO N
ABCDEFAGCAHB		INTERDICTION	ABCDEFEGA	D	EMOBILIZE
ABCDEFAGE	D	EPARTMENT	ABCDEFEGA	C	OMPUTATIO N
ABCDEFAGEC	D	EPARTMENTA L	ABCDEFFA	UN	DERSTOOD
ABCDEFAGFD		REGISTRATI ON	ABCDEFFA		IMPRESSI ON
ABCDEFAGHAB		ENCIPHERMEN T	ABCDEFFAGE		IMPRESSIVE
ABCDEFAGHEBC		CONFISCATION	ABCDEFFEDAGBC		INSTALLATIONS
ABCDEFAGHFAIB		INVESTIGATION	ABCDEFFGAB	C	ONGRESSION AL
ABCDEFAGHFAIBE		INVESTIGATIONS	ABCDEFGA		DISARMED
ABCDEFAGHFD		INVESTIGATE	ABCDEFGA	M	ECHANIZE D
ABCDEFAGHIF	B	REAKTHROUGH	ABCDEFGA	T	ECHNIQUE
ABCDEFBA		DECLARED	ABCDEFGA	R	ECOGNIZE
ABCDEFBA		DEPARTED	ABCDEFGA	H	ELICOPTE R
ABCDEFBA		DEPLOYED	ABCDEFGA		ENFILADE
ABCDEFBA		DEPORTED	ABCDEFGA		EQUALIZE
ABCDEFBA		DETACHED	ABCDEFGA		EQUIVALE NT
ABCDEFBA		EMPLOYME NT	ABCDEFGA	D	ESIGNATE
ABCEDFBA		ENTRAINE D	ABCDEFGA		EXCHANGE
ABCDEFBA		REGISTER	ABCDEFGA		GROUPING
ABCDEFBA	P	ROJECTOR	ABCDEFGA		GUARDING
ABCDEFBAB		MEASUREME NT	ABCDEFGA		INSECURI TY
ABCDEFBABGHD		MEASUREMENTS	ABCDEFGA	D	IPLOMATI C
ABCDEFBGA		ENDURANCE	ABCDEFGA	E	NTRUCKIN G
ABCDEFBGBA		DECIPHERED	ABCDEFGA		NUMBERIN G
ABCDEFCA		ESTIMATE	ABCDEFGA		OBJECTIO N
ABCDEFCA		NORTHERN	ABCDEFGA		OPERATIO N
ABCDEFCAB		ESTIMATES	ABCDEFGA		SOLDIERS
ABCDEFCAD	D	OMINATION	ABCDEFGA	DI	SPATCHES
ABCDEFCAGFC		ESTIMATEDAT	ABCDEFGA		WITHDRAW
ABCDEFCBA		DETONATED	ABCDEFGA		WITHDREW
ABCDEFCCFA		DISTRESSED	ABCDEFGAB	D	ESPATCHES
ABCDEFCEA		DISPERSED	ABCDEFGAB	U	NDERSTAND
ABCDEFCGA		ELABORATE	ABCDEFGAB		WITHDRAWI NG
ABCDEFDA	D	EPARTURE	ABCDEFGABF		ENLISTMENT
ABCDEFDAB	C	USTOMHOUS E	ABCDEFGAC	I	NSTRUMENT
ABCDEFDBAB		INTERVENIN G	ABCDEFGAC	F	OUNDATION
ABCDEFDBCAGB		INTERVENTION	ABCDEFGACB	I	NSTRUMENTS
ABCDEFDEAB		INTERFERIN G	ABCDEFGAD		SOUTHEAST
ABCDEFDGAB	DEM	ONSTRATION	ABCDEFGAD		SOUTHWEST
ABCDEFDGAHCD		INTERMEDIATE	ABCDEFGADG		SOUTHWESTE RN
ABCDEFDGHA		HYDROGRAPH IC	ABCDEFGAEHBC		CONSTRUCTION
ABCDEFEA	R	EINSTATE	ABCDEFGAFE		IMPRACTICA BLE
ABCDEFEAB	F	INGERPRIN T	ABCDEFGAG		WITHDRAWA L
ABCDEFEAGACE	R	EINSTATEMENT	ABCDEFGAHB		INSPECTION
ABCDEFEAGDB		CERTIFICATE	ABCDEFGAHCGIDE		RECONSTRUCTION

Table D-3—*Continued*

ABCDEFGBA		DESCRIBED
ABCDEFGBA		DESTROYED
ABCDEFGBA		DETRAINED
ABCDEFGBA		REMAINDER
ABCDEFGBA		TRANSPORT
ABCDEFGBACAHGD		TRANSPORTATION
ABCDEFGBAE		TRANSPORTS
ABCDEFGBHA		ESTABLISHE D
ABCDEFGBHIAJC		ESTABLISHMENT
ABCDEFGCAG		CONFIDENCE
ABCDEFGCHEA		RANGEFINDER
ABCDEFGDAHB		INSTRUCTION
ABCDEFGDAHBC		INSTRUCTIONS
ABCDEFGDBFHA	CE	NTRALIZATION
ABCDEFGDHAIC		OBSTRUCTIONS
ABCDEFGDHFAE		ORGANIZATION
ABCDEFGEA	H	EAVYBOMBE R
ABCDEFGEHA	D	ESCRIPTIVE
ABCDEFGFABF	I	NCOMPETENCE
ABCDEFGFAG	I	NCOMPETENT
ABCDEFGGAG	H	EAVYLOSSES
ABCDEFGHA		CONSPIRAC Y
ABCDEFGHA		DOMINATED
ABCDEFGHA	C	ENTRALIZE
ABCDEFGHA		EXCLUSIVE
ABCDEFGHA		EXPANSIVE
ABCDEFGHA		EXPLOSIVE
ABCDEFGHA		MECHANISM
ABCDEFGHAB	C	ONSUMPTION
ABCDEFGHADB		INFORMATION
ABCDEFGHAGC		CONVALESCEN T
ABCDEFGHBA		DESIGNATED
ABCDEFGHBA		DESPATCHED
ABCDEFGHBIJA		DISORGANIZED
ABCDEFGHCAEB		INTRODUCTION
ABCDEFGHCAEB	D	ISCREPANCIES
ABCDEFGHDAB	C	ONFIRMATION
ABCDEFGHDGCA		NORTHWESTERN
ABCDEFGHDIJA		REVOLUTIONAR Y
ABCDEFGHEEHA		COUNTERATTAC K
ABCDEFGHFA	D	EMONSTRATE
ABCDEFGHFCAG		AGRICULTURAL
ABCDEFGHIA		DISPATCHED
ABCDEFGHIA		OBSERVATIO N
ABCDEFGHIA		SUBMARINES
ABCDEFGHIAB	C	ONVERSATION
ABCDEFGHIAE	C	OMPENSATION
ABCDEFGHIAF	R	OADJUNCTION
ABCDEFGHIDAB	C	ONSIDERATION
ABCDEFGHIFJA		SEARCHLIGHTS
ABCDEFGHIGBA		DEMONSTRATED
ABCDEFGHIJDA		SIMULTANEOUS

Table D-4. List of general digraphic idiomorphs.

			AB	AB				
–G	EN	ER	AL	AL	AR	M–		
		NE	ED	ED				
–P	RO	CE	ED	ED				
–S	UC	CE	ED	ED				
–D	ET	RA	IN	IN	G–			
		–L	IN	IN	G–			
		–M	IN	IN	G–			
	OB	TA	IN	IN	G–			
		QU	IN	IN	E–			
		RA	IN	IN	G–			
	RE	MA	IN	IN	G–			
		SH	IN	IN	G–			
	–T	RA	IN	IN	G–			
		CR	IS	IS				
PO	SI	TI	ON	ON				
		–A	RE	RE	EN	FO	RC	ED
		–A	SU	SU	AL			
		BO	TH	TH	E–			
		WI	TH	TH	E–			
	–P	AR	TI	TI	ON			
	RE	PE	TI	TI	ON			
			VI	VI	D–			

		AB	––	AB		
	–M	AI	NT	AI	N–	
	RE	AR	GU	AR	D–	
		CH	UR	CH		
		DE	CI	DE		
		DE	CO	DE		
		DI	VI	DI	NG	
	SP	EA	RH	EA	D–	
	–R	ED	UC	ED		
–S	CH	ED	UL	ED		
	–B	EE	NN	EE	DE	D–
		EM	BL	EM		
	AM	EN	DM	EN	T–	
CO	NT	EN	TM	EN	T–	
–S	EV	EN	TE	EN		
–S	EV	EN	TE	EN	TH	
		EN	TR	EN	CH	
		ER	AS	ER		

			AB	––	AB		
		TH	ER	EF	ER	EN	CE
		TH	ER	ES	ER	VE	
		WH	ER	EV	ER		
–C	AR	EL	ES	SN	ES	S–	
		SC	HO	OL	HO	US	E–
–I	LL	UM	IN	AT	IN	G–	
			IN	CL	IN	E–	
	–F	IR	IN	GL	IN	E–	
		MA	IN	TA	IN		
–I	NF	AL	LI	BI	LI	TY	
		–A	ME	ND	ME	NT	
		SO	ME	TI	ME		
		–O	NE	NI	NE		
			NO	TK	NO	WN	
			NO	WK	NO	WN	
–A	PP	OI	NT	ME	NT		
–C	ON	TE	NT	ME	NT		
		–C	OM	PR	OM	IS	E–
		–P	ON	TO	ON		
	–T	HR	OU	GH	OU	T–	
		–N	OW	KN	OW	N–	
			PH	OS	PH	OR	US
			PO	ST	PO	NE	
	TR	OO	PS	HI	PS		
		PA	RA	PH	RA	SE	
		–P	RE	FE	RE	NC	E–
			RE	FE	RE	NC	E–
	–T	HE	RE	FO	RE		
		–P	RE	PA	RE		
			RE	TI	RE		
			RE	VE	RE	NT	
		–C	RO	SS	RO	AD	S–
CA	RE	LE	SS	NE	SS		
		AT	TE	MP	TE	D–	
			TH	AT	TH	E–	
	–F	OR	TH	WI	TH		
–I	NV	ES	TI	GA	TI	ON	
		ES	TI	MA	TI	ON	
	–D	ES	TI	NA	TI	ON	
		AC	TI	VI	TI	ES	
		–H	UM	DR	UM		

Table D-4—*Continued*

			AB	--	--	AB			
		-P	AN	AM	AC	AN	AL		
			AR	BI	TR	AR	Y-		
			AS	SO	ON	AS			
		AC	CE	PT	AN	CE			
			EM	PL	AC	EM	EN	T-	
-Q	UA	RT	ER	MA	ST	ER			
	-I	NT	ER	PR	ET	ER			
	-A	CC	ES	SO	RI	ES			
			IN	CL	UD	IN	G-		
		-D	IR	EC	TF	IR	E-		
		TO	MO	RR	OW	MO	RN	IN	G-
		PA	NA	MA	CA	NA	L-		
		-I	NT	ER	ME	NT			
		-I	NT	ER	VE	NT	IO	N-	
		CO	NT	IN	GE	NT			
		-C	ON	DI	TI	ON			
	-T	OM	OR	RO	WM	OR	NI	NG	
			RA	DI	OG	RA	M-		
			RE	AS	SU	RE			
		-P	RE	MA	TU	RE			
-D	EF	EN	SI	VE	PO	SI	TI	ON	
		IN	TE	RD	IC	TE	D-		
	QU	AR	TE	RM	AS	TE	R-		
		IN	TE	RP	RE	TE	R-		
		IN	TE	RR	UP	TE	D-		
	-F	OR	TI	FI	CA	TI	ON		

		AB	--	--	--	AB		
		AR	MO	RE	DC	AR		
		EN	FO	RC	EM	EN	T-	
	RE	EN	FO	RC	EM	EN	TS	
		IN	DE	TE	RM	IN	AT	E-
		IN	TE	RE	ST	IN	G-	
		IN	TE	RF	ER	IN	G-	
		IN	TE	RV	EN	IN	G-	
	-I	NC	OM	PE	TE	NC	E-	
	-C	ON	GR	ES	SI	ON	AL	
-D	EM	ON	ST	RA	TI	ON		
	-C	ON	SU	MP	TI	ON		
		PH	OT	OG	RA	PH		
		TH	IR	TE	EN	TH		

	AB	--	--	--	--	AB
-I	NS	TA	LL	AT	IO	NS
-C	ON	CE	NT	RA	TI	ON
-C	ON	FL	AG	RA	TI	ON
-C	ON	SI	DE	RA	TI	ON

	AB	--	AB	AB	
	IN	CL	IN	IN	G-
MA	IN	TA	IN	IN	G-

Table D-5. List of Playfair digraphic idiomorphs.

			AB	BA				
		SC	AB	BA	RD			
			AF	FA	BL	E–		
			AF	FA	IR			
		–B	AG	GA	GE			
	–H	AW	AI	IA	N–			
			AL	LA	RE	AS		
		–B	AL	LA	ST			
		–F	AL	LA	CY			
	IN	ST	AL	LA	TI	ON	S–	
	–P	AR	AL	LA	X–			
			AP	PA	RA	TU	S–	
			AP	PA	RE	L–		
			AP	PA	RE	NT		
			AP	PA	RE	NT	LY	
			AR	RA	NG	E–		
			AR	RA	Y–			
		–B	AR	RA	CK	S–		
		–B	AR	RA	GE			
	–E	MB	AR	RA	SS	ED		
		–N	AR	RA	TI	ON		
			AS	SA	IL	AN	T–	
			AS	SA	UL	T–		
	–A	MB	AS	SA	DO	R–		
	–I	MP	AS	SA	BL	E–		
		–M	AS	SA	CR	E–		
		–P	AS	SA	GE			
			AT	TA	CH			
			AT	TA	CK			
			AT	TA	IN			
		–B	AT	TA	LI	ON		
		–R	AT	TA	N–			
			BO	OB	YT	RA	P–	
		IN	DE	ED				
		–W	EB	BE	D–			
			EF	FE	CT			
			EF	FE	CT	IV	E–	
	CO	MP	EL	LE	D–			
	–E	XC	EL	LE	NC	E–		
	–E	XC	EL	LE	NT			
	–E	XP	EL	LE	D–			
	–I	MP	EL	LE	D–			
		–P	EL	LE	T–			
	PR	OP	EL	LE	D–			
	–R	EP	EL	LE	D–			
	SH	EL	LE	D–				
	–H	EM	ME	DI	N–			
		ST	EM	ME	D–			
		ST	EP	PE	D–			
		AV	ER	RE	D–			
	CO	NF	ER	RE	D–			
	–I	NT	ER	RE	D–			
	–R	EF	ER	RE	D–			
			ES	SE	NC	E–		
			ES	SE	NT	IA	L–	
	AD	DR	ES	SE	S–			
–C	OM	PR	ES	SE	D–			
	CO	NF	ES	SE	D–			
	IM	PR	ES	SE	D–			
		–L	ES	SE	N–			
		–M	ES	SE	NG	ER		
		PR	ES	SE	D–			
	PR	OF	ES	SE	D–			
–P	RO	GR	ES	SE	D–			
	–S	TR	ES	SE	D–			
	–S	TR	ES	SE	S–			
		–V	ES	SE	L–			
	WI	TN	ES	SE	S–			
		AB	ET	TE	D–			
–C	IG	AR	ET	TE	S–			
		–B	ET	TE	R–			
		–L	ET	TE	R–			
	–E	IG	HT	TH	RE	E–		
		–R	IB	BI	NG			
	FO	RB	ID	DI	NG			
		–D	IF	FI	CU	LT		
		–B	IL	LI	ON			
		–F	IL	LI	NG			
		–K	IL	LI	NG			
		–M	IL	LI	ME	TE	R–	
		–M	IL	LI	NG			
		–M	IL	LI	ON			
		SH	IL	LI	NG			
		SP	IL	LI	NG			
		–T	IL	LI	NG			
		–W	IL	LI	NG			
			IM	MI	GR	AN	T–	
			IM	MI	GR	AT	IO	N–
			IM	MI	NE	NT		
		SW	IM	MI	NG			
	–B	EG	IN	NI	NG			
		SP	IN	NI	NG			
		–W	IN	NI	NG			

Table D-5—*Continued*

			AB	BA				
		CL	IP	PI	NG			
		SH	IP	PI	NG			
	–S	TR	IP	PI	NG			
			IR	RI	GA	TI	ON	
		–M	IS	SI	NG			
		–M	IS	SI	ON			
	–A	DM	IS	SI	ON			
		EM	IS	SI	ON			
		–H	IS	SI	NG			
	PE	RM	IS	SI	ON			
TR	AN	SM	IS	SI	ON			
		EM	IT	TI	NG			
		–F	IT	TI	NG			
	–S	PL	IT	TI	NG			
	PE	RM	IT	TI	NG			
–A	FT	ER	NO	ON				
	FO	RE	NO	ON				
			NO	ON	TI	ME		
		–F	OL	LO	W–			
		–H	OL	LO	W–			
		–C	OM	MO	N–			
		–C	OM	MO	TI	ON		
PO	SI	TI	ON	NO	RT	HO	F–	
	–R	EC	ON	NO	IT	ER		
			OP	PO	RT	UN	E–	
			OP	PO	RT	UN	IT	Y–
			OP	PO	SE			
			OP	PO	SI	TE		
			OP	PO	SI	TI	ON	
		–C	OR	RO	BO	RA	TE	
		–C	OR	RO	DE			
	–T	OM	OR	RO	W–			
		–B	OT	TO	M–			
		–C	OT	TO	N–			
		CA	RE	ER				
		–S	UC	CU	MB	ED		

			AB	––	BA		
		PR	AC	TI	CA	BL	E–
		PR	AC	TI	CA	L–	
		–T	AC	TI	CA	L–	
			EN	GI	NE	ER	
		–G	EN	UI	NE		
	–I	NT	ER	FE	RE		
	–I	NT	ER	FE	RE	NC	E–
	–P	EN	ET	RA	TE		
		–R	EV	OL	VE	R–	
			IN	FI	NI	TE	
		–D	IS	PO	SI	TI	ON
		–S	IT	UA	TI	ON	
		CA	NA	DI	AN		
VE	TE	RI	NA	RI	AN		
		NI	NE	TE	EN		
		NI	NE	TE	EN	TH	
			PE	RC	EP	TI	ON
		–P	RE	MI	ER		
	–S	UR	RE	ND	ER		
		DE	SE	RV	ES		
	–O	UR	SE	LV	ES		
		RE	SE	RV	ES		
			SE	RV	ES		
	TH	EM	SE	LV	ES		

Table D-5—*Continued*

	AB	--	--	BA	
	DE	BA	RK	ED	
	DE	CL	AR	ED	
	DE	FE	ND	ED	
	DE	MA	ND	ED	
	DE	PA	RT	ED	
	DE	PL	OY	ED	
	DE	PO	RT	ED	
	DE	SE	RT	ED	
	DE	TA	CH	ED	
PR	EC	ED	EN	CE	
	EM	PL	OY	ME	NT
	EN	TR	AI	NE	D–
	ME	AS	UR	EM	EN T–
	NE	GL	IG	EN	CE
	NO	TA	TI	ON	
	PA	RA	GR	AP	H––
	RE	CE	IV	ER	
	RE	CO	RD	ER	
	RE	GI	ST	ER	
	RE	PE	AT	ER	
	RE	PO	RT	ER	
	RE	VO	LV	ER	
–P	RO	JE	CT	OR	
AS	SE	MB	LI	ES	

	AB	--	--	--	BA	
	DE	SE	CR	AT	ED	
	DE	SI	GN	AT	ED	
	DE	SP	AT	CH	ED	
	EN	EM	YP	LA	NE	S–
–D	ET	ER	IO	RA	TE	
–S	EV	EN	TY	FI	VE	
	IR	RE	GU	LA	RI	TY
	NO	MI	NA	TI	ON	
	SU	SP	IC	IO	US	

AB	--	--	--	--	BA
DE	MO	NS	TR	AT	ED
NO	TI	FI	CA	TI	ON

Table D-6. List of four-square digraphic idiomorphs (grouped by number of significant letters in the idiomorphic pattern).

TWO LETTERS

	A-	A-	
B LO CK	AD	ED	
I NV	AD	ED	
D	AM	AG	E
CO MM	AN	DS	
I SL	AN	DS	
A IR PL	AN	ES	
E NE MY PL	AN	ES	
DE SI GN	AT	ED	
E ST IM	AT	ED	
I ND IC	AT	ED	
C	AV	AL	RY
N	AV	AL	
P RO	CE	DU	RE
ME	CH	AN	IZ ED
IM ME	DI	AT	EL Y
WI TH	DR	AW	
WI TH	DR	EW	
	EM	ER	GE NC Y
L IE UT	EN	AN	T
	FI	FT	EE N
	FI	FT	H
	FI	FT	Y
BR ID	GE	HE	AD
V	IC	IN	IT Y
W	IT	HD	RA W
A DD	IT	IO	NA L
A MM UN	IT	IO	N
CO ND	IT	IO	N
RE CO GN	IT	IO	N
E LE	ME	NT	
	MI	LI	TA RY
	MI	NI	MU M
	NI	NT	H
P	OI	NT	
T	OM	OR	RO W
RE	QU	ES	T
RE	QU	IR	E
P RI	SO	NE	R
RE SI	ST	AN	CE
D IS PO SI	TI	ON	
PO SI	TI	ON	
SO	UT	H	
SQ	UA	DR	ON
FI GH TE	RP	LA	NE
MO TO	RI	ZE	D
D EP AR TU	RE		
UN	US	UA	L

	A-	--	A-	
S	AB	OT	AG	E
D ET	AC	HM	EN	T
H	AS	BE	EN	
	BA	TT	AL	IO N
	BO	MB	ED	
	CA	SU	AL	TI ES
	CA	SU	AL	TY
	CO	MB	AT	
	CO	OR	DI	NA TE S
	DI	RE	CT	IO N
	DI	SP	AT	CH
ME	DI	UM	BO	MB ER
R OA	DJ	UN	CT	IO N
R	EP	LA	CE	ME NT
R	ET	RE	AT	
S	EV	ER	AL	
JU	NC	TI	ON	
CO	NF	IR	MA	TI ON
I	NF	OR	MA	TI ON
I	NT	EL	LI	GE NC E
	PA	TR	OL	
	SA	BO	TA	GE
	SE	VE	RE	
AC	TI	VI	TY	
A	TT	EN	TI	ON
S	UC	CE	SS	FU LL Y

	A-	--	--	A-	
	AR	TI	LL	ER	Y
	AT	TA	CK	ED	
R	EE	NF	OR	CE	
R	EE	NF	OR	CE	ME NT
	ID	EN	TI	FY	
	IM	PO	SS	IB	LE
	MO	VE	ME	NT	
E	MP	LA	CE	ME	NT
	PE	RS	ON	NE	L
A	RT	IL	LE	RY	

	A-	--	--	--	A-	
	CO	MM	UN	IC	AT	IO NS
	CO	NC	EN	TR	AT	E
R	EO	RG	AN	IZ	AT	IO N
	LI	EU	TE	NA	NT	
CO	NS	TR	UC	TI	ON	

Table D-6—*Continued*

A-	--	--	--	--	A-
CO	MM	IS	SI	ON	ED

			-B	-B				
		UN	AB	LE				
	OB	ST	AC	LE				
			AD	VA	NC	E		
			AG	AI	NS	T		
		R	AI	LH	EA	D		
	PR	EP	AR	AT	IO	N		
	A	SS	AU	LT				
		B	OM	BA	RD			
		A	IR	BO	RN	E		
		S	EA	BO	RN	E		
	A	DV	AN	CI	NG			
			VI	CI	NI	TY		
				DE	TA	CH		
				DE	TA	CH	ME	NT
		H	AV	EB	EE	N		
		M	OV	EM	EN	T		
				EN	EM	Y		
			R	ES	ER	VE		
			R	ET	UR	N		
				FL	AN	K		
				FO	LL	OW		
		B	AG	GA	GE			
				HA	SB	EE	N	
A	PP	RO	AC	HI	NG			
	L	AU	NC	HI	NG			
	I	MM	ED	IA	TE	LY		
		IN	IT	IA	TE			
			F	IF	TH			
		TE	RR	IT	OR	Y		
			S	IX	TY			
	M	IS	CE	LL	AN	EO	US	
			E	LE	VA	TI	ON	
			E	LE	VE	N		
				LI	AI	SO	N	
			DA	MA	GE			
				MO	RN	IN	G	
			U	NU	SU	AL		
				OB	JE	CT	IV	E
		C	OL	ON				
		C	OL	ON	EL			
SU	PE	RI	OR	IT	Y			
		M	OT	OR	IZ	ED		
			OU	TS	KI	RT	S	

			-B	-B		
	EQ	UI	PM	EN	T	
	A	VE	RA	GE		
	B	AR	RA	GE		
		AI	RC	RA	FT	
AN	TI	AI	RC	RA	FT	
			RE	MA	IN	
R	EQ	UI	RE	ME	NT	
	M	IS	SI	NG		
		P	ER	SO	NN	EL
	ES	TI	MA	TE	DA	T
		P	LA	TO	ON	
		S	UP	PL	Y	
		S	UP	PO	RT	
		NA	VA	LB	AS	E
		F	OR	WA	RD	
		WI	ND	WA	RD	

		-B	--	-B		
	C	AS	UA	LT	Y	
	P	AT	RO	LS		
B	AT	TL	ES	HI	PS	
			GE	NE	RA	L
W	IL	LA	TT	AC	K	
T	RA	NS	MI	SS	IO	N
R	EC	OG	NI	TI	ON	
T	RO	OP	SH	IP		
		RE	GI	ME	NT	
		CA	RR	IE	RS	
		MI	SS	IO	NS	
			TW	EN	TY	
	R	EQ	UE	ST	ED	

	-B	--	--	-B			
I	DE	NT	IF	IC	AT	IO	N
M	EC	HA	NI	ZE	D		
D	EP	LO	YM	EN	T		
M	ES	SE	NG	ER			
D	ES	TR	OY	ER			
A	IR	SU	PP	OR	T		
V	IS	IB	IL	IT	Y		
	ME	SS	EN	GE	R		
I	MP	AS	SA	BL	E		
I	MP	OS	SI	BL	E		
A	NT	IA	IR	CR	AF	T	

Table D-6—*Continued*

```
   -B -- -- -B

C |OM MA ND IN|G
  |OP ER AT IO|N
  |PR IS ON ER|
  |PR OC ED UR|E
  |RE EN FO RC|E
  |TR AN SP OR|TA TI ON
  |YE ST ER DA|Y
```

```
       -B -- -- -- -B

    R|EC OM ME ND ED|
     |HE AV YL OS SE|S
 R EC|OM ME ND AT IO|N
    C|OM MU NI CA TI|ON
 R EC|ON NO IT ER IN|G
```

THREE LETTERS

```
   A- A- A-

 |  N AV AL BA|SE
R| EQ UI SI TI|ON
```

```
A- A- -- A-

|RE QU ES TE|D
```

```
      -B -B -B

B OM|BA RD ME|NT
    |EL EM EN|TS
  EN|GA GE ME|NT
```

FOUR LETTERS

```
  AB A- -B

H|EA DQ UA|RT ER S
 |EL EV EN|
```

```
  AB -B A-

  |CA NC EL|
RE|CO NN AI|SS AN CE
```

```
AB -B -- A-

|AD VA NC ED|
|EN EM YT AN|KS
```

```
AB -- A- -B

|SI GH TI NG|
```

```
A- AB -B

|AD DI TI|ON AL
```

```
A- AB -- -B

|SO UT HW ES|T
```

```
  A- A- -B -B

W|IT HD RA WA|L
```

```
A- A- -- A- A-

|CO MM AN DI NG|
```

```
A- A- -- -B -B

|RE QU IR EM EN T|
```

```
  A- -B AB

M|OR NI NG|
P|OS TP ON|E
```

```
A- -B -B -- A-

|RE CO NN OI TE|R
```

```
A- -B -- AB

|IN TE RD IC|T
```

```
  A- -B -- A- -B

S|AT IS FA CT OR|Y
```

```
A- -- A- C- C-

|DI SP AT CH ES|
```

Table D-6—*Continued*

```
 A- -- -- C- A- C-
|RO AD JU NC TI ON|

         -B AB A-
   DI SP|OS IT IO|N
       P|OS IT IO|N
        |PR ES EN|T
      RE|PR ES EN|T

         -B A- AB
      RE|PE AT ED|

   -B A- A- -B
  |DE ST RO YE|R

 -B A- -B -- A-
|UN ID EN TI FI|ED

   -B A- -- AB
U|NS UC CE SS|FU L

 -B A- -- A- -B
|ME DI UM BO MB|ER

   -B A- -- -B A-
  |VI SI BI LI TY|

 -B A- -- -- AB
|IN FO RM AT IO|N

 -B A- -- -- A- -B
|IN ST AL LA TI ON|

   -B -D -B -- -D
  |CR OS SR OA DS|

     -B -D -D -B
   AI|RS UP PO RT|
```

```
   -B -D -- -D -B
  |IN ST RU CT IO|N
 C|ON ST RU CT IO|N

          -B -- A- AB
F IG HT|ER PL AN ES|

   -B -- A- -- -- AB
 E|ST AB LI SH ME NT|

  -B -- -B A- A-
 |EN CO UN TE RE|D

 -B -- -- -B -D -D
|RE IN FO RC EM EN|T
```

FIVE LETTERS

```
  A- -B AB -- -B
 |NA VA LA TT AC|K

      A- -B -- -B AB
 R EC|ON NA IS SA NC|E

  -B A- A- -- AB
 |DI ST RI BU TI|ON

      -B A- -B AB
   RE|PL AC EM EN|T

  -B -D -- -D -B -D
 |IN ST RU CT IO NS|
```

Table D-6—*Continued*

SIX LETTERS

```
  AB CB C- A-
P|OS IT IO NS|

  AB -D -D AB
C|ON DI TI ON
 |RA DI OG RA|M

 A- A- -B AB A-
|RE QU IS IT IO|N

     A- CB -- A- CB
Q UA|RT ER MA ST ER|

 A- CB -- CB A-
|SC HO OL HO US|E

 A- -- CB A- -- CB
|ID EN TI FI CA TI|ON

  -B AB AD -D
A|DM IN IS TR|AT IV E
```

SEVEN LETTERS

```
 -B AD -- -B -D AD
|RE EN FO RC EM EN|T
```

EIGHT LETTERS

```
 AB -B AD -- -B AD
|QU AR TE RM AS TE|R

 AB -B C- AB CB
|EM PL AC EM EN|T

 AB -D C- AD C- -B
|IN TE RD IC TI ON|
```

Table D-7. List of words containing like letters repeated at various intervals.

AA	RU	BBER
AA	RU	BBLE
AA	A	CCEPT
AA	A	CCEPTABLE
AA(5)A	A	CCEPTANCE
AA	A	CCESS
AA	A	CCESSORY
AA	A	CCIDENTAL
AA	A	CCOMPANY
AA	A	CCOMMODATION
AA(5)A	A	CCORDANCE
AA	A	CCORDING
AA	O	CCUPATION
AA	O	CCUPY
AA	SU	CCEEDED
AA	SU	CCESS
AA	SU	CCESSFUL
AA	SU	CCESSFULLY
AA	SU	CCESSIVE
AA	TOBA	CCO
AA	UNSU	CCESSFUL
AA	A	DD
AA	A	DDITIONAL
AA	A	DDRESS
AA(5)A	A	DDRESSED
AA	A	DDRESSES
AA	BE	DDING
AA	LA	DDER
AA	SU	DDEN
AA(1)A	AGR	EEMENT
AA	B	EEN
AA(1)A	BEENN	EEDED
AA(2)AA(1)A	B	EENNEEDED
AA(2)A	B	EETLE
AA	BETW	EEN
AA(1)A	BR	EEZE
AA(1)A	CH	EESE
AA	COFF	EE
AA	COMMAND	EER
AA	COMMITT	EE
AA	CR	EEK
AA	DECR	EE
AA	DEGR	EE
AA	EIGHT	EEN
AA	EIGHT	EENTH
AA	EMPLOY	EE
AA	ENGIN	EER
AA	ENGIN	EERING
AA	F	EEL
AA	F	EET
AA	FIFT	EEN
AA	FIFT	EENTH
AA	FL	EE
AA	FL	EET
AA	FOURT	EEN
AA	FOURT	EENTH
AA	HASB	EEN
AA	HAVEB	EEN
AA	IND	EED
AA	K	EEP
AA(1)A	K	EEPER
AA	M	EET
AA	NINET	EEN
AA	NINET	EENTH
AA	PROC	EED
AA(1)A	PROC	EEDED
AA(5)A	R	EENFORCE
AA(5)A(1)A	R	EENFORCEMENT
AA	R	EENLIST
AA(5)A	R	EENLISTED
AA(6)A	R	EENLISTMENT
AA	REFUG	EE
AA	SCR	EEN
AA	SCR	EENING
AA	S	EE
AA	S	EEN
AA	SEVENT	EEN
AA	SEVENT	EENTH
AA	SIXT	EEN
AA	SIXT	EENTH
AA	SMOKESCR	EEN
AA	SP	EED
AA	ST	EEL
AA	STR	EET
AA(1)A	SUCC	EEDED
AA	SW	EEPING
AA	THIRT	EEN
AA	THIRT	EENTH
AA	THR	EE
AA	W	EEK
AA	WH	EEL
AA	YANK	EE
AA	A	FFAIR
AA	CHAU	FFEUR
AA	COE	FFICIENT
AA	CO	FFEE

Table D-7—*Continued*

AA	DI	FFERENCE
AA	DI	FFERENT
AA	DI	FFICULT
AA	DI	FFICULTIES
AA	E	FFECT
AA	E	FFECTED
AA	E	FFECTIVE
AA	E	FFICIENT
AA	E	FFICIENCY
AA	E	FFORT
AA	GENERALSTA	FF
AA	INE	FFICIENCY
AA	JUMPO	FF
AA	O	FF
AA	O	FFEND
AA	O	FFENDED
AA	O	FFENSE
AA	O	FFENSIVE
AA	O	FFICE
AA	O	FFICER
AA	O	FFICIAL
AA	POSTO	FFICE
AA	STA	FF
AA	SU	FFER
AA	SU	FFERED
AA	SU	FFICIENT
AA	TRA	FFIC
AA(1)A	BA	GGAGE
AA	FO	GGY
AA	STRA	GGLER
AA	SU	GGEST
AA	TRI	GGER
AA	BEAC	HHEAD
AA	ACTUA	LLY
AA	A	LL
AA	A	LLEGE
AA	A	LLEGIANCE
AA	A	LLIED
AA	A	LLIES
AA	A	LLOCATION
AA	A	LLOTMENT
AA	A	LLOW
AA	A	LLOWANCE
AA	A	LLY
AA	ARTI	LLERY
AA	BA	LLISTICS
AA	BA	LLOON
AA	BE	LLIGERENT
AA	BI	LLET
AA	BI	LLETED
AA	BU	LLETIN
AA	CA	LL
AA	CANCE	LLATION
AA	CANCE	LLED
AA	CE	LL
AA	CHA	LLENGE
AA	CO	LLAPSED
AA	CO	LLECT
AA	CO	LLECTION
AA	CO	LLEGE
AA	CO	LLISION
AA	COMPE	LLED
AA	DISTI	LL
AA	DO	LLAR
AA	DRI	LL
AA	ENRO	LL
AA	ENRO	LLED
AA	ENRO	LLMENT
AA	EXPE	LLED
AA	FA	LL
AA	FA	LLING
AA	FE	LL
AA	FI	LLING
AA	FO	LLOW
AA	FU	LL
AA	HI	LL
AA	I	LL
AA(3)A	I	LLEGAL
AA	I	LLITERATE
AA	I	LLNESS
AA	I	LLUMINATE
AA	I	LLUMINATING
AA	I	LLUMINATION
AA	I	LLUSTRATE
AA	I	LLUSTRATION
AA	INSTA	LL
AA	INSTA	LLATIONS
AA	INTE	LLIGENCE
AA	INTE	LLIGENT
AA	KI	LLED
AA	KI	LLING
AA	MI	LLIMETER
AA	MISCE	LLANEOUS
AA	OSCI	LLATE
AA	PARA	LLAX

Table D-7—*Continued*

AA(1)A	PARA	LLEL
AA	PATRO	LLING
AA	PAYRO	LL
AA	RA	LLY
AA	REBE	LLION
AA	REFI	LL
AA	REFI	LLING
AA	REPE	LLED
AA	RESPECTFU	LLY
AA	SHE	LL
AA	SHE	LLED
AA	SHE	LLFIRE
AA	SHE	LLING
AA	SHE	LLS
AA	SIGNA	LLING
AA	SMA	LL
AA	SPE	LL
AA	SUCCESSFU	LLY
AA	VA	LLEY
AA	VI	LLAGE
AA	WE	LL
AA	WI	LL
AA	WI	LLATTACK
AA	ACCO	MMODATION
AA	A	MMETER
AA	A	MMUNITION
AA	CO	MMA
AA	CO	MMAND
AA	CO	MMANDANT
AA	CO	MMANDED
AA	CO	MMANDEER
AA	CO	MMANDER
AA	CO	MMANDING
AA	CO	MMENCE
AA(4)A	CO	MMENCEMENT
AA	CO	MMEND
AA	CO	MMENDATION
AA	CO	MMENT
AA	CO	MMERCE
AA	CO	MMISSARY
AA	CO	MMISSION
AA	CO	MMISSIONER
AA	CO	MMIT
AA(2)A	CO	MMITMENT
AA	CO	MMITTEE
AA	CO	MMON
AA	CO	MMUNICATE
AA	CO	MMUNICATION
AA	CO	MMUNIQUE
AA	CO	MMUTE
AA	HA	MMER
AA	I	MMEDIATE
AA	I	MMIGRATION
AA	INFLA	MMABLE
AA	JA	MMING
AA	RECO	MMEND
AA	RECO	MMENDATION
AA	RECO	MMENDED
AA	SU	MMARY
AA	SU	MMER
AA	SU	MMIT
AA	SU	MMON
AA	SWI	MMING
AA	A	NNEX
AA(2)A	A	NNOUNCE
AA(2)A(4)A	A	NNOUNCEMENT
AA	A	NNUAL
AA	ANTE	NNA
AA	BA	NNER
AA	BEE	NNEEDED
AA(1)A	BEGI	NNING
AA	CA	NNOT
AA	CHA	NNEL
AA(4)A	CO	NNECTING
AA(5)A	CO	NNECTION
AA	GU	NNER
AA	MA	NNER
AA(1)A	MA	NNING
AA	PERSO	NNEL
AA(1)A	PLA	NNING
AA(5)A	RECO	NNAISSANCE
AA	RECO	NNOITER
AA(6)A	RECO	NNOITERING
AA	RU	NNER
AA(1)A	RU	NNING
AA	TO	NNAGE
AA	AFTERN	OON
AA	ASS	OONAS
AA	BALL	OON
AA	B	OOK
AA	B	OOTH
AA	CODEB	OOK
AA	C	OOK
AA	C	OOPERATE
AA(6)A	C	OOPERATION
AA	C	OORDINATE

Table D-7—*Continued*

AA(7)A	C	OORDINATION	AA	MA	PPING
AA(2)A	F	OOTHOLD	AA	O	PPOSE
AA	FOREN	OON	AA	O	PPOSITE
AA	H	OOK	AA	O	PPOSITION
AA	L	OOK	AA	PHILI	PPINES
AA(1)A	L	OOKOUT	AA	REA	PPOINTED
AA	N	OON	AA	REA	PPOINTMENT
AA	PLAT	OON	AA	SHI	PPING
AA	PONT	OON	AA	STO	PPED
AA	PR	OOF	AA	SU	PPLIES
AA	SCH	OOL	AA	SU	PPLY
AA(2)A	SCH	OOLHOUSE	AA	SU	PPORT
AA	SHARPSH	OOTER	AA	SU	PPORTING
AA	S	OON	AA	SU	PPOSE
AA	SP	OOLS	AA	A	RRANGE
AA	SP	OONS	AA	A	RRANGEMENT
AA	TATT	OO	AA	A	RREST
AA	T	OO	AA	A	RRESTED
AA	T	OOK	AA	A	RRIVAL
AA	T	OOL	AA	A	RRIVE
AA	TR	OOPS	AA	BA	RRACKS
AA	TR	OOPSHIP	AA	BA	RRAGE
AA	TR	OOPSHIPS	AA	CA	RRIAGE
AA	UNDERST	OOD	AA(2)A	CA	RRIER
AA	W	OODED	AA	CA	RRY
AA	W	OODS	AA	CONFE	RRED
AA	AIRSU	PPORT	AA	CO	RRECT
AA	A	PPARATUS	AA	CO	RRECTED
AA	A	PPARENT	AA	CO	RRECTION
AA	A	PPARENTLY	AA	CO	RRECTNESS
AA	A	PPEAR	AA	CO	RRESPONDENCE
AA	A	PPEARANCE	AA	CO	RRESPONDING
AA	A	PPEARED	AA(3)A	CO	RRIDOR
AA	A	PPLICATION	AA	CU	RRENT
AA	A	PPLY	AA	DEFE	RRED
AA	A	PPOINT	AA	DE	RRICK
AA	A	PPOINTED	AA(1)A	E	RROR
AA	A	PPOINTMENT	AA	FE	RRY
AA	A	PPROACH	AA	GA	RRISON
AA(2)A	A	PPROPRIATE	AA	HU	RRICANE
AA	A	PPROVAL	AA	INTE	RRUPT
AA	A	PPROVE	AA	INTE	RRUPTED
AA	A	PPROXIMATE	AA	INTE	RRUPTION
AA	DISA	PPEAR	AA(5)A	I	RREGULAR
AA	DISA	PPEARANCE	AA(5)A	I	RREGULARITIES
AA	DISA	PPEARED	AA(5)A	I	RREGULARITY
AA	DRO	PPED	AA	I	RRIGATION
AA	HA	PPEN	AA(1)A	MI	RROR

Table D-7—*Continued*

AA	PREA	RRANGED	AA	CLA	SSIFICATION
AA	PREFE	RRED	AA	COMMI	SSARY
AA	SIE	RRA	AA	COMMI	SSION
AA(4)A	SU	RRENDER	AA	COMMI	SSIONER
AA(4)A	SU	RRENDERED	AA	COMPA	SS
AA	SU	RROUND	AA	COMPLETENE	SS
AA	TE	RRAIN	AA	COMPRE	SSED
AA	TE	RRIBLE	AA	CONCE	SSION
AA	TE	RRIFIC	AA	CONFE	SSION
AA(3)A	TE	RRITORY	AA	CONGRE	SS
AA(1)A	TE	RROR	AA	CONGRE	SSIONAL
AA	TOMO	RROW	AA	CORRECTNE	SS
AA	TRANSFE	RRED	AA	CRO	SS
AA	TRANSFE	RRING	AA	CRO	SSING
AA	TU	RRET	AA(4)A	CRO	SSROADS
AA	ACCE	SS	AA	DARKNE	SS
AA	ACCE	SSORY	AA	DEPRE	SSION
AA	ACRO	SS	AA	DISCU	SS
AA	ADDRE	SS	AA	DISCU	SSED
AA	ADDRE	SSED	AA	DISCU	SSION
AA(1)A	ADDRE	SSES	AA	DISMI	SS
AA	ADMI	SSION	AA	DISMI	SSAL
AA	AMBA	SSADOR	AA	DI	SSEMINATED
AA	ASPO	SSIBLE	AA	DI	SSEMINATION
AA	A	SSAULT	AA	DISTRE	SS
AA	A	SSEMBLE	AA	DISTRE	SSED
AA(6)A	A	SSEMBLIES	AA	DRE	SS
AA	A	SSEMBLY	AA	DRE	SSING
AA(4)A	ASSE	SSMENTS	AA(2)A	EMBA	SSIES
AA(1)AA(4)A	A	SSESSMENTS	AA	EMBA	SSY
AA	A	SSET	AA	EXCE	SS
AA(2)A	A	SSETS	AA	EXCE	SSIVE
AA	A	SSIGNED	AA	EXPRE	SS
AA	A	SSIGNMENT	AA	FORTRE	SS
AA(7)A	A	SSIGNMENTS	AA	GA	SSING
AA(1)A	A	SSIST	AA(1)A	GLA	SSES
AA(1)A	A	SSISTANCE	AA(1)A	HEAVYLO	SSES
AA(1)A	A	SSISTANT	AA	ILLNE	SS
AA	A	SSOCIATE	AA	IMPA	SSABLE
AA	A	SSOCIATION	AA	IMPO	SSIBLE
AA(4)A	A	SSOONAS	AA	IMPRE	SSED
AA	A	SSURANCE	AA	IMPRE	SSION
AA	A	SSURE	AA	IMPRE	SSIVE
AA	BUSINE	SS	AA	I	SSUE
AA	CARELE	SS	AA(2)A	I	SSUES
AA	CARELESSNE	SS	AA	I	SSUING
AA(2)AA	CARELE	SSNESS	AA	LE	SS
AA(1)A	CHA	SSIS	AA	LE	SSON

Table D-7—*Continued*

AA	LO	SS
AA(1)A	LO	SSES
AA	MA	SS
AA	ME	SS
AA	ME	SSAGE
AA(3)A	ME	SSAGES
AA	ME	SSENGER
AA	ME	SSING
AA	MI	SSILE
AA	MI	SSING
AA	MI	SSION
AA(3)A	MI	SSIONS
AA	NECE	SSARY
AA	NECE	SSITATE
AA	NECE	SSITY
AA	PA	SS
AA	PA	SSAGE
AA	PA	SSED
AA	PA	SSENGER
AA(1)A	PA	SSES
AA	PA	SSIVE
AA	PA	SSPORT
AA	PERMI	SSION
AA	POSSE	SSION
AA(1)AA	PO	SSESSION
AA	PO	SSIBLE
AA	PREPAREDNE	SS
AA	PRE	SS
AA	PRE	SSED
AA	PRE	SSURE
AA	PROGRE	SS
AA	PROGRE	SSIVE
AA	READINE	SS
AA	RECONNAI	SSANCE
AA	REDCRO	SS
AA	SE	SSION
AA	STRE	SS
AA	SUBMI	SSION
AA	SUCCE	SS
AA	SUCCE	SSFUL
AA	SUCCE	SSFULLY
AA	SUCCE	SSIVE
AA	TRANSMI	SSION
AA	UNLE	SS
AA	UNSUCCE	SSFUL
AA	USELE	SS
AA	VE	SSEL
AA(2)A	VE	SSELS
AA	WIRELE	SS
AA	WITNE	SS
AA(1)A	WITNE	SSES
AA	A	TTACH
AA(6)A	A	TTACHMENT
AA	A	TTACK
AA	A	TTAIN
AA(6)A	A	TTAINMENT
AA(3)A	A	TTEMPT
AA(3)A	A	TTEMPTED
AA(2)A	A	TTENTION
AA	BA	TTALION
AA	BA	TTEN
AA	BA	TTERED
AA	BA	TTERIES
AA	BA	TTERY
AA	BA	TTLE
AA	BA	TTLEFIELD
AA	BA	TTLESHIP
AA	BE	TTER
AA	BI	TTER
AA	BO	TTOM
AA	BOYCO	TT
AA	CIGARE	TTE
AA	COMMI	TTEE
AA	COUNTERA	TTACK
AA	FI	TTING
AA	GE	TTING
AA	LE	TTER
AA	LE	TTERED
AA	LI	TTER
AA	LI	TTLE
AA	NAVALA	TTACK
AA	NAVALBA	TTLE
AA	OMI	TTED
AA	SE	TTLE
AA	SPO	TTING
AA	SUBMI	TTED
AA	TA	TTOO
AA	THA	TTHE
AA	WILLA	TTACK
AA	WRI	TTEN
AA	MU	ZZLE
AA	NO	ZZLE
A(1)A		ABANDON
A(1)A		AGAIN
A(1)A		AGAINST
A(1)A		ALARM

Table D-7—*Continued*

A(1)A(2)A		ALASKA
A(1)A	ALM	ANAC
A(1)A		ANALYSIS
A(1)A		ANALYZE
A(1)A	APP	ARATUS
A(1)A	APPE	ARANCE
A(1)A(2)A		ARABIA
A(1)A(2)A		AVAILABLE
A(1)A		AWAIT
A(1)A		AWARD
A(1)A		AWAY
A(1)A	C	ALAMITY
A(1)A(1)A	C	ANADA
A(1)A	CAN	ADA
A(1)A	C	ANAL
A(1)A	C	APABILITY
A(1)A	C	APACITY
A(1)A	C	ATASTROPHE
A(1)A	C	AVALRY
A(1)A	CH	ARACTER
A(1)A	CH	ARACTERISTIC
A(1)A	CLE	ARANCE
A(1)A	COMB	ATANT
A(1)A	CONTR	ABAND
A(1)A	D	AMAGE
A(1)A	D	AMAGED
A(1)A	D	AMAGING
A(1)A	DISAPPE	ARANCE
A(1)A	EXC	AVATE
A(1)A	EXC	AVATION
A(1)A	EXPL	ANATION
A(1)A	F	ATAL
A(1)A	F	ATALITY
A(1)A	FIRE	ALARM
A(1)A	G	ARAGE
A(1)A	GENERAL	ALARM
A(1)A(1)A	GENER	ALALARM
A(1)A	J	APAN
A(1)A	M	ANAGE
A(1)A	M	ANAGEMENT
A(1)A	N	APALM
A(1)A	N	AVAL
A(1)A(2)A	NAV	ALATTACK
A(1)A(1)A(2)A	N	AVALATTACK
A(1)A(2)A	N	AVALBASE
A(1)A(2)A	N	AVALBATTLE
A(1)A	N	AVALFORCES
A(1)A	NONCOMB	ATANT
A(1)A	PAN	AMA
A(1)A(1)A	P	ANAMA
A(1)A	P	APA
A(1)A	P	ARACHUTE
A(1)A	P	ARADE
A(1)A(2)A	P	ARAGRAPH
A(1)A(2)A	P	ARALLAX
A(1)A	P	ARALLEL
A(1)A	PREP	ARATION
A(1)A	PROCL	AMATION
A(1)A	QU	ARANTINE
A(1)A	S	ALARY
A(1)A	SEP	ARATE
A(1)A	SEP	ARATION
A(1)A	T	AXATION
A(1)A	V	ACANCY
A(1)A	WITHDR	AWAL
A(1)A	PRO	BABLE
A(1)A	PRO	BABLY
A(1)A	BI	CYCLE
A(1)A		CYCLONE
A(1)A	MOTOR	CYCLE
A(1)A	BEENNEE	DED
A(1)A	BLOCKA	DED
A(1)A	BOMBAR	DED
A(1)A	COMMAN	DED
A(1)A	DECI	DED
A(1)A		DEDICATE
A(1)A		DEDICATION
A(1)A	DEFEN	DED
A(1)A	DEMAN	DED
A(1)A	ENCO	DED
A(1)A	EXPAN	DED
A(1)A	EXPEN	DED
A(1)A	EXTEN	DED
A(1)A	GROUN	DED
A(1)A	GUAR	DED
A(1)A	INVA	DED
A(1)A	LAN	DED
A(1)A	OFFEN	DED
A(1)A	PROCEE	DED
A(1)A	RAI	DED
A(1)A	RECOMMEN	DED
A(1)A	SUCCEE	DED
A(1)A	SUSPEN	DED
A(1)A	UNEXPEN	DED
A(1)A	WOO	DED
A(1)A	WOUN	DED

Table D-7—*Continued*

A(1)A		DID
A(1)A	AGRE	EMENT
A(1)A	ALL	EGE
A(1)A	AMM	ETER
A(1)A	AMUS	EMENT
A(1)A	ANNOUNC	EMENT
A(1)A	ARRANG	EMENT
A(1)A	BAROM	ETER
A(1)A	BATT	ERED
A(1)A	BEENNE	EDED
A(1)A	BELLIG	ERENT
A(1)A	BESI	EGED
A(1)A	BILL	ETED
A(1)A	BRE	EZE
A(1)A	BRIDG	EHEAD
A(1)A	CAR	ELESS
A(1)A(3)A	CAR	ELESSNESS
A(1)A	CEM	ETERY
A(1)A(1)A	C	EMETERY
A(1)A	CENT	ERED
A(1)A	CHE	ESE
A(1)A	COLL	EGE
A(1)A	COMMENC	EMENT
A(1)A	COMPL	ETE
A(1)A	COMPL	ETELY
A(1)A	COMPLET	ENESS
A(1)A(1)A	COMPL	ETENESS
A(1)A	CONCR	ETE
A(1)A(2)A	CONF	ERENCE
A(1)A	CONFIN	EMENT
A(1)A	CONQU	ERED
A(1)A	COV	ERED
A(1)A	CR	EDENTIAL
A(1)A(2)A	D	ECEMBER
A(1)A(7)A	D	ECENTRALIZE
A(1)A(7)A	D	ECENTRALIZED
A(1)A	DECIPH	ERED
A(1)A	D	EFEAT
A(1)A(2)A	D	EFEATED
A(1)A	D	EFECT
A(1)A	D	EFECTOR
A(1)A(4)A	D	EFECTIVE
A(1)A	D	EFEND
A(1)A(2)A	D	EFENDED
A(1)A(2)A	D	EFENDER
A(1)A(2)A	D	EFENSE
A(1)A(4)A	D	EFENSIVE
A(1)A	D	EFER
A(1)A(2)A	D	EFERRED
A(1)A	D	EPEND
A(1)A	D	EPENDABILITY
A(1)A(5)A	D	EPENDABLE
A(1)A(2)A	D	EPENDENT
A(1)A	D	ESERT
A(1)A(2)A	D	ESERTED
A(1)A(2)A	D	ESERTER
A(1)A	D	ETECTOR
A(1)A	D	ETENTION
A(1)A(6)A	D	ETERIORATE
A(1)A	D	ETERMINATION
A(1)A(4)A	D	ETERMINE
A(1)A(4)A	D	ETERMINED
A(1)A	D	EVELOP
A(1)A(3)A	D	EVELOPED
A(1)A(4)A	D	EVELOPMENT
A(1)A(2)A	DIFF	ERENCE
A(1)A	DIFF	ERENT
A(1)A	DISPLAC	EMENT
A(1)A	DYNAMOM	ETER
A(1)A		ELECTRICITY
A(1)A	EL	EMENT
A(1)A(1)A		ELEMENT
A(1)A	EL	EMENTARY
A(1)A(1)A		ELEMENTARY
A(1)A(3)A		ELEVATE
A(1)A		ELEVATION
A(1)A	EL	EVEN
A(1)A(1)A		ELEVEN
A(1)A	ELSEWH	ERE
A(1)A(2)A		EMERGENCY
A(1)A	EMPLAC	EMENT
A(1)A	ENCIPH	ERED
A(1)A	ENCOUNT	ERED
A(1)A(2)A		ENEMIES
A(1)A		ENEMY
A(1)A(6)A		ENEMYPLANES
A(1)A		ENEMYTANKS
A(1)A	ENFORC	EMENT
A(1)A	ENGAG	EMENT
A(1)A	ENTANGL	EMENT
A(1)A		EVERY
A(1)A	EXCIT	EMENT
A(1)A(5)A		EXECUTIVE
A(1)A(4)A		EXERCISE
A(1)A	EXTR	EME
A(1)A		EYE

Table D-7—*Continued*

A(1)A	F	EDERAL
A(1)A	G	ENERAL
A(1)A	G	ENERALALARM
A(1)A	G	ENERALSTAFF
A(1)A	GONIOM	ETER
A(1)A	GYROM	ETER
A(1)AA	HAV	EBEEN
A(1)A	H	ERE
A(1)A	HIND	ERED
A(1)A	HYDROM	ETER
A(1)A	HYGROM	ETER
A(1)A	IC	EBERG
A(1)A	IMPROV	EMENT
A(1)A(2)A	INCOMP	ETENCE
A(1)A	INCOMP	ETENT
A(1)A(2)A	IND	EPENDENT
A(1)A(6)A	IND	ETERMINATE
A(1)A	INT	EREST
A(1)A	INT	ERESTING
A(1)A	INTERF	ERE
A(1)A(2)A	INTERF	ERENCE
A(1)A	INTERPR	ETER
A(1)A	INTERV	ENE
A(1)A	KE	EPER
A(1)A	KILOM	ETER
A(1)A	LETT	ERED
A(1)A	L	EVEL
A(1)A	MANAG	EMENT
A(1)A	MEASUR	EMENT
A(1)A	MEASUR	EMENTS
A(1)A	M	ETEOROLOGICAL
A(1)A	M	ETER
A(1)A	MILLIM	ETER
A(1)A	MOV	EMENT
A(1)A	N	ECESSARY
A(1)A(6)A	N	ECESSITATE
A(1)A	N	ECESSITY
A(1)AA	NIN	ETEEN
A(1)AA	NIN	ETEENTH
A(1)A	OBSOL	ETE
A(1)A	ORD	ERED
A(1)A	PARENTH	ESES
A(1)A(4)A	P	ENETRATE
A(1)A	P	ENETRATION
A(1)A	PLAC	EMENT
A(1)A	PREC	EDE
A(1)A(1)A	PR	ECEDE
A(1)A(2)A	PREC	EDENCE
A(1)A(1)A(2)A	PR	ECEDENCE
A(1)A	PR	ECEDING
A(1)A	PR	EFER
A(1)A(2)A	PREF	ERENCE
A(1)A(1)A(2)A	PR	EFERENCE
A(1)A(2)A	PR	EFERRED
A(1)A	PR	ESENT
A(1)A	PR	ESERVATION
A(1)A(2)A	PR	ESERVE
A(1)A	PROCE	EDED
A(1)A	PSYCHROM	ETER
A(1)A	QU	EBEC
A(1)A	R	EBELLION
A(1)A	R	ECEIPT
A(1)A(2)A	R	ECEIVE
A(1)A(2)A	R	ECEIVER
A(1)A	R	ECEIVING
A(1)A(5)A	R	ECEPTACLE
A(1)A	REENFORC	EMENT
A(1)A	R	EFER
A(1)A(2)A	REF	ERENCE
A(1)A(1)A(2)A	R	EFERENCE
A(1)A	REIMBURS	EMENT
A(1)A	REINFORC	EMENT
A(1)A	REINSTAT	EMENT
A(1)A	R	EJECT
A(1)A(2)A	R	EJECTED
A(1)A	R	EJECTOR
A(1)A(2)A	R	ELEASE
A(1)A	RELI	EVE
A(1)A(2)A	R	EMEDIES
A(1)A	R	EMEDY
A(1)A(2)A	R	EMEMBER
A(1)A(2)A	R	EPEATED
A(1)A(2)A	R	EPEATER
A(1)A	R	EPEL
A(1)A(2)A	R	EPELLED
A(1)A	REPLAC	EMENT
A(1)A	REPR	ESENT
A(1)A	REPR	ESENTATION
A(1)A(6)A	REPR	ESENTATIVE
A(1)A	REQUIR	EMENT
A(1)A	R	ESEARCH
A(1)A	R	ESERVATION
A(1)A(2)A	R	ESERVE
A(1)A	R	ETENTION
A(1)A(2)A	R	EVENUE
A(1)A(2)A	R	EVERSE

Table D-7—*Continued*

A(1)A	REVI	EWED
A(1)A	SCH	EME
A(1)A	SEAL	EVEL
A(1)A	S	ELECT
A(1)A(2)A	S	ELECTED
A(1)A	S	EVEN
A(1)A(2)AA	S	EVENTEEN
A(1)A(2)AA	S	EVENTEENTH
A(1)A	S	EVENTH
A(1)A	S	EVENTY
A(1)A(6)A	S	EVENTYFIVE
A(1)A	S	EVERAL
A(1)A	SEV	ERE
A(1)A(1)A	S	EVERE
A(1)A	SI	EGE
A(1)A	SPH	ERE
A(1)A	STAT	EMENT
A(1)A	SUCCE	EDED
A(1)A	SUFF	ERED
A(1)A	SURREND	ERED
A(1)A	T	ELEGRAM
A(1)A(4)A	T	ELEPHONE
A(1)A	TH	ERE
A(1)A(3)A	TH	EREFORE
A(1)A	THERMOM	ETER
A(1)A	TH	ESE
A(1)A	THREAT	ENED
A(1)A	US	ELESS
A(1)A	V	ETERINARIAN
A(1)A	W	ERE
A(1)A	WH	ERE
A(1)A	WIR	ELESS
A(1)A		FIFTEEN
A(1)A		FIFTEENTH
A(1)A		FIFTH
A(1)A		FIFTY
A(1)A	BAG	GAGE
A(1)A	EN	GAGE
A(1)A	EN	GAGEMENT
A(1)A(2)A	EN	GAGING
A(1)A	EIG	HTH
A(1)A	WIT	HTHE
A(1)A	ACTIV	ITIES
A(1)A(1)A	ACT	IVITIES
A(1)A	ACT	IVITY
A(1)A	ADD	ITIONAL
A(1)A(5)A	ADM	INISTRATION
A(1)A(5)A	ADM	INISTRATIVE
A(1)A	ADV	ISING
A(1)A	AMMUN	ITION
A(1)A	ANT	IAIRCRAFT
A(1)A	ANT	ICIPATE
A(1)A(3)A	ANT	ICIPATION
A(1)A	ARTIF	ICIAL
A(1)A(1)A	ART	IFICIAL
A(1)A	AUDIB	ILITY
A(1)A(1)A	AUD	IBILITY
A(1)A	CAPAB	ILITY
A(1)A	CERT	IFICATE
A(1)A	CIV	ILIAN
A(1)A(1)A	C	IVILIAN
A(1)A(3)A	CLASS	IFICATION
A(1)A	COAL	ITION
A(1)A	COEFF	ICIENT
A(1)A	COLL	ISION
A(1)A	COLL	ISIONS
A(1)A	COMPET	ITION
A(1)A	COMPOS	ITION
A(1)A(2)A	CONC	ILIATION
A(1)A	COND	ITION
A(1)A	CR	ISIS
A(1)A	CR	ITIC
A(1)A	CR	ITICAL
A(1)A	CRIT	ICISE
A(1)A(1)A	CR	ITICISE
A(1)A	CRIT	ICISM
A(1)A(1)A	CR	ITICISM
A(1)A	CR	ITIQUE
A(1)A	DEC	ISION
A(1)A	DEF	ICIENCY
A(1)A	DEF	ICIENT
A(1)A	DEF	INITE
A(1)A	DEFIN	ITION
A(1)A(1)A	DEF	INITION
A(1)A(3)A	DEMOB	ILIZATION
A(1)A	DEMOB	ILIZE
A(1)A	DEPENDAB	ILITY
A(1)A	DETRA	INING
A(1)A	DIET	ITIAN
A(1)A	DIM	INISH
A(1)A(1)A	D	IMINISH
A(1)A	DIR	IGIBLE
A(1)A(1)A	D	IRIGIBLE
A(1)A	D	ISINFECT
A(1)A	D	ISINFECTED
A(1)A	DISPOS	ITION

Table D-7—*Continued*

A(1)A	D	IVIDE	A(1)A(3)A	MOB	ILIZATION
A(1)A	DIV	IDING	A(1)A	MOB	ILIZE
A(1)A(1)A	D	IVIDING	A(1)A	MUN	ITIONS
A(1)A	DIV	ISION	A(1)A	OBTA	INING
A(1)A(1)A	D	IVISION	A(1)A	OFF	ICIAL
A(1)A	EFF	ICIENCY	A(1)A	OP	INION
A(1)A	EFF	ICIENT	A(1)A	OPPOS	ITION
A(1)A	ELECTR	ICITY	A(1)A	PAC	IFIC
A(1)A	EL	IGIBLE	A(1)A	PART	ITION
A(1)A	ENTERPR	ISING	A(1)A(2)A	PH	ILIPPINES
A(1)A	EXH	IBITED	A(1)A	POL	ITICAL
A(1)A	EXHIB	ITION	A(1)A	POL	ITICS
A(1)A(1)A	EXH	IBITION	A(1)A	POS	ITION
A(1)A	EXPED	ITING	A(1)A	POS	ITIONS
A(1)A	EXPED	ITION	A(1)A	POS	ITIVE
A(1)A	FACIL	ITIES	A(1)A	PRA	IRIE
A(1)A(1)A	FAC	ILITIES	A(1)A(3)A	PREL	IMINARIES
A(1)A	F	ILING	A(1)A	PREL	IMINARY
A(1)A	F	INISH	A(1)A	PROH	IBIT
A(1)A	F	IRING	A(1)A	PROV	ISION
A(1)A	FORT	IFIED	A(1)A	PROV	ISIONS
A(1)A	HOSTIL	ITIES	A(1)A	PROX	IMITY
A(1)A(1)A	HOST	ILITIES	A(1)A(3)A	QUAL	IFICATION
A(1)A	HOST	ILITY	A(1)A	RA	IDING
A(1)A(3)A	IDENT	IFICATION	A(1)A	RA	INING
A(1)A	IGN	ITION	A(1)A	RECE	IVING
A(1)A	INCL	INING	A(1)A	RECOGN	ITION
A(1)A	IND	IVIDUAL	A(1)A	RECRU	ITING
A(1)A	INEFF	ICIENCY	A(1)A	REMA	INING
A(1)A	IN	ITIAL	A(1)A	REQU	IRING
A(1)A(1)A		INITIAL	A(1)A	REQUIS	ITION
A(1)A	IN	ITIATE	A(1)A(1)A	REQU	ISITION
A(1)A(1)A		INITIATE	A(1)A	RESPONSIB	ILITY
A(1)A	IRREGULAR	ITIES	A(1)A(1)A	RESPONS	IBILITY
A(1)A	LIAB	ILITY	A(1)A	RET	IRING
A(1)A	L	IAISON	A(1)A	R	IDING
A(1)A	L	IMIT	A(1)A	R	IGID
A(1)A(3)A	L	IMITATION	A(1)A	SEMIR	IGID
A(1)A	LIM	ITING	A(1)A(1)A	SEM	IRIGID
A(1)A(1)A	L	IMITING	A(1)A	SERV	ICING
A(1)A	L	INING	A(1)A	SIGN	IFICANCE
A(1)A	MAR	ITIME	A(1)A	SIGN	IFICANT
A(1)A	MED	ICINE	A(1)A	S	IMILAR
A(1)A	M	ILITARY	A(1)A(3)A	S	IMILARITY
A(1)A	MIL	ITIA	A(1)A	SPEC	IFIC
A(1)A(1)A	M	ILITIA	A(1)A(3)A	SPEC	IFICATION
A(1)A	M	INIMUM	A(1)A	SUFF	ICIENT
A(1)A	M	INING	A(1)A	SUITAB	ILITY

Table D-7—*Continued*

A(1)A	SUSP	ICION
A(1)A	SUSP	ICIONS
A(1)A	SUSP	ICIOUS
A(1)A	TERR	IFIC
A(1)A	TRAD	ITIONAL
A(1)A	TRA	INING
A(1)A	TRANSPAC	IFIC
A(1)A	UNIDENT	IFIED
A(1)A	UT	ILITY
A(1)A(1)A	UT	ILIZE
A(1)A(3)A	VER	IFICATION
A(1)A	VIC	INITY
A(1)A(1)A	V	ICINITY
A(1)A	VISIB	ILITY
A(1)A(1)A	VIS	IBILITY
A(1)A(1)A(1)A	V	ISIBILITY
A(1)A	V	ISIBLE
A(1)A	V	ISIT
A(1)A	V	ISITOR
A(1)A	V	ISITS
A(1)A	W	IRING
A(1)A	GENERA	LALARM
A(1)A	PARAL	LEL
A(1)A	AR	MAMENT
A(1)A	DYNA	MOMETER
A(1)A	MAXI	MUM
A(1)A		MEMBER
A(1)A		MEMORANDA
A(1)A(6)A		MEMORANDUM
A(1)A		MEMORIAL
A(1)A	MINI	MUM
A(1)A	RE	MEMBER
A(1)A	THER	MOMETER
A(1)A	A	NONYMOUS
A(1)A	BEGIN	NING
A(1)A	CONCER	NING
A(1)A	CONTI	NENTAL
A(1)A	DETRAI	NING
A(1)A	DOMI	NANCE
A(1)A	DOMI	NANT
A(1)A	INCLI	NING
A(1)A	INTERVE	NING
A(1)A	LIEUTE	NANT
A(1)A	LI	NING
A(1)A	MAINTE	NANCE
A(1)A	MAN	NING
A(1)A	MI	NING
A(1)A	MOR	NING
A(1)A		NINE
A(1)A(4)A		NINETEEN
A(1)A(4)A		NINETEENTH
A(1)A		NINETY
A(1)A		NINTH
A(1)A(7)A		NONCOMBATANT
A(1)A	OBTAI	NING
A(1)A	ORD	NANCE
A(1)A	PERMA	NENT
A(1)A	PLAN	NING
A(1)A	RAI	NING
A(1)A	REMAI	NING
A(1)A	RETUR	NING
A(1)A	RUN	NING
A(1)A	SCREE	NING
A(1)A	TRAI	NING
A(1)A(2)A	U	NKNOWN
A(1)A	AUT	OMOBILE
A(1)A	CHRON	OLOGICAL
A(1)A(1)A	CHR	ONOLOGICAL
A(1)A	C	OLON
A(1)A	C	OLONEL
A(1)A	C	OLORS
A(1)A	EC	ONOMIC
A(1)A	H	ONOR
A(1)A	LOC	OMOTIVE
A(1)A(1)A	L	OCOMOTIVE
A(1)A	LO	OKOUT
A(1)A	METEOR	OLOGICAL
A(1)A(1)A	METE	OROLOGICAL
A(1)A	MON	OPOLY
A(1)A(1)A	M	ONOPOLY
A(1)A	M	OTOR
A(1)A	M	OTORCYCLE
A(1)A	M	OTORIZED
A(1)A	PH	OTOGRAPHY
A(1)A	PR	OMOTE
A(1)A(2)A	PR	OMOTION
A(1)A(3)A	PR	OPORTION
A(1)A	PR	OPOSALS
A(1)A	PR	OPOSE
A(1)A	PROT	OCOL
A(1)A(1)A	PR	OTOCOL
A(1)A	PR	OVOST
A(1)A	RIG	OROUS
A(1)A	SEMIC	OLON
A(1)A(2)A	T	OMORROW
A(1)A	T	OPOGRAPHIC

Table D-7—*Continued*

A(1)A	VIG	OROUS
A(1)A	NEWS	PAPER
A(1)A	NEWS	PAPERS
A(1)A		PAPA
A(1)A		PIPE
A(1)A		POPULATED
A(1)A		POPULATION
A(1)A	AI	RCRAFT
A(1)A	ANTIAI	RCRAFT
A(1)A	ARBIT	RARY
A(1)A	CA	RTRIDGE
A(1)A	D	RYRUN
A(1)A	ENTE	RPRISE
A(1)A	ENTE	RPRISING
A(1)A	ER	ROR
A(1)A	FINGE	RPRINT
A(1)A	FO	RTRESS
A(1)A	INTE	RPRETATION
A(1)A(3)A	INTE	RPRETER
A(1)A	LIB	RARY
A(1)A	MIR	ROR
A(1)A	NEA	RER
A(1)A	SU	RPRISE
A(1)A	TER	ROR
A(1)A	ADDRES	SES
A(1)A	ANALY	SIS
A(1)AA	AS	SESSMENT
A(1)AA(4)A	AS	SESSMENTS
A(1)A	AS	SIST
A(1)A	AS	SISTANCE
A(1)A	AS	SISTANT
A(1)A	CA	SES
A(1)A	CHAS	SIS
A(1)A	CRI	SIS
A(1)A	CLAS	SES
A(1)A	DEFEN	SES
A(1)A	DI	SASTER
A(1)A	EXERCI	SES
A(1)A	EXPEN	SES
A(1)A	HEAVYLOS	SES
A(1)A	LOS	SES
A(1)A	OUTPO	STS
A(1)A	PARENTHE	SES
A(1)A	PARENTHE	SIS
A(1)A	PAS	SES
A(1)A	PER	SISTENT
A(1)AA	POS	SESSION
A(1)A	PROTE	STS
A(1)A	PURPO	SES
A(1)A	RE	SIST
A(1)A	RE	SISTANCE
A(1)AA		SESSION
A(1)A	SUB	SISTENCE
A(1)A		SUSPECTED
A(1)A		SUSPEND
A(1)A		SUSPENDED
A(1)A(3)A		SUSPENSE
A(1)A(3)A		SUSPENSION
A(1)A		SUSPICION
A(1)A(6)A		SUSPICIONS
A(1)A(6)A		SUSPICIOUS
A(1)A		SYSTEM
A(1)A	WITNES	SES
A(1)A	AL	TITUDE
A(1)A	AN	TITANK
A(1)A	CI	TATION
A(1)A	COMPE	TITION
A(1)A	COMPU	TATION
A(1)A	CONSTI	TUTE
A(1)A(1)A	CONS	TITUTE
A(1)A	CONSTI	TUTING
A(1)A(1)A	CONS	TITUTING
A(1)A	CONSTI	TUTION
A(1)A(1)A	CONS	TITUTION
A(1)A	DESTI	TUTE
A(1)A(1)A	DES	TITUTE
A(1)A	DIC	TATED
A(1)A	DIC	TATOR
A(1)A	DIE	TITIAN
A(1)A	INSTI	TUTION
A(1)A(1)A	INS	TITUTION
A(1)A	INTERPRE	TATION
A(1)A	INVI	TATION
A(1)A	LA	TITUDE
A(1)A	LIMI	TATION
A(1)A	NECESSI	TATE
A(1)A	PAR	TITION
A(1)A	RADIOS	TATION
A(1)A	REINS	TATE
A(1)A(4)A	REINS	TATEMENT
A(1)A	REPRESEN	TATIONS
A(1)A	REPRESEN	TATIVE
A(1)A	SANI	TATION
A(1)A(4)A	S	TATEMENT
A(1)A	S	TATES
A(1)A	S	TATION

Table D-7—*Continued*

A(1)A	S	TATIONS
A(1)A(2)A	S	TATISTICS
A(1)A	S	TATUS
A(1)A	SUBSTI	TUTE
A(1)A(1)A	SUBS	TITUTE
A(1)A	SUBSTI	TUTION
A(1)A(1)A	SUBS	TITUTION
A(1)AA		TATTOO
A(1)A	TEN	TATIVE
A(1)A		TITLE
A(1)A		TOTAL
A(1)A		TOTALING
A(1)A	TRANSPOR	TATION
A(1)A	UNITEDS	TATES
A(1)A	WI	THTHE
A(1)A	A	UGUST
A(1)A	CONTIN	UOUS
A(1)A	F	UTURE
A(1)A	INA	UGURATION
A(1)A	UN	USUAL
A(1)A(1)A		UNUSUAL
A(1)A		USUAL
A(1)A	Z	ULU
A(1)A	SUR	VIVED
A(1)A	A	WKWARD
A(2)A		ADJACENT
A(2)A		ADVANCE
A(2)A		ADVANCED
A(2)A		ADVANCING
A(2)A	ADV	ANTAGE
A(2)A(2)A		ADVANTAGE
A(2)A	ADV	ANTAGEOUS
A(2)A(2)A		ADVANTAGEOUS
A(2)A		AFFAIR
A(2)A	AL	ASKA
A(2)A		ALFA
A(2)A(1)A		ALMANAC
A(2)A		ALWAYS
A(2)A	AMB	ASSADOR
A(2)A(2)A		AMBASSADOR
A(2)A(1)A		APPARATUS
A(2)A		APPARENT
A(2)A		APPARENTLY
A(2)A	AR	ABIA
A(2)A		AREA
A(2)A		ARMAMENT
A(2)A		ARRANGE
A(2)A		ARRANGEMENT
A(2)A		ASIA
A(2)A		ASIATIC
A(2)A		ASSAULT
A(2)A		ATLANTIC
A(2)A		ATTACH
A(2)A		ATTACHMENT
A(2)A		ATTACK
A(2)A		ATTAIN
A(2)A		ATTAINMENT
A(2)A	AV	AILABLE
A(2)A		AVIATION
A(2)A		AVIATOR
A(2)A	B	AGGAGE
A(2)A	B	ARRACKS
A(2)A	B	ARRAGE
A(2)A	B	ATTALION
A(2)A	C	AMPAIGN
A(2)A	C	ANVAS
A(2)A	C	APTAIN
A(2)A	C	ASUAL
A(2)A	C	ASUALTIES
A(2)A	C	ASUALTY
A(2)A	CH	APLAIN
A(2)A	CO	ASTAL
A(2)A	COMM	ANDANT
A(2)A	COUNTER	ATTACK
A(2)A	DEB	ARKATION
A(2)A	DI	AGRAM
A(2)A	EMB	ARKATION
A(2)A	EV	ACUATE
A(2)A	EV	ACUATING
A(2)A	EV	ACUATION
A(2)A	EV	ALUATION
A(2)A	GR	ADUAL
A(2)A	INFL	AMMABLE
A(2)A	INST	ALLATIONS
A(2)A	INST	ANTANEOUS
A(2)A	J	ANUARY
A(2)A	M	ANDATE
A(2)A	M	ANDATED
A(2)A	M	ANUAL
A(2)A	MEMOR	ANDA
A(2)A	NAVAL	ATTACK
A(2)A	NAV	ALBASE
A(2)A	NAV	ALBATTLE
A(2)A	P	ACKAGE
A(2)A	PAR	AGRAPH
A(2)A	PAR	ALLAX
A(2)A	P	ASSAGE

Table D-7—*Continued*

A(2)A	PRE	ARRANGED	A(2)A		CONCLUDE
A(2)A	R	ADIAL	A(2)A		CONCLUSION
A(2)A	R	ADIATE	A(2)A		CONCRETE
A(2)A	R	ADIATION	A(2)A	EN	CIRCLE
A(2)A	RET	ALIATION	A(2)A	EN	CIRCLING
A(2)A	SE	APLANES	A(2)A	IMPRA	CTICABLE
A(2)A	ST	ANDARD	A(2)A	PRA	CTICAL
A(2)A	ST	ANDARDS	A(2)A	SE	CRECY
A(2)A	TH	ATHAVE	A(2)A	SIGNIFI	CANCE
A(2)A	TRANS	ATLANTIC	A(2)A	TA	CTICAL
A(2)A(2)A	TR	ANSATLANTIC	A(2)A	TA	CTICS
A(2)A	V	ARIATION	A(2)A	VA	CANCY
A(2)A	VETERIN	ARIAN	A(2)A	HUN	DRED
A(2)A	W	ARFARE	A(2)A	IN	DEED
A(2)A	WILL	ATTACK	A(2)A	ONEHUN	DRED
A(2)A	ATOMIC	BOMB	A(2)A	STAN	DARD
A(2)A		BARBED	A(2)A	STAN	DARDS
A(2)A		BOMB	A(2)A	ABS	ENCE
A(2)A		BOMBARD	A(2)A	ADDR	ESSED
A(2)A		BOMBARDED	A(2)A	ADDR	ESSES
A(2)A		BOMBARDMENT	A(2)A	AGR	EEMENT
A(2)A		BOMBER	A(2)A	APP	EARED
A(2)A		BRIBE	A(2)A	ARR	ESTED
A(2)A		BRIBERY	A(2)A	BATT	ERIES
A(2)A		BULB	A(2)A	BATTL	EFIELD
A(2)A	HEAVY	BOMBER	A(2)A	BEENN	EEDED
A(2)A	LIGHT	BOMBER	A(2)AA(1)A	BE	ENNEEDED
A(2)A	MEDIUM	BOMBER	A(2)A	BE	ETLE
A(2)A		CANCEL	A(2)A(1)A	B	ESIEGED
A(2)A		CANCELLATION	A(2)A	B	ETTER
A(2)A		CANCELLED	A(2)AA	B	ETWEEN
A(2)A		CHECK	A(2)A	BR	EEZE
A(2)A		CIRCLE	A(2)A	CANC	ELLED
A(2)A		CIRCUIT	A(2)A	C	EASE
A(2)A		CIRCUITOUS	A(2)A	C	ENTER
A(2)A		CIRCULAR	A(2)A(1)A	C	ENTERED
A(2)A		CIRCULATE	A(2)A	C	ENTERING
A(2)A		CIRCULATION	A(2)A	CHALL	ENGE
A(2)A(6)A		CIRCUMSTANCES	A(2)A	CH	EESE
A(2)A		CIRCUMSTANTIAL	A(2)A	CIGAR	ETTE
A(2)A		CONCEAL	A(2)A	COINCID	ENCE
A(2)A		CONCEALMENT	A(2)A	COMM	ENCE
A(2)A		CONCENTRATE	A(2)A(1)A	COMM	ENCEMENT
A(2)A		CONCENTRATING	A(2)A	COMM	ERCE
A(2)A		CONCENTRATION	A(2)A	COMP	ELLED
A(2)A		CONCERNING	A(2)A	COMPR	ESSED
A(2)A		CONCESSION	A(2)A	COND	EMNED
A(2)A		CONCILIATION	A(2)A	COND	ENSED

Table D-7—*Continued*

A(2)A	CONFER	ENCE	A(2)A		ENTER
A(2)A	CONF	ERRED	A(2)A		ENTERING
A(2)A	CONFID	ENCE	A(2)A(5)A		ENTERPRISE
A(2)A	CONVAL	ESCENT	A(2)A		ENTERPRISING
A(2)A	CONV	ENIENT	A(2)A(6)A		ENTERTAINMENT
A(2)A	CORR	ECTED	A(2)A		ENVELOP
A(2)A	CORRESPOND	ENCE	A(2)A(3)A		ENVELOPE
A(2)A	DEC	EMBER	A(2)A		ETHER
A(2)A	DECIPH	ERMENT	A(2)A		EXCEPT
A(2)A	DECR	EASE	A(2)A		EXCESS
A(2)A(2)A	D	ECREASE	A(2)A(4)A		EXCESSIVE
A(2)A	DECR	EASED	A(2)A		EXPECT
A(2)A(2)A	D	ECREASED	A(2)A(3)A		EXPEDITE
A(2)AA	D	ECREE	A(2)A		EXPEDITING
A(2)A	DEF	EATED	A(2)A		EXPEDITION
A(2)A	DEF	ENDED	A(2)A	EXP	ELLED
A(2)A	DEF	ENDER	A(2)A(2)A		EXPELLED
A(2)A	DEF	ENSE	A(2)A		EXPEND
A(2)A	DEF	ENSES	A(2)A	EXP	ENDED
A(2)A	DEF	ERRED	A(2)A(2)A		EXPENDED
A(2)AA	D	EGREE	A(2)A	EXP	ENSES
A(2)A	DEP	ENDENT	A(2)A(2)A		EXPENSES
A(2)A	D	EPRESSION	A(2)A(4)A		EXPENSIVE
A(2)A	DES	ERTED	A(2)A	EXPERI	ENCE
A(2)A	DES	ERTER	A(2)A(2)A	EXP	ERIENCE
A(2)A	DIFFER	ENCE	A(2)A(2)A(2)A		EXPERIENCE
A(2)A	DISAPP	EARED	A(2)A(3)A		EXPERIMENT
A(2)A	DIS	EASE	A(2)A		EXTEND
A(2)A	DISINF	ECTED	A(2)A	EXT	ENDED
A(2)A	DISP	ERSE	A(2)A(2)A		EXTENDED
A(2)A	DISP	ERSED	A(2)A		EXTENDING
A(2)A	DISTR	ESSED	A(2)A		EXTENSION
A(2)A		EAGER	A(2)A(4)A		EXTENSIVE
A(2)A		ECHELON	A(2)A		EXTENT
A(2)A(3)A		ECHELONED	A(2)A		EXTERIOR
A(2)A(4)A		ECHELONMENT	A(2)A(6)A		EXTERMINATE
A(2)A		EDGE	A(2)A		EXTERMINATION
A(2)A		EFFECT	A(2)A	FI	ERCE
A(2)A	EFF	ECTED	A(2)A	GR	EASE
A(2)A(2)A		EFFECTED	A(2)A	HAV	EBEEN
A(2)A(4)A		EFFECTIVE	A(2)A	H	ELPER
A(2)A(1)A	ELS	EWHERE	A(2)A	IMPR	ESSED
A(2)A(2)A(1)A		ELSEWHERE	A(2)A	INCID	ENCE
A(2)A	EM	ERGENCY	A(2)A	INCOMPET	ENCE
A(2)A	ENCIPH	ERMENT	A(2)A	INCR	EASED
A(2)A	EN	EMIES	A(2)A	INDEP	ENDENT
A(2)A	ENT	ENTE	A(2)A	INF	ECTED
A(2)A(2)A		ENTENTE	A(2)A	INFLU	ENCE

Table D-7—*Continued*

A(2)A	INTELLIG	ENCE
A(2)A	INT	ERCEPT
A(2)A	INTERC	EPTED
A(2)A(2)A	INT	ERCEPTED
A(2)A(1)A	INT	ERFERE
A(2)A	INTERFER	ENCE
A(2)A(1)A(2)A	INT	ERFERENCE
A(2)A	INT	ERFERING
A(2)A(4)A	INT	ERMEDIATE
A(2)A	INT	ERMENT
A(2)A(1)A	INT	ERVENE
A(2)A	INT	ERVENING
A(2)A	INT	ERVENTION
A(2)A	INV	ENTED
A(2)A	K	EEPER
A(2)A	L	EADER
A(2)A	L	EAVE
A(2)A	L	ETTER
A(2)A(1)A	L	ETTERED
A(2)A	LIC	ENSE
A(2)A	LI	EUTENANT
A(2)A	MAN	EUVER
A(2)A	MAT	ERIEL
A(2)A	M	EAGER
A(2)A	M	EMBER
A(2)A	MESS	ENGER
A(2)A(2)A	M	ESSENGER
A(2)A	N	EARER
A(2)A	N	EAREST
A(2)A	NEGLIG	ENCE
A(2)A	NIN	ETEEN
A(2)A	NIN	ETEENTH
A(2)A	NORTHW	ESTERN
A(2)A	NOV	EMBER
A(2)A	OBS	ERVE
A(2)A	OBS	ERVER
A(2)A	OFF	ENDED
A(2)A	OFF	ENSE
A(2)A	OVERWH	ELMED
A(2)A	PASS	ENGER
A(2)A	PRECED	ENCE
A(2)A	PREFER	ENCE
A(2)A	PREF	ERRED
A(2)A	PREPAR	EDNESS
A(2)A	PRES	ERVE
A(2)A	PR	ESSED
A(2)A	PROC	EEDED
A(2)A	PROT	ECTED
A(2)A	PROT	ESTED
A(2)A	REC	EIVE
A(2)A	REC	EIVER
A(2)A	RECOMM	ENDED
A(2)A	R	ECREATION
A(2)A	R	ECREATIONAL
A(2)A	REFER	ENCE
A(2)A	REJ	ECTED
A(2)A	REL	EASE
A(2)A	R	ELIEF
A(2)A(1)A	R	ELIEVE
A(2)A	REM	EDIES
A(2)A	REM	EMBER
A(2)A	REP	EATED
A(2)A	REP	EATER
A(2)A	REP	ELLED
A(2)A(1)A	R	EPRESENT
A(2)A(1)A	R	EPRESENTATION
A(2)A(1)A(6)A	R	EPRESENTATIVE
A(2)A	R	EQUEST
A(2)A	REQU	ESTED
A(2)A(2)A	R	EQUESTED
A(2)A	RES	ERVE
A(2)A	RES	ERVES
A(2)A	R	ESPECT
A(2)A	R	ESPECTFULLY
A(2)A	R	ESPECTS
A(2)A	R	ETREAT
A(2)A	REV	ENUE
A(2)A	REV	ERSE
A(2)A	R	EVIEW
A(2)A(1)A	R	EVIEWED
A(2)A	R	EVIEWING
A(2)A(1)A	S	EALEVEL
A(2)A	S	EAMEN
A(2)A	S	ECRECY
A(2)A	S	ECRETARY
A(2)A	S	EIZE
A(2)A	SEL	ECTED
A(2)A	SENT	ENCE
A(2)A(2)A	S	ENTENCE
A(2)A	SEPT	EMBER
A(2)A(2)A	S	EPTEMBER
A(2)A	S	ERGEANT
A(2)AA	SEV	ENTEEN
A(2)AA	SEV	ENTEENTH
A(2)A	SH	ELLED
A(2)A	SOUTHW	ESTERN

Table D-7—*Continued*

A(2)A	SUBSIST	ENCE	A(2)A	BEG	INNING
A(2)A	SUCC	EEDED	A(2)A	B	INDING
A(2)A	SURR	ENDER	A(2)A	BU	ILDING
A(2)A(1)A	SURR	ENDERED	A(2)A	CHARACTER	ISTIC
A(2)A	SUSP	ECTED	A(2)A	CO	INCIDENCE
A(2)A	SUSP	ENDED	A(2)A	COMM	ISSION
A(2)A	SUSP	ENSE	A(2)A	COMM	ISSIONER
A(2)A(5)A	T	EMPERATURE	A(2)A	CONSCR	IPTION
A(2)A(1)A	THR	EATENED	A(2)A	COUNCIL	IATION
A(2)A	TRANSF	ERRED	A(2)A	DESCR	IPTION
A(2)A	TRANSV	ERSE	A(2)A	DESCR	IPTIVE
A(2)A	TRAV	ERSE	A(2)A(1)A	D	IETITIAN
A(2)A	TW	ELVE	A(2)A	D	IFFICULT
A(2)A	UNEXP	ENDED	A(2)A(4)A	D	IFFICULTIES
A(2)A(2)A	UN	EXPENDED	A(2)A	DISC	IPLINE
A(2)A	V	ESSEL	A(2)A(2)A	D	ISCIPLINE
A(2)A	V	ESSELS	A(2)A	D	ISMISS
A(2)A	W	EDNESDAY	A(2)A	D	ISMISSAL
A(2)A	W	ESTERLY	A(2)A	D	ISTILL
A(2)A	W	ESTERN	A(2)A(3)A	D	ISTINCTION
A(2)A	WH	ETHER	A(2)A(3)A	D	ISTINGUISH
A(2)A	WITN	ESSES	A(2)A(3)A	D	ISTINGUISHED
A(2)A	WR	ECKED	A(2)A	DISTINGU	ISHING
A(2)A	Y	ESTERDAY	A(2)A(3)A(2)A	D	ISTINGUISHING
A(2)A	BA	GGAGE	A(2)A	DR	IFTING
A(2)A	DAMA	GING	A(2)A	ENL	ISTING
A(2)A	ENGA	GING	A(2)A	F	ILLING
A(2)A	FOR	GING	A(2)A	F	INDING
A(2)A		GAUGE	A(2)A	F	ISHING
A(2)A		GEOGRAPHIC	A(2)A	F	ITTING
A(2)A		GEOGRAPHICAL	A(2)A(1)A		IGNITION
A(2)A	LAN	GUAGE	A(2)A		ILLITERATE
A(2)A	NE	GLIGENCE	A(2)A(4)A		IMMIGRATION
A(2)A	NE	GLIGENT	A(2)A		INCIDENCE
A(2)A	ZI	GZAG	A(2)A		INCIDENT
A(2)A		HIGH	A(2)A		INDIA
A(2)A		HIGHER	A(2)A		INDICATE
A(2)A		HIGHEST	A(2)A		INDICATED
A(2)A	T	HATHAVE	A(2)A(3)A		INDICATING
A(2)A	W	HETHER	A(2)A(3)A		INDICATION
A(2)A	W	HICH	A(2)A		INDIRECT
A(2)A	ADM	ISSION	A(2)A(1)A		INDIVIDUAL
A(2)A	A	IRFIELD	A(2)A	INFL	ICTING
A(2)A	AS	IATIC	A(2)A	INS	IGNIA
A(2)A	ASSOC	IATION	A(2)A(2)A		INSIGNIA
A(2)A	AV	IATION	A(2)A	INTERD	ICTION
A(2)A	BALL	ISTIC	A(2)A(3)A		INVITATION
A(2)A	BALL	ISTICS	A(2)A(3)A		IRRIGATION

Table D-7—*Continued*

A(2)A	K	ILLING
A(2)A(1)A	L	IABILITY
A(2)A	L	IFTING
A(2)A	L	IQUID
A(2)A	LOG	ISTICS
A(2)A	M	IDNIGHT
A(2)A	M	ILLIMETER
A(2)A	M	ISFIRE
A(2)A	M	ISFIRES
A(2)A	M	ISSILE
A(2)A	M	ISSING
A(2)A	M	ISSION
A(2)A	M	ISSIONS
A(2)A	PATR	IOTIC
A(2)A	PERM	ISSION
A(2)A	PHIL	IPPINES
A(2)A	PR	INCIPAL
A(2)A	PR	INCIPLE
A(2)A	PR	INTING
A(2)A	PR	IORITY
A(2)A	RAD	IATION
A(2)A	REF	ILLING
A(2)A	RESTR	ICTION
A(2)A	RETAL	IATION
A(2)A	REV	IEWING
A(2)A	SH	IPPING
A(2)A(1)A	S	IGNIFICANCE
A(2)A(1)A	S	IGNIFICANT
A(2)A	S	IGNIFY
A(2)A	S	INKING
A(2)A	SK	IRMISH
A(2)A	STAT	ISTICS
A(2)A	SUBM	ISSION
A(2)A	SUPER	IORITY
A(2)A	SW	IMMING
A(2)A	TRANSM	ISSION
A(2)A	VAR	IATION
A(2)A	V	ICTIM
A(2)A	W	ITHIN
A(2)A	AVAI	LABLE
A(2)A	FUE	LOIL
A(2)A	PARA	LLEL
A(2)A	COM	MITMENT
A(2)A		MAIM
A(2)A	MEDIU	MBOMBER
A(2)A	ABA	NDON
A(2)A	ADVA	NCING
A(2)A	AFTER	NOON
A(2)A	AN	NOUNCE
A(2)A(4)A	AN	NOUNCEMENT
A(2)AA	A	NTENNA
A(2)A	ASSIG	NMENT
A(2)A	ASSIG	NMENTS
A(2)A	ATTAI	NMENT
A(2)A	BEGI	NNING
A(2)A	BI	NDING
A(2)A	COMMA	NDANT
A(2)A	COMMA	NDING
A(2)A	CO	NCENTRATE
A(2)A(5)A	CO	NCENTRATING
A(2)A(6)A	CO	NCENTRATION
A(2)A	CO	NDENSED
A(2)A	CO	NFINE
A(2)A(3)A	CO	NFINEMENT
A(2)A(1)A	CO	NTINENTAL
A(2)A	CONTI	NGENT
A(2)A(2)A	CO	NTINGENT
A(2)A	CO	NTINUAL
A(2)A(5)A	CO	NTINUATION
A(2)A	CO	NTINUE
A(2)A	CO	NTINUOUS
A(2)A	CONVE	NIENT
A(2)A(2)A	CO	NVENIENT
A(2)A	CORRESPO	NDENCE
A(2)A	CORRESPO	NDING
A(2)A	DEPE	NDENT
A(2)A	DISCONTI	NUANCE
A(2)A(2)A	DISCO	NTINUANCE
A(2)A	DISCO	NTINUE
A(2)A	ECHELO	NMENT
A(2)A	E	NGINE
A(2)A	E	NGINEER
A(2)A(4)A	E	NGINEERING
A(2)A(5)A	E	NTANGLEMENT
A(2)A	E	NTENTE
A(2)A	ENTERTAI	NMENT
A(2)A	EXTE	NDING
A(2)A	FI	NDING
A(2)A	FLA	NKING
A(2)A	FORE	NOON
A(2)A	GOVER	NMENT
A(2)A	I	NCENDIARY
A(2)A	I	NCENTIVE
A(2)A	INDEPE	NDENT
A(2)A	I	NFANTRY
A(2)A	I	NLAND

Table D-7—*Continued*

A(2)A	INSTA	NTANEOUS
A(2)A	I	NTEND
A(2)A	I	NTENSIVE
A(2)A	I	NTENT
A(2)A(3)A	I	NTENTION
A(2)A	INTER	NMENT
A(2)A	I	NVENT
A(2)A	I	NVENTED
A(2)A(3)A	I	NVENTION
A(2)A	LA	NDING
A(2)A(1)A	MAI	NTENANCE
A(2)A	MA	NNING
A(2)A		NOON
A(2)A	OPI	NION
A(2)A	PAI	NTING
A(2)A	PLA	NNING
A(2)A	PO	NTON
A(2)A	PRI	NTING
A(2)A	QUARA	NTINE
A(2)A	RU	NNING
A(2)A	SE	NTENCE
A(2)A	SE	NTINEL
A(2)A	SI	NKING
A(2)A	SU	NKEN
A(2)A	U	NION
A(2)A	UNK	NOWN
A(2)A	U	NTENABLE
A(2)A(4)A	ACC	OMMODATION
A(2)A	B	OTTOM
A(2)A	B	OYCOTT
A(2)A	C	OMMON
A(2)A	C	OMPOSED
A(2)A(4)A	C	OMPOSITION
A(2)A(5)A	C	ONFORMATION
A(2)A	C	ONVOY
A(2)A	C	ORPORAL
A(2)A(4)A	C	ORPORATION
A(2)A	CUST	OMHOUSE
A(2)A	D	OCTOR
A(2)A	EN	ORMOUS
A(2)A	EXPL	OSION
A(2)A	EXPL	OSIONS
A(2)A	F	OGHORN
A(2)A	F	OLLOW
A(2)A	FO	OTHOLD
A(2)A	G	ONIOMETER
A(2)A	GYR	OSCOPIC
A(2)A	L	OOKOUT
A(2)A	N	ONCOMBATANT
A(2)A		OBSOLETE
A(2)A		OCTOBER
A(2)A		OPPOSE
A(2)A		OPPOSITE
A(2)A(4)A		OPPOSITION
A(2)A	P	OISON
A(2)AA	P	ONTOON
A(2)A	P	OSTOFFICE
A(2)A	PROM	OTION
A(2)A	REC	ONNOITER
A(2)A	REC	ONNOITERING
A(2)A	R	OMEO
A(2)A	SCHO	OLHOUSE
A(2)A	TOM	ORROW
A(2)A	VICT	ORIOUS
A(2)A	AP	PROPRIATE
A(2)A	IM	PROPER
A(2)A		PREPARATION
A(2)A		PREPARE
A(2)A		PREPAREDNESS
A(2)A		PREPARING
A(2)A		PROPER
A(2)A		PROPORTION
A(2)A		PROPOSALS
A(2)A		PROPOSE
A(2)A		PUMP
A(2)A		PURPOSE
A(2)A		PURPOSES
A(2)A	AI	RBORNE
A(2)A	APP	ROPRIATE
A(2)A	A	RMOR
A(2)A(4)A	A	RMOREDCAR
A(2)A	A	RMORY
A(2)A	CAR	RIER
A(2)A	CO	RPORAL
A(2)A	CO	RPORATION
A(2)A	COU	RIER
A(2)A	DEPA	RTURE
A(2)A	DESE	RTER
A(2)A	DETE	RIORATE
A(2)A	E	RROR
A(2)A	EXTE	RIOR
A(2)A(4)A	EXT	RAORDINARY
A(2)A	FEB	RUARY
A(2)A	FO	RWARD
A(2)A	HA	RBOR
A(2)A	HEADQUA	RTERS

Table D-7—*Continued*

A(2)A	HYD	ROGRAPHIC	A(2)A(4)A	AS	SESSMENTS
A(2)A	INTE	RFERE	A(2)AA(4)A	A	SSESSMENTS
A(2)A	INTE	RFERENCE	A(2)A	AS	SETS
A(2)A	INTE	RFERING	A(2)A	A	SSIST
A(2)A	INTE	RIOR	A(2)A	A	SSISTANCE
A(2)A	MI	RROR	A(2)A	A	SSISTANT
A(2)A	MO	RTAR	A(2)AA	CARELES	SNESS
A(2)A	MU	RDER	A(2)A	CEN	SORSHIP
A(2)A	OBSE	RVER	A(2)A	CHA	SSIS
A(2)A	O	RDER	A(2)A	CRUI	SERS
A(2)A	O	RDERED	A(2)AA	DI	SCUSS
A(2)A	O	RDERS	A(2)AA	DI	SCUSSED
A(2)A	PA	RAGRAPH	A(2)AA	DI	SCUSSION
A(2)A	PE	RFORMANCE	A(2)A	DI	SEASE
A(2)A	P	RAIRIE	A(2)AA	DI	SMISS
A(2)AA	P	REARRANGED	A(2)AA	DI	SMISSAL
A(2)A	P	RIOR	A(2)A	DI	SPOSITION
A(2)A	P	RIORITY	A(2)A	EMBAS	SIES
A(2)A	P	ROGRAM	A(2)A	GLA	SSES
A(2)A	P	ROGRESS	A(2)A	HEAVYLO	SSES
A(2)A	P	ROGRESSIVE	A(2)A	IS	SUES
A(2)A	QUA	RTER	A(2)A	LO	SSES
A(2)A(5)A	QUA	RTERMASTER	A(2)A	PA	SSES
A(2)A	QUA	RTERS	A(2)A	POS	SESSION
A(2)A		REAR	A(2)AA	PO	SSESSION
A(2)A(3)A		REARGUARD	A(2)A	PROPO	SALS
A(2)A	RECO	RDER	A(2)A	REPRI	SALS
A(2)A		RECREATION	A(2)A		SESSION
A(2)A		RECREATIONAL	A(2)A(1)A		SUBSISTENCE
A(2)A		RECRUIT	A(2)A		SUBSTITUTE
A(2)A		RECRUITING	A(2)A		SUBSTITUTION
A(2)A		REORGANIZATION	A(2)A		SUNSET
A(2)A		REPRESENT	A(2)AA	TRAN	SMISSION
A(2)A		REPRESENTATION	A(2)A	VES	SELS
A(2)A		REPRESENTATIVE	A(2)A	VI	SITS
A(2)A		REPRISAL	A(2)A	WITNE	SSES
A(2)A		REPRISALS	A(2)A	ADJU	TANT
A(2)A		RETREAT	A(2)A	ADMINIS	TRATION
A(2)A		RETROACTIVE	A(2)A	ADMINIS	TRATIVE
A(2)A	STA	RTER	A(2)A	ARBI	TRATION
A(2)A	SUPE	RIOR	A(2)A	ASSIS	TANT
A(2)A	SUPE	RIORITY	A(2)A	AT	TENTION
A(2)A	TE	RROR	A(2)A	CA	TASTROPHE
A(2)A	WA	RFARE	A(2)A	CIRCUMS	TANTIAL
A(2)A	ADDRE	SSES	A(2)A	COMBA	TANT
A(2)AA	A	SPOSSIBLE	A(2)A	CONCEN	TRATE
A(2)A	AS	SESSMENT	A(2)A	CONCEN	TRATING
A(2)AA	A	SSESSMENT	A(2)A	CONCEN	TRATION

Table D-7—*Continued*

A(2)A	CON	TACT
A(2)A	DEMONS	TRATE
A(2)A	DEMONS	TRATED
A(2)A	DEMONS	TRATION
A(2)A	DE	TECTOR
A(2)A	DE	TENTION
A(2)A	EN	TENTE
A(2)A(6)A	EN	TERTAINMENT
A(2)A	EX	TENT
A(2)A	FOX	TROT
A(2)A	ILLUS	TRATE
A(2)A	ILLUS	TRATION
A(2)A	IMPOR	TANT
A(2)A	INCOMPE	TENT
A(2)A	INI	TIATE
A(2)A	INS	TANT
A(2)A	INS	TANTANEOUS
A(2)A	INS	TANTLY
A(2)A	IN	TENT
A(2)A	IN	TENTION
A(2)A	NONCOMBA	TANT
A(2)A	OU	TPUT
A(2)A	PENE	TRATE
A(2)A	PENE	TRATION
A(2)A	PERSIS	TENT
A(2)A	PRO	TECT
A(2)A	PRO	TECTED
A(2)A	PRO	TECTION
A(2)A	PRO	TECTOR
A(2)A	PRO	TEST
A(2)A	PRO	TESTED
A(2)A	PRO	TESTS
A(2)A	REGIS	TRATION
A(2)A	RE	TENTION
A(2)A	SI	TUATION
A(2)A	S	TART
A(2)A	S	TARTER
A(2)A	STA	TISTICS
A(2)A	S	TRATEGIC
A(2)A	S	TRATEGICAL
A(2)A	S	TRATEGY
A(2)A		TACTICAL
A(2)A		TACTICS
A(2)A		TATTOO
A(2)A		TENT
A(2)A(1)A		TENTATIVE
A(2)A		TENTH
A(2)A		TEXT
A(2)A		THAT
A(2)A		THATHAVE
A(2)AA		THATTHE
A(2)A	TWEN	TIETH
A(2)A	WA	TERTANK
A(2)A	AGRIC	ULTURAL
A(2)A	D	UGOUT
A(2)A	O	UTGUARD
A(2)A	O	UTPUT
A(2)A	P	URSUE
A(2)A	P	URSUIT
A(2)A(6)A		UNSUCCESSFUL
A(2)A		UNSUITABLE
A(2)A	RE	VOLVE
A(2)A	RE	VOLVER
A(2)A	AN	YWAY
A(2)A		ZIGZAG
A(3)A		ACTUALLY
A(3)A		ALPHA
A(3)A		ANIMAL
A(3)A		ANNUAL
A(3)A(4)A		ANTIAIRCRAFT
A(3)A		ANYWAY
A(3)A		APPEAR
A(3)A(1)A		APPEARANCE
A(3)A		APPEARED
A(3)A		AVERAGE
A(3)A		AWKWARD
A(3)A	C	ANADA
A(3)A	C	ARRIAGE
A(3)A	CENTR	ALIZATION
A(3)A	CIRCUMST	ANTIAL
A(3)A	DIS	APPEAR
A(3)A	DIS	APPEARED
A(3)A	E	ASTWARD
A(3)A	EL	ABORATE
A(3)A	ESTIM	ATEDAT
A(3)A	EX	AMINATION
A(3)A	GENER	ALALARM
A(3)A	GENER	ALSTAFF
A(3)A	HE	ADQUARTERS
A(3)A	L	ABORATORY
A(3)A	L	ANGUAGE
A(3)A	M	AINTAIN
A(3)A	M	AINTAINED
A(3)A	M	ANUFACTURE
A(3)A	M	ARSHAL
A(3)A	M	ARTIAL

Table D-7—*Continued*

A(3)A	N	ATURAL
A(3)A	NATUR	ALIZATION
A(3)A(3)A	N	ATURALIZATION
A(3)A	N	ATURALIZE
A(3)A	N	AVIGATION
A(3)A	ORG	ANIZATION
A(3)A	P	ANAMA
A(3)A	R	AILWAY
A(3)A	RE	ARGUARD
A(3)A	RECONN	AISSANCE
A(3)A	REORG	ANIZATION
A(3)A	S	ABOTAGE
A(3)A	S	ANITARY
A(3)A	S	ANITATION
A(3)A	SPE	ARHEAD
A(3)A	TR	ANSPACIFIC
A(3)A		CAPACITY
A(3)A		CHURCH
A(3)A(4)A		COINCIDENCE
A(3)A		CONSCRIPTION
A(3)A		COUNCIL
A(3)A	DEFI	CIENCY
A(3)A	EFFI	CIENCY
A(3)A	ELE	CTRICITY
A(3)A	GYROS	COPIC
A(3)A	INEFFI	CIENCY
A(3)A	PA	CIFIC
A(3)A	SPE	CIFIC
A(3)A	SPE	CIFICATION
A(3)A	TE	CHNICAL
A(3)A	TRANSPA	CIFIC
A(3)A		DECIDE
A(3)A(1)A		DECIDED
A(3)A		DECODE
A(3)A		DIVIDE
A(3)A		DIVIDING
A(3)A	HIN	DERED
A(3)A	IN	DIVIDUAL
A(3)A	MAN	DATED
A(3)A	OR	DERED
A(3)A	RE	DUCED
A(3)A	SURREN	DERED
A(3)A	WE	DNESDAY
A(3)A	WIN	DWARD
A(3)A	ASS	EMBLE
A(3)A	ASS	ESSMENT
A(3)A	ASS	ESSMENTS
A(3)A	ATT	EMPTED
A(3)A	AV	ERAGE
A(3)A(1)A	BE	ENNEEDED
A(3)AA(1)A	B	EENNEEDED
A(3)A	B	EETLE
A(3)A	B	EFORE
A(3)A	B	ETWEEN
A(3)A	CAREL	ESSNESS
A(3)A	C	EMETERY
A(3)A	COMPL	ETENESS
A(3)A	CONC	EALMENT
A(3)A	COOP	ERATE
A(3)A	CORR	ECTNESS
A(3)A	D	ECIDE
A(3)A	D	ECIDED
A(3)A	D	ECODE
A(3)A	D	ECREE
A(3)A	D	EGREE
A(3)A	D	ELAYED
A(3)A	D	ELIVER
A(3)A	DEV	ELOPE
A(3)A	DEV	ELOPED
A(3)A	D	EVICE
A(3)A	D	EVISE
A(3)A		EASTERLY
A(3)A		EASTERN
A(3)A	ECH	ELONED
A(3)A		EITHER
A(3)A		ELEMENT
A(3)A		ELEMENTARY
A(3)A	EL	EVATE
A(3)A		ELEVEN
A(3)A		ENTRENCH
A(3)A	ENTR	ENCHED
A(3)A(3)A		ENTRENCHED
A(3)A	ENV	ELOPE
A(3)A		ERASE
A(3)A		ERASER
A(3)A	EXP	EDITE
A(3)A	EXP	ERIMENT
A(3)A		EXPRESS
A(3)A(1)A		EXTREME
A(3)A	FUS	ELAGE
A(3)A	GOV	ERNMENT
A(3)A	GR	ENADE
A(3)A	H	EAVIER
A(3)A	ILLIT	ERATE
A(3)A	IMP	EDIMENTA
A(3)A	INS	ECURE

Table D-7—*Continued*

A(3)A	INT	ERNMENT	A(3)A	T	HATTHE
A(3)A	INT	ERPRETATION	A(3)A	T	HOUGH
A(3)A(1)A	INT	ERPRETER	A(3)A	ACT	IVITIES
A(3)A	INT	ERVIEW	A(3)A	ANTIC	IPATION
A(3)A	L	EAGUE	A(3)A	APPL	ICATION
A(3)A	OP	ERATE	A(3)A	ART	IFICIAL
A(3)A(2)A	OV	ERWHELMED	A(3)A	AUD	IBILITY
A(3)A(1)A	PAR	ENTHESES	A(3)A	BR	IGADIER
A(3)A	PAR	ENTHESIS	A(3)A	CENTRAL	IZATION
A(3)A	PR	ECEDE	A(3)A	C	IRCUIT
A(3)A(2)A	PR	ECEDENCE	A(3)A	C	IRCUITOUS
A(3)A(2)A	PR	EFERENCE	A(3)A	C	ITATION
A(3)A	PR	EPARE	A(3)A	CLASSIF	ICATION
A(3)A(2)A	PR	EPAREDNESS	A(3)A	COMMUN	ICATION
A(3)A	PR	ESIDENT	A(3)A	CONST	ITUTING
A(3)A	PR	ESIDENTIAL	A(3)A	CONST	ITUTION
A(3)A	PROC	EDURE	A(3)A	COORD	INATION
A(3)A	R	EACHED	A(3)A	CR	ITICISE
A(3)A	R	ECOVER	A(3)A	CR	ITICISM
A(3)A	R	EDUCE	A(3)A	DED	ICATION
A(3)A	R	EDUCED	A(3)A	DEF	INITION
A(3)A(2)A	R	EFERENCE	A(3)A	DEMOBIL	IZATION
A(3)A	R	EFUGE	A(3)A	DETERM	INATION
A(3)AA	R	EFUGEE	A(3)A	D	IMINISH
A(3)A	R	EFUSE	A(3)A	D	IRIGIBLE
A(3)A	R	EGIMENT	A(3)A	DISSEM	INATION
A(3)A	R	EGIMENTAL	A(3)A	DIST	INCTION
A(3)A	R	ESCUE	A(3)A	DIST	INGUISH
A(3)A	R	ESUME	A(3)A	DIST	INGUISHED
A(3)A	R	ETIRE	A(3)A(2)A	DIST	INGUISHING
A(3)A	SCH	EDULE	A(3)A	D	ISTRIBUTE
A(3)A	S	ECURE	A(3)A	DISTR	IBUTING
A(3)A	S	ETTLE	A(3)A(3)A	D	ISTRIBUTING
A(3)A	SEV	ENTEEN	A(3)A	DISTR	IBUTION
A(3)A	SEV	ENTEENTH	A(3)A(3)A	D	ISTRIBUTION
A(3)A	S	EVERE	A(3)A	D	ISTRICT
A(3)AA	SMOK	ESCREEN	A(3)A	D	ISTRICTS
A(3)A	SP	EARHEAD	A(3)A	D	IVIDING
A(3)A	THER	EFORE	A(3)A	D	IVISION
A(3)A	TW	ENTIETH	A(3)A	D	IVISIONS
A(3)A	W	EATHER	A(3)A	DOM	INATION
A(3)A		GARAGE	A(3)A	ENC	IRCLING
A(3)A		GOING	A(3)A	EST	IMATION
A(3)A	C	HURCH	A(3)A	EXAM	INATION
A(3)A	FLAS	HLIGHT	A(3)A	EXH	IBITION
A(3)A	P	HOSPHOROUS	A(3)A	EXTERM	INATION
A(3)A	SC	HOOLHOUSE	A(3)A	EXT	INGUISH
A(3)A	SEARC	HLIGHTS	A(3)A	FAC	ILITIES

Table D-7—*Continued*

A(3)A	F	IGHTING
A(3)A	HOST	ILITIES
A(3)A	IDENTIF	ICATION
A(3)A	ILLUM	INATING
A(3)A	ILLUM	INATION
A(3)A(1)A		INCLINING
A(3)A	IND	ICATING
A(3)A	IND	ICATION
A(3)A		INFLICT
A(3)A(2)A		INFLICTING
A(3)A		INITIATE
A(3)A		INQUIRE
A(3)A		INQUIRY
A(3)A	INSP	IRATION
A(3)A(3)A		INSPIRATION
A(3)A		INSPIRE
A(3)A	INST	ITUTION
A(3)A(3)A		INSTITUTION
A(3)A	INVEST	IGATION
A(3)A	INVEST	IGATIONS
A(3)A	INV	ITATION
A(3)A	IRR	IGATION
A(3)A		ISSUING
A(3)A	L	IMITING
A(3)A	LIM	ITATION
A(3)A	MA	INTAIN
A(3)A	MA	INTAINED
A(3)A	M	ILITIA
A(3)A	MOBIL	IZATION
A(3)A	NATURAL	IZATION
A(3)A	NAV	IGATION
A(3)A	ORGAN	IZATION
A(3)A	PRELIM	INARIES
A(3)A	QUALIF	ICATION
A(3)A	RECONNO	ITERING
A(3)A	REORGAN	IZATION
A(3)A	REQU	ISITION
A(3)A	RESPONS	IBILITY
A(3)A	SAN	ITATION
A(3)A	SEM	IRIGID
A(3)A	S	IGHTING
A(3)A	SIM	ILARITY
A(3)A	SPECIF	ICATION
A(3)A	SUBST	ITUTION
A(3)A(1)A	SU	ITABILITY
A(3)A	VERIF	ICATION
A(3)A	VETER	INARIAN
A(3)A	V	ICINITY
A(3)A	VIS	IBILITY
A(3)A(1)A	V	ISIBILITY
A(3)A	CO	LONEL
A(3)A	COMP	LETELY
A(3)A	F	LASHLIGHT
A(3)A	IL	LEGAL
A(3)A		LEVEL
A(3)A		LITTLE
A(3)A		LOCAL
A(3)A	SEA	LEVEL
A(3)A	A	MUSEMENT
A(3)A	CO	MMITMENT
A(3)A(1)A		MAXIMUM
A(3)A(1)A		MINIMUM
A(3)A		MOVEMENT
A(3)A	ALTER	NATING
A(3)A(4)A	A	NNOUNCEMENT
A(3)A	A	NTENNA
A(3)A	APPOI	NTMENT
A(3)A	ASCE	NSION
A(3)A	ATTE	NTION
A(3)A(1)A	CO	NCERNING
A(3)A	CO	NDEMN
A(3)A	CO	NDEMNED
A(3)A	CONFI	NEMENT
A(3)A	CO	NTAIN
A(3)A	DETE	NTION
A(3)A	DIME	NSION
A(3)A	E	NCOUNTERED
A(3)A	E	NTRENCH
A(3)A	E	NTRENCHED
A(3)A	EXPA	NSION
A(3)A	EXTE	NSION
A(3)A	ILLUMI	NATING
A(3)A	I	NDEMNITY
A(3)A	I	NSIGNIA
A(3)A	I	NSTANT
A(3)A(2)A	I	NSTANTANEOUS
A(3)A	I	NSTANTLY
A(3)A	INTE	NTION
A(3)A	I	NTERNAL
A(3)A(4)A	I	NTERNATIONAL
A(3)A(2)A	I	NTERNMENT
A(3)A	INTERVE	NTION
A(3)A	I	NTRENCH
A(3)A	INVE	NTION
A(3)A	LAU	NCHING
A(3)A	MACHI	NEGUN

Table D-7—*Continued*

A(3)A	MAI	NTAIN	A(3)A	C	ROSSROADS
A(3)A	MAI	NTAINED	A(3)A	DEST	ROYER
A(3)A	MOU	NTAIN	A(3)A	DEST	ROYERS
A(3)A		NOTING	A(3)A	E	RASER
A(3)A	O	NEHUNDRED	A(3)A	FA	RTHER
A(3)A	PO	NTOON	A(3)A	FU	RTHER
A(3)A	REAPPOI	NTMENT	A(3)A	IMP	ROPER
A(3)A	RETE	NTION	A(3)A	INTERP	RETER
A(3)A	SEVE	NTEEN	A(3)A	LABO	RATORY
A(3)A	SEVE	NTEENTH	A(3)A	NO	RTHERLY
A(3)A	SUSPE	NSION	A(3)A	NO	RTHERN
A(3)A	U	NIDENTIFIED	A(3)A	OPE	RATOR
A(3)A	AIRC	ONTROL	A(3)A	P	REARRANGED
A(3)A	AN	ONYMOUS	A(3)A	P	REFER
A(3)A	CHR	ONOLOGICAL	A(3)A	P	REFERENCE
A(3)AA	C	ODEBOOK	A(3)AA	P	REFERRED
A(3)A	C	ONTROL	A(3)A	P	REPARATION
A(3)A	C	ONTROVERSY	A(3)A	P	REPARE
A(3)A	CR	OSSROADS	A(3)A	P	REPAREDNESS
A(3)A	FIREC	ONTROL	A(3)A	P	REPARING
A(3)A	F	OOTHOLD	A(3)A	P	RESCRIBED
A(3)AA	F	ORENOON	A(3)A	P	RESERVATION
A(3)A	F	OXTROT	A(3)A	P	RESERVE
A(3)A	H	ORIZON	A(3)A	P	RIMARY
A(3)A	LAB	ORATORY	A(3)A	P	ROPER
A(3)A	L	OCOMOTIVE	A(3)A	P	ROPORTION
A(3)A	METE	OROLOGICAL	A(3)A		RAILROAD
A(3)A	M	ONOPOLY	A(3)A	REA	RGUARD
A(3)A		OUTBOARD	A(3)A		RECORD
A(3)A		OUTPOST	A(3)A(2)A		RECORDER
A(3)A		OUTPOSTS	A(3)A		REDCROSS
A(3)A	PH	OSPHORUS	A(3)A		REFER
A(3)A	P	ONTOON	A(3)A		REFERENCE
A(3)A	P	OSTPONE	A(3)A		REGARDING
A(3)A	PROP	ORTION	A(3)A		REPORT
A(3)A	PR	OTOCOL	A(3)A		REPORTED
A(3)A	A	PPROPRIATE	A(3)A		RESERVATION
A(3)A		PASSPORT	A(3)A		RESERVE
A(3)A		PHOSPHORUS	A(3)A		RESERVES
A(3)A		POSTPONE	A(3)A		RESTRAINT
A(3)A		PROMPT	A(3)A		RESTRICTED
A(3)A	TROO	PSHIP	A(3)A		RESTRICTION
A(3)A	TROO	PSHIPS	A(3)A		RETIRE
A(3)A	A	RBITRATION	A(3)A		RETIRING
A(3)A	B	RIBERY	A(3)A		RETURN
A(3)A	CA	RRIER	A(3)A		RETURNED
A(3)A	CONT	ROVERSY	A(3)A		RETURNING
A(3)A	COR	RIDOR	A(3)A		REVERSE

Table D-7—*Continued*

A(3)A		RIGOROUS	A(3)A	SU	SPENSION
A(3)A		RIVER	A(3)A	TRAN	SMISSION
A(3)A		ROGER	A(3)A	TRAN	SVERSE
A(3)A	SEC	RETARY	A(3)A	TROOP	SHIPS
A(3)A	TEMPE	RATURE	A(3)AA	U	SELESS
A(3)A	TER	RITORY	A(3)A	VE	SSELS
A(3)A	THE	REFORE	A(3)A	WAR	SHIPS
A(3)A	T	RAVERSE	A(3)A	AC	TIVITIES
A(3)A	VETE	RINARIAN	A(3)A	AC	TIVITY
A(3)A	A	SCENSION	A(3)A	ALLO	TMENT
A(3)A	A	SPOSSIBLE	A(3)A	AN	TEDATING
A(3)A	A	SSESSMENT	A(3)A	APPOIN	TMENT
A(3)A(4)A	A	SSESSMENTS	A(3)A	A	TLANTIC
A(3)A	A	SSETS	A(3)A	AT	TEMPT
A(3)A	BALLI	STICS	A(3)A	AT	TEMPTED
A(3)A	BATTLE	SHIPS	A(3)A	A	TTENTION
A(3)AA	BU	SINESS	A(3)A	AU	TOMATIC
A(3)A	CARELES	SNESS	A(3)A	COMMI	TMENT
A(3)AA	CARELE	SSNESS	A(3)A	COMPAR	TMENT
A(3)A	COLLI	SIONS	A(3)A	CONS	TITUTE
A(3)A	DI	SCUSS	A(3)A	CONS	TITUTION
A(3)A	DI	SCUSSED	A(3)A	CONS	TRUCTION
A(3)A	DI	SCUSSION	A(3)A	CON	TRACT
A(3)A	DI	SMISS	A(3)AA	COUN	TERATTACK
A(3)A	DI	SMISSAL	A(3)A	DEPAR	TMENT
A(3)A	DI	SPERSE	A(3)A	DEPAR	TMENTAL
A(3)A	DI	SPERSED	A(3)A	DES	TITUTE
A(3)A	DI	SPERSION	A(3)A	DES	TRUCTION
A(3)AA	DI	STRESS	A(3)A	DE	TONATE
A(3)AA	DI	STRESSED	A(3)A	DE	TONATED
A(3)A	DIVI	SIONS	A(3)A	DE	TONATION
A(3)A	EMBA	SSIES	A(3)A	DIS	TINCTION
A(3)A	EXPLO	SIONS	A(3)A	DIS	TRICT
A(3)A	I	SSUES	A(3)A	DIS	TRICTS
A(3)A	LOGI	STICS	A(3)A	EIGH	TEENTH
A(3)A	MARK	SMANSHIP	A(3)A	ENLIS	TMENT
A(3)A	MES	SAGES	A(3)A	ES	TIMATE
A(3)A	MIS	SIONS	A(3)A	ESTIMA	TEDAT
A(3)A	PO	SSESSION	A(3)A(3)A	ES	TIMATEDAT
A(3)A	PROVI	SIONS	A(3)A	ES	TIMATES
A(3)A	RE	SPONSIBLE	A(3)A	ES	TIMATION
A(3)A	RE	SPONSIBILITY	A(3)A	EX	TRACT
A(3)A		SATISFACTORY	A(3)A	FA	TALITY
A(3)A		SATISFY	A(3)A	FIF	TEENTH
A(3)A		SHIPS	A(3)A	FOUR	TEENTH
A(3)A	STATI	STICS	A(3)A	HOS	TILITIES
A(3)AA		STRESS	A(3)A	HOS	TILITY
A(3)A	SU	SPENSE	A(3)A	ILLI	TERATE

Table D-7—*Continued*

A(3)A	INS	TITUTION	A(4)A		ADJUTANT
A(3)A	INS	TRUCT	A(4)A		AERONAUTICS
A(3)A	INS	TRUCTION	A(4)A		AIRCRAFT
A(3)A	INS	TRUCTIONS	A(4)A		AIRPLANE
A(3)A	INS	TRUCTOR	A(4)A		ALASKA
A(3)A	INVES	TIGATE	A(4)A		ALLOCATION
A(3)A	INVES	TIGATION	A(4)A		ALLOWANCE
A(3)A	INVES	TIGATIONS	A(4)A		ALMANAC
A(3)A	NINE	TEENTH	A(4)A		AMBULANCE
A(3)A	OBS	TRUCTIONS	A(4)A	ANTI	AIRCRAFT
A(3)A	OU	TPOST	A(4)A		ANTITANK
A(3)A	OU	TPOSTS	A(4)A		APPARATUS
A(3)A	PA	TRIOTIC	A(4)A		APPROACH
A(3)A	REAPPOIN	TMENT	A(4)A		ARABIA
A(3)A	RECONS	TRUCTION	A(4)A		ARRIVAL
A(3)A	REENLIS	TMENT	A(4)A		ASSURANCE
A(3)A	RES	TRICTED	A(4)A		AUTOMATIC
A(3)A	RES	TRICTION	A(4)A		AVAILABLE
A(3)A	RE	TREAT	A(4)A	BE	ACHHEAD
A(3)A	SEVEN	TEENTH	A(4)A	C	AUSEWAY
A(3)A	SIX	TEENTH	A(4)A	CO	ASTGUARD
A(3)A	S	TREET	A(4)A	GEOGR	APHICAL
A(3)A	SUBS	TITUTE	A(4)A	IMPR	ACTICABLE
A(3)A	SUBS	TITUTION	A(4)A	IN	AUGURATION
A(3)A		TAXATION	A(4)A	INTERN	ATIONAL
A(3)A		THATTHE	A(4)A	M	ARKSMANSHIP
A(3)A		THIRTEEN	A(4)A	M	ATERIAL
A(3)A	THIR	TEENTH	A(4)A	N	ATIONAL
A(3)A(3)A		THIRTEENTH	A(4)A	N	ATIONALISM
A(3)A		THIRTY	A(4)A	N	ATIONALITY
A(3)A		TRACT	A(4)A	N	AUTICAL
A(3)A		TRACTOR	A(4)A	NAV	ALATTACK
A(3)A	TRANSA	TLANTIC	A(4)A	N	AVALBASE
A(3)A(2)A		TWENTIETH	A(4)A	N	AVALBATTLE
A(3)A		TWENTY	A(4)A	P	ARAGRAPH
A(3)A		TWENTYFIVE	A(4)A	P	ARALLAX
A(3)A(1)A	UNI	TEDSTATES	A(4)A	PR	ACTICAL
A(3)A	U	TILITY	A(4)A	R	ADIOACTIVE
A(3)A	WI	THOUT	A(4)A	R	AILHEAD
A(3)A	B	UREAU	A(4)A	R	AILROAD
A(3)A	CHA	UFFEUR	A(4)A	RECRE	ATIONAL
A(3)A	CIRC	UITOUS	A(4)A	S	ATISFACTORY
A(3)A	COMM	UNIQUE	A(4)A	S	ATURDAY
A(3)A	S	URPLUS	A(4)A	T	ACTICAL
A(3)A	S	URROUND	A(4)A	W	ATERTANK
A(3)A		UNUSUAL	A(4)A		CHARACTER
A(3)A		WESTWARD	A(4)A(7)A		CHARACTERISTIC
A(3)A		WINDWARD	A(4)A		CHEMICAL

Table D-7—*Continued*

A(4)A		CLERICAL
A(4)A	COIN	CIDENCE
A(4)A		COLLECT
A(4)A		COLLECTION
A(4)A		CONDUCT
A(4)A		CONNECTING
A(4)A		CONNECTION
A(4)A		CONTACT
A(4)A		CORRECT
A(4)A		CORRECTED
A(4)A		CORRECTION
A(4)A		CORRECTNESS
A(4)A		CRITIC
A(4)A		CRITICAL
A(4)A		CRITICISE
A(4)A		CRITICISM
A(4)A	IN	CIDENCE
A(4)A	ME	CHANIC
A(4)A	PRE	CEDENCE
A(4)A	RE	CEPTACLE
A(4)A	CON	DEMNED
A(4)A	CON	DENSED
A(4)A		DEFEND
A(4)A		DEFENDER
A(4)A(1)A		DEFENDED
A(4)A		DEMAND
A(4)A(1)A		DEMANDED
A(4)A		DEPEND
A(4)A		DEPENDABILITY
A(4)A		DEPENDABLE
A(4)A		DEPENDENT
A(4)A		DISLODGE
A(4)A		DOWNED
A(4)A	IN	DEPENDENT
A(4)A	ALT	ERNATE
A(4)A	ASS	EMBLIES
A(4)A	B	EACHHEAD
A(4)A	B	ECAUSE
A(4)A(1)A	B	EENNEEDED
A(4)A(1)A	B	ELLIGERENT
A(4)A	B	ESIEGED
A(4)A	C	ENTERED
A(4)A	COMM	ENCEMENT
A(4)A	COMP	ENSATE
A(4)A	CONF	ERENCE
A(4)A	CONSID	ERABLE
A(4)A	D	ECEMBER
A(4)A	D	ECIPHER
A(4)A(1)A	D	ECIPHERED
A(4)A(2)A	D	ECIPHERMENT
A(4)A	D	ECLARE
A(4)A	D	ECLARED
A(4)A	D	EFEATED
A(4)A	DEF	ECTIVE
A(4)A	D	EFENDED
A(4)A	D	EFENDER
A(4)A	D	EFENSE
A(4)A	D	EFENSES
A(4)A	DEF	ENSIVE
A(4)A	D	EFERRED
A(4)A	D	EFICIENCY
A(4)A	D	EFICIENT
A(4)A	D	EMANDED
A(4)A	D	EPARTED
A(4)A	D	EPENDENT
A(4)A	D	EPLOYED
A(4)A	D	EPORTED
A(4)A	D	ESERTED
A(4)A	D	ESERTER
A(4)A	D	ETACHED
A(4)A	DET	ERMINE
A(4)A	DET	ERMINED
A(4)A	DEV	ELOPMENT
A(4)A	DIFF	ERENCE
A(4)A	ECH	ELONMENT
A(4)A	EFF	ECTIVE
A(4)AA		EIGHTEEN
A(4)AA		EIGHTEENTH
A(4)A	ELS	EWHERE
A(4)A		EMERGENCY
A(4)A		ENCODE
A(4)A		ENCODED
A(4)A		ENEMIES
A(4)A		ENGAGE
A(4)A(1)A		ENGAGEMENT
A(4)A		ENGINE
A(4)AA		ENGINEER
A(4)AA		ENGINEERING
A(4)A		ENTIRE
A(4)A		EUROPE
A(4)A		EUROPEAN
A(4)A	EXC	ESSIVE
A(4)A		EXCITE
A(4)A(1)A		EXCITEMENT
A(4)A	EX	ERCISE
A(4)A	EX	ERCISES

Table D-7—*Continued*

A(4)A	EXP	ENSIVE	A(4)A	R	EJECTED
A(4)A	EXT	ENSIVE	A(4)A	R	ELEASE
A(4)A	FL	EXIBLE	A(4)A	R	ELIEVE
A(4)A	IMM	EDIATE	A(4)A	R	EMEDIES
A(4)A	IMPR	ESSIVE	A(4)A	R	EMEMBER
A(4)A	INC	ENTIVE	A(4)A	R	EPAIRED
A(4)A	INCOMP	ETENCE	A(4)A	R	EPEATED
A(4)A	IND	EPENDENT	A(4)A	R	EPEATER
A(4)A(2)A	INT	ELLIGENCE	A(4)A	R	EPELLED
A(4)A	INT	ELLIGENT	A(4)A	R	EPLACE
A(4)A	INT	ENSIVE	A(4)A(1)A	R	EPLACEMENT
A(4)A	INT	ERFERE	A(4)A	R	EPORTED
A(4)A	INTERF	ERENCE	A(4)A	R	EPRESENT
A(4)A(2)A	INT	ERFERENCE	A(4)A	R	EPRESENTATION
A(4)A	INTERM	EDIATE	A(4)A(6)A	R	EPRESENTATIVE
A(4)A	INT	ERPOSE	A(4)A	R	EPULSED
A(4)A	INT	ERVENE	A(4)A	R	EQUIRE
A(4)A	L	ECTURE	A(4)A(1)A	R	EQUIREMENT
A(4)A	L	ETTERED	A(4)A	R	ESERVE
A(4)A	MAINT	ENANCE	A(4)A	R	ESERVES
A(4)A(1)A	M	EASUREMENT	A(4)A	R	ESTORED
A(4)A(1)A	M	EASUREMENTS	A(4)A	R	ETURNED
A(4)A	M	ESSAGE	A(4)A	R	EVENUE
A(4)A	M	ESSAGES	A(4)A	R	EVERSE
A(4)A	MISC	ELLANEOUS	A(4)A	R	EVIEWED
A(4)A(2)A	N	EGLIGENCE	A(4)A	R	EVOLVE
A(4)A	N	EGLIGENT	A(4)A	R	EVOLVER
A(4)A	OBJ	ECTIVE	A(4)A	S	EALEVEL
A(4)A	OFF	ENSIVE	A(4)A	S	ELECTED
A(4)A	PEN	ETRATE	A(4)A	S	ENTINEL
A(4)A	P	ERMANENT	A(4)A	S	ERVICE
A(4)A	PREC	EDENCE	A(4)AA	S	EVENTEEN
A(4)A	PREF	ERENCE	A(4)AA	S	EVENTEENTH
A(4)A	PR	EFERRED	A(4)A	SMOK	ESCREEN
A(4)A	PR	ESERVE	A(4)A	SUCC	ESSIVE
A(4)A	PR	ESSURE	A(4)A	SURR	ENDERED
A(4)A	PROGR	ESSIVE	A(4)A	TEL	EPHONE
A(4)A	RANG	EFINDER	A(4)A(1)A	TH	ERMOMETER
A(4)A	R	EADINESS	A(4)A	THR	EATENED
A(4)A	R	ECEIVE	A(4)A	UNT	ENABLE
A(4)A	R	ECEIVER	A(4)A	V	EHICLES
A(4)A	R	ECOMMEND	A(4)A		FORTIFIED
A(4)A	R	ECOMMENDATION	A(4)A	EN	GAGING
A(4)A(2)A	R	ECOMMENDED	A(4)A	FI	GHTING
A(4)A	R	ECORDER	A(4)A	SI	GHTING
A(4)A	REF	ERENCE	A(4)A	BREAKT	HROUGH
A(4)A	R	EFUGEE	A(4)A	S	HARPSHOOTER
A(4)A	R	EGISTER	A(4)A	T	HROUGH

Table D-7—*Continued*

A(4)A	ARB	ITRATION	A(4)A		LEGISLATION
A(4)A	CONC	ILIATION	A(4)A		LIABILITY
A(4)A	CONF	IDENTIAL	A(4)A	NAVA	LBATTLE
A(4)A	CONF	IRMATION	A(4)A	ATO	MICBOMB
A(4)A	CONF	ISCATION	A(4)A	BO	MBARDMENT
A(4)A	CONT	INUATION	A(4)A	COM	MENCEMENT
A(4)A	DES	IGNATION	A(4)A	CO	MPARTMENT
A(4)A	D	IETITIAN	A(4)A	E	MPLOYMENT
A(4)A	DIFF	ICULTIES	A(4)A	I	MPEDIMENTA
A(4)A	D	IMENSION	A(4)A		MARKSMANSHIP
A(4)A	D	IRECTION	A(4)A		MEDIUM
A(4)A(1)A	D	ISPOSITION	A(4)A(2)A		MEDIUMBOMBER
A(4)A	D	ISSEMINATED	A(4)A		MILLIMETER
A(4)A(3)A	D	ISSEMINATION	A(4)A	AMMU	NITION
A(4)A	ENG	INEERING	A(4)A	ANNOU	NCEMENT
A(4)A		IDENTICAL	A(4)A	A	NTITANK
A(4)A(1)A(3)A		IDENTIFICATION	A(4)A	ARRA	NGEMENT
A(4)A		IDENTIFY	A(4)A	CE	NTERING
A(4)A		IGNITION	A(4)A	COI	NCIDENCE
A(4)A		ILLUMINATE	A(4)A	COMME	NCEMENT
A(4)A(3)A		ILLUMINATING	A(4)A	CO	NFERENCE
A(4)A(3)A		ILLUMINATION	A(4)A	CO	NFIDENCE
A(4)A		IMMEDIATE	A(4)A	CO	NFIDENT
A(4)A	IMM	IGRATION	A(4)A	CO	NFIDENTIAL
A(4)A		IMPEDIMENTA	A(4)A	CON	NECTING
A(4)A		INDIVIDUAL	A(4)A	CO	NTINENTAL
A(4)A(1)A		INEFFICIENCY	A(4)A	COORDI	NATION
A(4)A		INHABITED	A(4)A	DEFI	NITION
A(4)A		INTERIOR	A(4)A	DESIG	NATION
A(4)A		INVADING	A(4)A	DETERMI	NATION
A(4)A		INVASION	A(4)A	DETO	NATION
A(4)A	LEG	ISLATION	A(4)A	DISSEMI	NATION
A(4)A	L	IABILITY	A(4)A	DISTI	NCTION
A(4)A	NAT	IONALISM	A(4)A	DOMI	NATION
A(4)A	NAT	IONALITY	A(4)A	E	NDURANCE
A(4)A	PH	ILIPPINES	A(4)A	E	NGAGING
A(4)A	PRES	IDENTIAL	A(4)A	ENGI	NEERING
A(4)A	RES	IGNATION	A(4)A	E	NTERING
A(4)A	S	IGNIFICANCE	A(4)A	E	NTRAIN
A(4)A	S	IGNIFICANT	A(4)A	E	NTRAINED
A(4)A	S	ITUATION	A(4)A	EXAMI	NATION
A(4)A(1)A	UN	IDENTIFIED	A(4)A	EXPLA	NATION
A(4)A	V	ICTORIOUS	A(4)A	EXTERMI	NATION
A(4)A	AGRICU	LTURAL	A(4)A	IG	NITION
A(4)A	BATT	LEFIELD	A(4)A	ILLUMI	NATION
A(4)A	E	LIGIBLE	A(4)A	I	NCIDENCE
A(4)A	F	LEXIBLE	A(4)A	I	NCIDENT
A(4)A	I	LLEGAL	A(4)A(2)A	I	NDEPENDENT

Table D-7—*Continued*

A(4)A	I	NFLUENCE	A(4)A	T	ORPEDO
A(4)A	INTER	NATIONAL	A(4)AA		PHILIPPINES
A(4)A	I	NVADING	A(4)A	TO	POGRAPHIC
A(4)A	JU	NCTION	A(4)A	AI	RCONTROL
A(4)A	MAI	NTENANCE	A(4)A	ARMO	REDCAR
A(4)A	MU	NITIONS	A(4)A	CHA	RACTER
A(4)A		NATIONAL	A(4)A	CHA	RACTERISTIC
A(4)A		NATIONALISM	A(4)A	CI	RCULAR
A(4)A		NATIONALITY	A(4)A	CO	RRIDOR
A(4)A	NI	NETEEN	A(4)A	C	RUISER
A(4)A	NI	NETEENTH	A(4)A	C	RUISERS
A(4)A		NOTHING	A(4)A	DI	RECTOR
A(4)A	RA	NGEFINDER	A(4)A	EXTRAO	RDINARY
A(4)A	RECOG	NITION	A(4)A	FI	REALARM
A(4)A	RESIG	NATION	A(4)A	INST	RUCTOR
A(4)A	ROADJU	NCTION	A(4)A	NO	RTHWARD
A(4)A	SIG	NALLING	A(4)A	P	REFERRED
A(4)A	SY	NCHRONIZE	A(4)A	P	RESSURE
A(4)A	U	NEXPENDED	A(4)A		REPAIR
A(4)A	U	NKNOWN	A(4)A		REPAIRED
A(4)A	VETERI	NARIAN	A(4)A		REQUIRE
A(4)A	ACCOMM	ODATION	A(4)A		REQUIREMENT
A(4)A	ALL	OCATION	A(4)A		REQUIRING
A(4)A	AT	OMICBOMB	A(4)A		RESEARCH
A(4)A	C	ODEBOOK	A(4)A		RESOURCES
A(4)A	COMP	OSITION	A(4)A		RESTORED
A(4)A	CORP	ORATION	A(4)A		RUBBER
A(4)A	C	ORRIDOR	A(4)A		RUNNER
A(4)A	DEC	ORATION	A(4)A	SUR	RENDER
A(4)A	DET	ONATION	A(4)A	SUR	RENDERED
A(4)A	DISP	OSITION	A(4)A	TE	RRITORY
A(4)A	F	ORENOON	A(4)A	T	RACTOR
A(4)A	INTR	ODUCTORY	A(4)A	T	RAILERS
A(4)A	L	OCATION	A(4)A	T	RAWLER
A(4)A		OPINION	A(4)A	T	RIGGER
A(4)A	OPP	OSITION	A(4)A	ASSES	SMENTS
A(4)A		OVERCOMING	A(4)A	AS	SOONAS
A(4)A	P	OSITION	A(4)A	BU	SINESS
A(4)A	P	OSITIONS	A(4)A	CARELE	SSNESS
A(4)A	PR	OJECTOR	A(4)A	CROS	SROADS
A(4)A	PR	OMOTION	A(4)A	DI	STRESS
A(4)A	PR	OTECTOR	A(4)A	DI	STRESSED
A(4)A	PR	OVISION	A(4)A	I	SLANDS
A(4)A	PR	OVISIONS	A(4)A	ME	SSAGES
A(4)A	REV	OLUTION	A(4)A	MI	SFIRES
A(4)A	REV	OLUTIONARY	A(4)A	MI	SSIONS
A(4)A	T	OBACCO	A(4)A	OUT	SKIRTS
A(4)A	T	OMORROW	A(4)A	PRI	SONERS

Table D-7—*Continued*

A(4)A	RE	SERVES
A(4)A	RE	SPECTS
A(4)A		SHARPSHOOTER
A(4)A		SHELLS
A(4)A		SMOKESCREEN
A(4)A		SPOOLS
A(4)A		SPOONS
A(4)A		STATES
A(4)A(3)A		STATISTICS
A(4)A		STATUS
A(4)A		STRESS
A(4)A		STRIPS
A(4)AA		SUBMISSION
A(4)A		SUBSISTENCE
A(4)AA		SUCCESS
A(4)AA		SUCCESSFUL
A(4)AA		SUCCESSFULLY
A(4)AA		SUCCESSIVE
A(4)A		SUGGEST
A(4)A		SUNRISE
A(4)A		SUPPOSE
A(4)A	TRAN	SPORTS
A(4)A	UNITED	STATES
A(4)AA	UN	SUCCESSFUL
A(4)A	U	SELESS
A(4)A	AL	TERNATE
A(4)A	AL	TERNATING
A(4)A	A	TTEMPT
A(4)A	A	TTEMPTED
A(4)A	CHARAC	TERISTIC
A(4)A	CON	TINENTAL
A(4)A	CON	TINUATION
A(4)A	COUN	TERATTACK
A(4)A	DIS	TRIBUTE
A(4)A	DIS	TRIBUTING
A(4)A	DIS	TRIBUTION
A(4)A	ELEC	TRICITY
A(4)A	EXCI	TEMENT
A(4)A	INS	TALLATIONS
A(4)A	IN	TEGRITY
A(4)A	IN	TEREST
A(4)A	IN	TERESTING
A(4)A	IN	TERNATIONAL
A(4)A	LIEU	TENANT
A(4)A	NOR	THEAST
A(4)A	NOR	THWEST
A(4)A	NOR	THWESTERN
A(4)A	OU	TSKIRTS
A(4)A	REINSTA	TEMENT
A(4)A	RES	TRAINT
A(4)A	RE	TALIATION
A(4)A	RE	TROACTIVE
A(4)A	SOU	THEAST
A(4)A	SOU	THWEST
A(4)A	SOU	THWESTERN
A(4)A	STA	TEMENT
A(4)A	S	TATISTICS
A(4)A		TARGET
A(4)A		TENTATIVE
A(4)A		TERRITORY
A(4)A		THREAT
A(4)A		THREATENED
A(4)A		TRADITIONAL
A(4)A		TURRET
A(4)A		TWELFTH
A(4)A	L	UMINOUS
A(4)A	MAN	UFACTURE
A(5)A		ACCEPTABLE
A(5)A		ACCEPTANCE
A(5)A		ACCOMPANY
A(5)A		ACCORDANCE
A(5)A		ADVANTAGE
A(5)A		ADVANTAGEOUS
A(5)A		ALLEGIANCE
A(5)A		ALTERNATE
A(5)A		ALTERNATING
A(5)A		AMBASSADOR
A(5)A		AMERICA
A(5)A		AMERICAN
A(5)A		ANTENNA
A(5)A		APPEARANCE
A(5)A		APPLICATION
A(5)A		APPROVAL
A(5)A		ARBITRARY
A(5)A		ARBITRATION
A(5)A		ASSISTANCE
A(5)A		ASSISTANT
A(5)A		ASSOCIATE
A(5)A		ASSOCIATION
A(5)A		ASSOONAS
A(5)A	C	ABLEGRAM
A(5)A	C	AMOUFLAGE
A(5)A	C	ANCELLATION
A(5)A	DIS	APPEARANCE
A(5)A	EXTR	AORDINARY
A(5)A	M	AINTENANCE

Table D-7—*Continued*

A(5)A	QU	ALIFICATION
A(5)A	QU	ARTERMASTER
A(5)A	R	ADIOGRAM
A(5)A	R	ADIOSTATION
A(5)A	STR	ATEGICAL
A(5)A	TR	ANSATLANTIC
A(5)A	AC	CEPTANCE
A(5)A	AC	CORDANCE
A(5)A		CHRONICLE
A(5)A		COEFFICIENT
A(5)A		COMMENCE
A(5)A		COMMENCEMENT
A(5)A		COMMERCE
A(5)A		CONFISCATION
A(5)A		CONFLICT
A(5)A		CONTACT
A(5)A	DIS	CREPANCIES
A(5)A	DIS	CREPANCY
A(5)A	E	CONOMIC
A(5)A	AD	DRESSED
A(5)A	A	DVANCED
A(5)A	BRI	DGEHEAD
A(5)A		DAMAGED
A(5)A		DECIDED
A(5)A		DELAYED
A(5)A		DROPPED
A(5)A	IN	DICATED
A(5)A	ACC	EPTABLE
A(5)A	ACC	EPTANCE
A(5)A	ALL	EGIANCE
A(5)A	APP	EARANCE
A(5)A	CAR	ELESSNESS
A(5)A	CL	EARANCE
A(5)A	CO	EFFICIENT
A(5)A	CONC	ENTRATE
A(5)A(2)A	CORR	ESPONDENCE
A(5)A	D	ECREASE
A(5)A	D	ECREASED
A(5)A	D	EDICATE
A(5)A	D	EFINITE
A(5)A	D	EPARTMENT
A(5)A	D	EPARTMENTAL
A(5)A	DEP	ENDABLE
A(5)A	D	EPLOYMENT
A(5)A	D	ESCRIBE
A(5)A	D	ESCRIBED
A(5)A	D	ESTROYED
A(5)A	D	ESTROYER
A(5)A	D	DESTROYERS
A(5)A	D	ETACHMENT
A(5)A	D	ETONATE
A(5)A	D	ETONATED
A(5)A	D	ETRAINED
A(5)A	D	EVELOPED
A(5)A	DISAPP	EARANCE
A(5)A	DISCR	EPANCIES
A(5)A	DISS	EMINATED
A(5)A		EFFECTED
A(5)A		EFFICIENCY
A(5)A		EFFICIENT
A(5)A		EIGHTEEN
A(5)A		EIGHTEENTH
A(5)A		ELEVATE
A(5)A(1)A		ELSEWHERE
A(5)A(1)A		EMPLACEMENT
A(5)AA		EMPLOYEE
A(5)A		EMPLOYER
A(5)A		ENCIPHER
A(5)A(1)A		ENCIPHERED
A(5)A(2)A		ENCIPHERMENT
A(5)A		ENFORCE
A(5)A(1)A		ENFORCEMENT
A(5)A		ENGINEER
A(5)A		ENGINEERING
A(5)A		ENLISTED
A(5)A		ENROLLED
A(5)A		ENTENTE
A(5)A	ENT	ERPRISE
A(5)A		EQUIPMENT
A(5)A		ESCORTED
A(5)A		EXCLUDE
A(5)A	EX	ECUTIVE
A(5)A		EXPANDED
A(5)A		EXPELLED
A(5)A		EXPENDED
A(5)A		EXPENSES
A(5)A	EXP	ERIENCE
A(5)A(2)A		EXPERIENCE
A(5)A		EXTENDED
A(5)A		EXTREME
A(5)A	FIGHT	ERPLANE
A(5)A	H	ELICOPTER
A(5)A	IN	EFFICIENCY
A(5)A	INT	ERCEPTED
A(5)A	INT	ERPRETER
A(5)A	INT	ERRUPTED

Table D-7—*Continued*

A(5)A	J	ETPLANE	A(5)A	D	ISPERSION
A(5)A	M	EDICINE	A(5)A	IDENT	IFICATION
A(5)A	M	ESSENGER	A(5)A		IMPASSIBLE
A(5)A	N	EWSPAPER	A(5)A		IMPOSSIBLE
A(5)A	N	EWSPAPERS	A(5)A		INCENDIARY
A(5)A	ON	EHUNDRED	A(5)A		INCENTIVE
A(5)A	PAR	ENTHESES	A(5)A		INCLINING
A(5)A	P	ERSISTENT	A(5)A		INCLUDING
A(5)A	P	ERSONNEL	A(5)A		INCLUSIVE
A(5)A	PR	EMATURE	A(5)A		INDEMNITY
A(5)A	PR	ESCRIBED	A(5)A		INFLATION
A(5)A	QUART	ERMASTER	A(5)A		INSIGNIA
A(5)A	REC	EPTACLE	A(5)A		INTEGRITY
A(5)A	RE	ENFORCE	A(5)A		INTELLIGENCE
A(5)A(1)A	RE	ENFORCEMENT	A(5)A		INTELLIGENT
A(5)A	RE	ENLISTED	A(5)A		INTENSIVE
A(5)A	R	EMAINDER	A(5)A		INTENTION
A(5)A	R	EQUESTED	A(5)A		INTERDICT
A(5)A	R	ESOURCES	A(5)A(2)A		INTERDICTION
A(5)A	S	EABORNE	A(5)A		INTERVIEW
A(5)A	S	EAPLANES	A(5)A		INVENTION
A(5)A	S	ENTENCE	A(5)A		INVESTIGATE
A(5)A	S	EPARATE	A(5)A(3)A		INVESTIGATION
A(5)A	S	EPTEMBER	A(5)A(3)A		INVESTIGATIONS
A(5)A	S	EVENTEEN	A(5)A	L	IMITATION
A(5)A	S	EVENTEENTH	A(5)A	MOB	ILIZATION
A(5)A	SH	ELLFIRE	A(5)A	PREL	IMINARIES
A(5)A	TEMP	ERATURE	A(5)A	QUAL	IFICATION
A(5)A	T	ERRIBLE	A(5)A	RAD	IOSTATION
A(5)A	TH	EREFORE	A(5)A	REG	ISTRATION
A(5)A	UN	EXPENDED	A(5)A	S	IGNALLING
A(5)A	UNID	ENTIFIED	A(5)A	S	IMILARITY
A(5)A	UNIT	EDSTATES	A(5)A	SPEC	IFICATION
A(5)A	BE	GINNING	A(5)A	SU	ITABILITY
A(5)A		GASSING	A(5)A	VER	IFICATION
A(5)A		GETTING	A(5)A	V	ISIBILITY
A(5)A	RE	GARDING	A(5)A	CHRONO	LOGICAL
A(5)A	EIG	HTEENTH	A(5)A	C	LERICAL
A(5)A	ADMIN	ISTRATION	A(5)A	INF	LAMMABLE
A(5)A	ADMIN	ISTRATIVE	A(5)A		LOGICAL
A(5)A	ANT	ICIPATION	A(5)A	METEORO	LOGICAL
A(5)A	CLASS	IFICATION	A(5)A	PO	LITICAL
A(5)A	CONS	IDERATION	A(5)A	CO	MMENCEMENT
A(5)A	DEMOB	ILIZATION	A(5)A	E	MPLACEMENT
A(5)A	D	ISCIPLINE	A(5)A	I	MPROVEMENT
A(5)A	D	ISCONTINUANCE	A(5)A		MANAGEMENT
A(5)A	D	ISCONTINUE	A(5)A		MARITIME
A(5)A	D	ISCUSSION	A(5)A		MAXIMUM

Table D-7—*Continued*

A(5)A		MINIMUM	A(5)A	REC	OGNITION
A(5)A	REI	MBURSEMENT	A(5)A	TRANSP	ORTATION
A(5)A	COMME	NDATION	A(5)A		PHILIPPINES
A(5)A	COMPE	NSATION	A(5)A		PRINCIPAL
A(5)A	CONCE	NTRATING	A(5)A		PRINCIPLE
A(5)A	CO	NCERNING	A(5)A	AI	RSUPPORT
A(5)A	CO	NDITION	A(5)A	A	RBITRARY
A(5)A	CO	NNECTING	A(5)A	A	RTILLERY
A(5)A	CON	NECTION	A(5)A	BA	ROMETER
A(5)A	CO	NTINGENT	A(5)A	B	REAKTHROUGH
A(5)A	CONTI	NUATION	A(5)A	FI	RECONTROL
A(5)A	CO	NTRABAND	A(5)A	GENE	RALALARM
A(5)A	CO	NVENIENT	A(5)A	GY	ROMETER
A(5)A	DISCO	NTINUANCE	A(5)A	HYD	ROMETER
A(5)A	E	NEMYTANKS	A(5)A	HYG	ROMETER
A(5)A	E	NLISTING	A(5)A	INTE	RPRETER
A(5)A	ENTA	NGLEMENT	A(5)A	IR	REGULAR
A(5)A	FOU	NDATION	A(5)A	IR	REGULARITIES
A(5)A	I	NCLINING	A(5)A	IR	REGULARITY
A(5)A	I	NCLUDING	A(5)A	P	REMATURE
A(5)A	I	NTERMENT	A(5)A	P	RISONER
A(5)A	I	NTERVENE	A(5)A	P	RISONERS
A(5)A(1)A	I	NTERVENING	A(5)A	P	ROCEDURE
A(5)A(3)A	I	NTERVENTION	A(5)A	PSYCH	ROMETER
A(5)A	I	NVASION	A(5)A	QUARTE	RMASTER
A(5)A	MA	NAGEMENT	A(5)A		RADIOGRAM
A(5)A	RECOMME	NDATION	A(5)A		RECOVER
A(5)A	RECON	NAISSANCE	A(5)A		REENFORCE
A(5)A	REPRESE	NTATION	A(5)A		REENFORCEMENT
A(5)A	SIG	NIFICANCE	A(5)A		REGISTRATION
A(5)A	SIG	NIFICANT	A(5)A		REGULAR
A(5)A	TRA	NSATLANTIC	A(5)A		REIMBURSEMENT
A(5)A	ASS	OCIATION	A(5)A		REINFORCE
A(5)A	C	OALITION	A(5)A		REINFORCEMENT
A(5)A	C	OLLISION	A(5)A	ST	RAGGLER
A(5)A	C	OLLISIONS	A(5)A	SU	RRENDER
A(5)A	C	ONDITION	A(5)A	SU	RRENDERED
A(5)A	CONF	ORMATION	A(5)A	T	RANSFER
A(5)A	C	ONTINUOUS	A(5)AA	T	RANSFERRED
A(5)A	C	ORRESPONDENCE	A(5)AA	T	RANSFERRING
A(5)A	C	ORRESPONDING	A(5)A	T	RANSPORT
A(5)A	F	ORMATION	A(5)A	T	RANSPORTATION
A(5)A	INF	ORMATION	A(5)A	T	RANSPORTS
A(5)A	INTR	ODUCTION	A(5)A	T	RANSVERSE
A(5)A		OPERATOR	A(5)A	ASSE	SSMENTS
A(5)A	PR	OPORTION	A(5)A	A	SSOONAS
A(5)A	PR	OTECTION	A(5)A	CIRCUM	STANCES
A(5)A	RADI	OSTATION	A(5)A	CRO	SSROADS

Table D-7—*Continued*

A(5)A	DI	STRICTS	A(5)A	UNI	TEDSTATES
A(5)A	E	STABLISH	A(5)A	S	UBSTITUTE
A(5)A	E	STABLISHED	A(5)A	S	UBSTITUTION
A(5)A	E	STABLISHMENT	A(6)A		ANTICIPATE
A(5)A	NEW	SPAPERS	A(6)A		ANTICIPATION
A(5)A	PHO	SPHORUS	A(6)A	CL	ASSIFICATION
A(5)A	PO	SITIONS	A(6)A	DEP	ARTMENTAL
A(5)A	RE	SOURCES	A(6)A	TR	ADITIONAL
A(5)A		SAILORS	A(6)A	TR	ANSPORTATION
A(5)A		SECTORS	A(6)A	A	CCEPTANCE
A(5)A		SERIOUSLY	A(6)A	A	CCORDANCE
A(5)A		SKIRMISH	A(6)A		CERTIFICATE
A(5)A		SUBMISSION	A(6)A	CIR	CUMSTANCES
A(5)A		SUCCESS	A(6)A		CLEARANCE
A(5)A		SUCCESSFUL	A(6)A		COMMUNICATE
A(5)A		SUCCESSFULLY	A(6)A		COMMUNICATION
A(5)A		SUCCESSIVE	A(6)A		CONSTRUCTION
A(5)A		SURPLUS	A(6)A	RE	CONSTRUCTION
A(5)A		SURPRISE	A(6)A	A	DDRESSED
A(5)A		SUSPENSE	A(6)A		DECLARED
A(5)A		SUSPENSION	A(6)A		DEFEATED
A(5)A	UN	SUCCESSFUL	A(6)A		DEFENDED
A(5)A	AN	TICIPATE	A(6)A		DEFERRED
A(5)A	AN	TICIPATION	A(6)A		DEMANDED
A(5)A	CER	TIFICATE	A(6)A		DEPARTED
A(5)A	CON	TINGENT	A(6)A		DEPLOYED
A(5)A	IDEN	TIFICATION	A(6)A		DEPORTED
A(5)A	INS	TRUMENT	A(6)A		DESERTED
A(5)A	INS	TRUMENTS	A(6)A		DETACHED
A(5)A	IN	TERCEPT	A(6)A		DICTATED
A(5)A	IN	TERCEPTED	A(6)A		DISARMED
A(5)A	IN	TERDICT	A(6)A	UN	DERSTAND
A(5)A	IN	TERDICTION	A(6)A	UN	DERSTOOD
A(5)A	IN	TERMENT	A(6)A	B	EENNEEDED
A(5)A(1)A	IN	TERPRETATION	A(6)A	B	ELLIGERENT
A(5)A	IN	TERPRETER	A(6)A	D	ECIPHERED
A(5)A	IN	TERRUPT	A(6)A	D	EFECTIVE
A(5)A	IN	TERRUPTED	A(6)A	D	EFENSIVE
A(5)A	IN	TERRUPTION	A(6)A	D	EPARTURE
A(5)A	IN	TERVENTION	A(6)A	D	ESIGNATE
A(5)A	IN	TRODUCTION	A(6)A	D	ESIGNATED
A(5)A	IN	TRODUCTORY	A(6)A	D	ESPATCHED
A(5)A	QUAR	TERMASTER	A(6)A	D	ESPATCHES
A(5)A	SA	TISFACTORY	A(6)A	D	ESTITUTE
A(5)A	SUI	TABILITY	A(6)A	DET	ERIORATE
A(5)A		TONIGHT	A(6)A	D	ETERMINE
A(5)A		TRAJECTORY	A(6)A	D	ETERMINED
A(5)A(3)A		TRANSATLANTIC	A(6)A	D	EVELOPMENT

Table D-7—*Continued*

A(6)A		ECHELONED	A(6)A	R	EENLISTED
A(6)A		ELIGIBLE	A(6)A	RE	ENLISTMENT
A(6)A		EMBASSIES	A(6)A	R	EFERENCE
A(6)A		EMPLOYEE	A(6)A(1)A	R	EIMBURSEMENT
A(6)A		EMPLOYMENT	A(6)A	R	EINFORCE
A(6)A		ENCIRCLE	A(6)A(1)A	R	EINFORCEMENT
A(6)A		ENCOUNTER	A(6)A	R	EINSTATE
A(6)A(1)A		ENCOUNTERED	A(6)A(1)A	R	EINSTATEMENT
A(6)A	EN	EMYPLANES	A(6)A	R	EPLACEMENT
A(6)A		ENFILADE	A(6)A	REPRES	ENTATIVE
A(6)A		ENGAGEMENT	A(6)A	R	EQUIREMENT
A(6)A		ENLISTMENT	A(6)A	R	ESTRICTED
A(6)A		ENROLLMENT	A(6)A	SEV	ENTYFIVE
A(6)A		ENTANGLE	A(6)A	T	ECHNIQUE
A(6)A(1)A		ENTANGLEMENT	A(6)A	T	ELEPHONE
A(6)A	ENT	ERTAINMENT	A(6)A	T	ENTATIVE
A(6)A		ENTRAINED	A(6)A	TH	ERMOMETER
A(6)A		ENVELOPE	A(6)A	TW	ENTYFIVE
A(6)A		EQUALIZE	A(6)A	DISTIN	GUISHING
A(6)A		EQUIVALENT	A(6)A		GROUPING
A(6)A		ESTIMATE	A(6)A		GUARDING
A(6)A		ESTIMATEDAT	A(6)A	SI	GNALLING
A(6)A		ESTIMATES	A(6)A	C	IRCULATION
A(6)A		EVACUATE	A(6)A	D	IPLOMATIC
A(6)A		EXCAVATE	A(6)A	D	ISORGANIZED
A(6)A		EXCHANGE	A(6)A	D	ISPOSITION
A(6)A		EXCITEMENT	A(6)A	D	ISTINCTION
A(6)A		EXERCISE	A(6)A	D	ISTINGUISH
A(6)A		EXERCISES	A(6)A	D	ISTINGUISHED
A(6)A		EXHIBITED	A(6)A	DIST	INGUISHING
A(6)A		EXPEDITE	A(6)A(2)A	D	ISTINGUISHING
A(6)A		EXPERIMENT	A(6)A	F	INGERPRINT
A(6)A	EXT	ERMINATE	A(6)A(3)A		IDENTIFICATION
A(6)A	INDET	ERMINATE	A(6)A		IMPRACTICABLE
A(6)A	INV	ESTIGATE	A(6)A		IMPRESSION
A(6)A	M	EASUREMENT	A(6)A		IMPRESSIVE
A(6)A	M	EASUREMENTS	A(6)A		INDICATING
A(6)A	M	ECHANIZED	A(6)A		INDICATION
A(6)A	NEC	ESSITATE	A(6)A		INEFFICIENCY
A(6)A	OV	ERWHELMED	A(6)A		INFLICTING
A(6)A	P	ENETRATE	A(6)A		INSECURITY
A(6)A	PR	EARRANGED	A(6)A		INSPECTION
A(6)A	PR	ECEDENCE	A(6)A		INVITATION
A(6)A	PR	EFERENCE	A(6)A		IRRIGATION
A(6)A	PR	EPAREDNESS	A(6)A	UN	IDENTIFIED
A(6)A	R	ECOGNIZE	A(6)A	W	ITHDRAWING
A(6)A	R	EENFORCE	A(6)A		MEASUREMENT
A(6)A(1)A	R	EENFORCEMENT	A(6)A		MEASUREMENTS

Table D-7—*Continued*

A(6)A	ME	MORANDUM
A(6)A	COMMU	NICATION
A(6)A	CO	NCEALMENT
A(6)A	CONCE	NTRATION
A(6)A	CO	NCESSION
A(6)A	CO	NCLUSION
A(6)A	CO	NFESSION
A(6)A	CO	NFINEMENT
A(6)A	CO	NNECTION
A(6)A	DISTI	NGUISHING
A(6)A	E	NCIRCLING
A(6)A	E	NEMYPLANES
A(6)A	E	NLISTMENT
A(6)A	E	NROLLMENT
A(6)A(2)A	E	NTERTAINMENT
A(6)A	E	NTRUCKING
A(6)A	FI	NGERPRINT
A(6)A	I	NDICATING
A(6)A	I	NFLATION
A(6)A	I	NFLICTING
A(6)A	I	NSTANTANEOUS
A(6)A	I	NSTRUMENT
A(6)A	I	NSTRUMENTS
A(6)A	I	NTENTION
A(6)A	I	NTERNMENT
A(6)A	I	NVENTION
A(6)A		NEGLIGENCE
A(6)A		NEGLIGENT
A(6)A		NINETEEN
A(6)A		NINETEENTH
A(6)A		NORTHERN
A(6)A		NUMBERING
A(6)A	ORGA	NIZATION
A(6)A	RECO	NNAISSANCE
A(6)A	RECON	NOITERING
A(6)A	REE	NLISTMENT
A(6)A	REORGA	NIZATION
A(6)A	SA	NITATION
A(6)A	TRA	NSFERRING
A(6)A	U	NDERSTAND
A(6)A	C	OLLECTION
A(6)A	C	OMMISSION
A(6)A	C	OMMISSIONER
A(6)A	C	ONCESSION
A(6)A	C	ONCLUSION
A(6)A	C	ONFESSION
A(6)A	C	ONNECTION
A(6)A	CO	OPERATION
A(6)A	C	ORRECTION
A(6)A	D	OMINATION
A(6)A	F	OUNDATION
A(6)A		OBJECTION
A(6)A		OPERATION
A(6)A	P	OPULATION
A(6)A	P	OSSESSION
A(6)A		PARAGRAPH
A(6)A	AG	RICULTURAL
A(6)A	B	RIGADIER
A(6)A	INT	RODUCTORY
A(6)A	I	RREGULAR
A(6)A	I	RREGULARITIES
A(6)A	I	RREGULARITY
A(6)A	P	ROJECTOR
A(6)A	P	ROTECTOR
A(6)A		REARGUARD
A(6)A		RECEIVER
A(6)A		RECONSTRUCTION
A(6)A		RECORDER
A(6)A		REGISTER
A(6)A		REJECTOR
A(6)A		REMEMBER
A(6)A		REPEATER
A(6)A		REVOLVER
A(6)A	THE	RMOMETER
A(6)A	T	RAJECTORY
A(6)A	T	RANSFERRED
A(6)A	T	RANSFERRING
A(6)A	AS	SEMBLIES
A(6)A	CA	SUALTIES
A(6)A	CU	STOMHOUSE
A(6)A	DE	SPATCHES
A(6)A	DE	STROYERS
A(6)A	DI	SPATCHES
A(6)A	DI	STINGUISH
A(6)A	DI	STINGUISHED
A(6)A	DI	STINGUISHING
A(6)A	E	STIMATES
A(6)A		SOLDIERS
A(6)A		SOUTHEAST
A(6)A		SOUTHWEST
A(6)A		SOUTHWESTERN
A(6)A		STATIONS
A(6)A		SUPPLIES
A(6)A	SU	SPICIONS
A(6)A	SU	SPICIOUS
A(6)A	AT	TACHMENT

Table D-7—*Continued*

A(6)A	AT	TAINMENT	A(7)A		DISCUSSED
A(6)A	CEN	TRALIZATION	A(7)A		DISPERSED
A(6)A	DE	TACHMENT	A(7)A		DOMINATED
A(6)A	DE	TERIORATE	A(7)A	UNI	DENTIFIED
A(6)A	DE	TERMINATION	A(7)A	C	ENTRALIZE
A(6)A	ENTER	TAINMENT	A(7)A	DEC	ENTRALIZE
A(6)A	EX	TERMINATE	A(7)A	DEC	ENTRALIZED
A(6)A	EX	TERMINATION	A(7)A	D	EMOBILIZE
A(6)A	INDE	TERMINATE	A(7)A	D	EPENDABLE
A(6)A	IN	TERNMENT	A(7)A		ECHELONMENT
A(6)A	NA	TIONALITY	A(7)A		EFFECTIVE
A(6)A	REINS	TATEMENT	A(7)A		ELABORATE
A(6)A	S	TATEMENT	A(7)A		EMPLACEMENT
A(6)A		TEMPERATURE	A(7)A		ENCIPHERED
A(6)A		TWENTIETH	A(7)A		ENDURANCE
A(6)A	C	USTOMHOUSE	A(7)A		ENFORCEMENT
A(6)A	SIM	ULTANEOUS	A(7)A		ENTRENCHED
A(6)A	S	UCCESSFUL	A(7)A		EXCESSIVE
A(6)A	S	UCCESSFULLY	A(7)A		EXCLUSIVE
A(6)A	S	USPICIOUS	A(7)A		EXECUTIVE
A(6)A	UNS	UCCESSFUL	A(7)A		EXPANSIVE
A(6)A	SE	VENTYFIVE	A(7)A		EXPENSIVE
A(6)A		WITHDRAW	A(7)A		EXPLOSIVE
A(6)A		WITHDRAWAL	A(7)A		EXTENSIVE
A(6)A		WITHDRAWING	A(7)A	H	EADQUARTERS
A(6)A		WITHDREW	A(7)A	H	EAVYBOMBER
A(7)A		ACCIDENTAL	A(7)A	H	EAVYLOSSES
A(7)A		ACCOMMODATION	A(7)A	INT	ELLIGENCE
A(7)A		ADDITIONAL	A(7)A	INT	ERMEDIATE
A(7)A		APPROPRIATE	A(7)A	N	EGLIGENCE
A(7)A		APPROXIMATE	A(7)A	R	EAPPOINTED
A(7)A		ARMOREDCAR	A(7)A	R	ECEPTACLE
A(7)A		ARTIFICIAL	A(7)A	R	ECOMMENDED
A(7)A	N	ATURALIZATION	A(7)A	R	ECONNOITER
A(7)A	CHARA	CTERISTIC	A(7)A	R	ECONNOITERING
A(7)A		CLASSIFICATION	A(7)A	RE	ENFORCEMENT
A(7)A		CONFERENCE	A(7)A	R	EENLISTMENT
A(7)A		CONFIDENCE	A(7)A	R	ESISTANCE
A(7)A		CONSPIRACY	A(7)A	EN	GINEERING
A(7)A		CONVALESCENT	A(7)A	P	HOTOGRAPHY
A(7)A	IN	COMPETENCE	A(7)A	T	HIRTEENTH
A(7)A	D	ECIPHERMENT	A(7)A	ADM	INISTRATION
A(7)A		DECREASED	A(7)A	ADM	INISTRATIVE
A(7)A		DESCRIBED	A(7)A	D	IFFICULTIES
A(7)A		DESTROYED	A(7)A	D	ISTRIBUTING
A(7)A		DETONATED	A(7)A	D	ISTRIBUTION
A(7)A		DETRAINED	A(7)A		IMMIGRATION
A(7)A		DEVELOPED	A(7)A		INDETERMINATE

Table D-7—*Continued*

A(7)A		INFORMATION	A(7)A	CO	ORDINATION
A(7)A		INSPIRATION	A(7)A	C	ORPORATION
A(7)A		INSTITUTION	A(7)A	DEM	ONSTRATION
A(7)A		INSTRUCTION	A(7)A		OCCUPATION
A(7)A		INSTRUCTIONS	A(7)A		OPPOSITION
A(7)A		INTERESTING	A(7)A	PR	OCLAMATION
A(7)A		INTERFERING	A(7)A		PHOTOGRAPHY
A(7)A		INTERMEDIATE	A(7)A	A	RMOREDCAR
A(7)A		INTERNATIONAL	A(7)A	EXT	RAORDINARY
A(7)A		INTERVENING	A(7)A	NO	RTHWESTERN
A(7)A		MECHANISM	A(7)A	P	RELIMINARIES
A(7)A		MEDIUMBOMBER	A(7)A	P	RELIMINARY
A(7)A	AN	NOUNCEMENT	A(7)A		REMAINDER
A(7)A	CO	NGRESSIONAL	A(7)A	SHA	RPSHOOTER
A(7)A	CO	NSTITUTING	A(7)A	A	SSEMBLIES
A(7)A	CO	NSUMPTION	A(7)A	AS	SESSMENTS
A(7)A	CO	NVALESCENT	A(7)A	AS	SIGNMENTS
A(7)A	DEMO	NSTRATION	A(7)A	HO	STILITIES
A(7)A	E	NFORCEMENT	A(7)A	IN	STRUMENTS
A(7)A	E	NGINEERING	A(7)A	MEA	SUREMENTS
A(7)A	I	NCOMPETENCE	A(7)A		SEAPLANES
A(7)A	I	NCOMPETENT	A(7)A		STANDARDS
A(7)A	I	NDEPENDENT	A(7)A	A	TTACHMENT
A(7)A	I	NDETERMINATE	A(7)A	A	TTAINMENT
A(7)A	I	NDICATION	A(7)A	ES	TIMATEDAT
A(7)A	I	NEFFICIENCY	A(7)A	IN	TELLIGENT
A(7)A	I	NSPECTION	A(7)A	IN	TERMEDIATE
A(7)A	I	NTELLIGENCE	A(7)A	IN	TERPRETATION
A(7)A	I	NTELLIGENT	A(7)A	NA	TURALIZATION
A(7)A	I	NTERESTING	A(7)A		THERMOMETER
A(7)A	I	NTERFERENCE	A(7)A		THIRTEENTH
A(7)A	I	NTERFERING	A(7)A		TRANSPORT
A(7)A	I	NTERVENING	A(7)A(1)A		TRANSPORTATION
A(7)A	I	NVITATION	A(7)A		TRANSPORTS
A(7)A	NO	NCOMBATANT	A(7)A		YESTERDAY
A(7)A	PE	NETRATION	A(8)A		ADMINISTRATION
A(7)A	RECO	NNOITERING	A(8)A		ADMINISTRATIVE
A(7)A	REE	NFORCEMENT	A(8)A		ANTIAIRCRAFT
A(7)A	REI	NFORCEMENT	A(8)A		COINCIDENCE
A(7)A	REI	NSTATEMENT	A(8)A	DIS	CONTINUANCE
A(7)A	TRA	NSMISSION	A(8)A		DECIPHERED
A(7)A	ACC	OMMODATION	A(8)A		DESIGNATED
A(7)A	C	OMPETITION	A(8)A		DESPATCHED
A(7)A	C	OMPOSITION	A(8)A		DETERMINED
A(7)A	C	OMPUTATION	A(8)A		DISPATCHED
A(7)A	C	ONGRESSIONAL	A(8)A		DISTRESSED
A(7)A	C	ONSUMPTION	A(8)A	C	ERTIFICATE
A(7)A	C	OOPERATION	A(8)A	CORR	ESPONDENCE

Table D-7—*Continued*

A(8)A	D	EMONSTRATE	A(8)A	CO	NSTRUCTION
A(8)A	D	EMONSTRATED	A(8)A	CO	NTINUATION
A(8)A	D	ESCRIPTIVE	A(8)A	CO	NVERSATION
A(8)A	D	ETERIORATE	A(8)A	E	NCIPHERMENT
A(8)A		ENCIPHERMENT	A(8)A	E	NTANGLEMENT
A(8)A		ENCOUNTERED	A(8)A	E	NTERPRISING
A(8)A		ENEMYPLANES	A(8)A	I	NFORMATION
A(8)A		ENTANGLEMENT	A(8)A	I	NSPIRATION
A(8)A		ENTERPRISE	A(8)A	I	NSTITUTION
A(8)A		ESTABLISHED	A(8)A	I	NSTRUCTION
A(8)A	IND	ETERMINATE	A(8)A	I	NSTRUCTIONS
A(8)A	IRR	EGULARITIES	A(8)A	I	NTERNATIONAL
A(8)A	M	EDIUMBOMBER	A(8)A		NAVIGATION
A(8)A	N	ECESSITATE	A(8)A	RECO	NSTRUCTION
A(8)A	P	ERFORMANCE	A(8)A	C	OMMENDATION
A(8)A	PR	ELIMINARIES	A(8)A	C	OMPENSATION
A(8)A	R	EAPPOINTMENT	A(8)A	C	ONCILIATION
A(8)A	R	EENFORCEMENT	A(8)A	C	ONFIRMATION
A(8)A	R	EIMBURSEMENT	A(8)A	C	ONFISCATION
A(8)A	R	EINFORCEMENT	A(8)A	C	ONFORMATION
A(8)A	R	EINSTATEMENT	A(8)A	C	ONSCRIPTION
A(8)A	REPR	ESENTATIVE	A(8)A	C	ONSTITUTION
A(8)A	R	ESPONSIBLE	A(8)A	C	ONSTRUCTION
A(8)A	R	ETROACTIVE	A(8)A	C	ONTINUATION
A(8)A	S	EVENTYFIVE	A(8)A	C	ONVERSATION
A(8)A	T	EMPERATURE	A(8)A	DEM	OBILIZATION
A(8)A		HYDROGRAPHIC	A(8)A	M	OBILIZATION
A(8)A	D	ISCREPANCIES	A(8)A		OBSERVATION
A(8)A		ILLUSTRATION	A(8)A		OBSTRUCTIONS
A(8)A		INAUGURATION	A(8)A	REC	OMMENDATION
A(8)A		INSTALLATIONS	A(8)A	REC	ONSTRUCTION
A(8)A		INTERDICTION	A(8)A	R	OADJUNCTION
A(8)A		INTERRUPTION	A(8)A	QUA	RTERMASTER
A(8)A		INTERVENTION	A(8)A	A	SSESSMENTS
A(8)A		INTRODUCTION	A(8)A	A	SSIGNMENTS
A(8)A(1)A		IRREGULARITIES	A(8)A	IN	STRUCTIONS
A(8)A		IRREGULARITY	A(8)A	INVE	STIGATIONS
A(8)A		MEMORANDUM	A(8)A	OB	STRUCTIONS
A(8)A	ADMI	NISTRATION	A(8)A	REPRE	SENTATIONS
A(8)A	A	NNOUNCEMENT	A(8)A		SCHOOLHOUSE
A(8)A	CA	NCELLATION	A(8)A		SUBMARINES
A(8)A	CO	NCENTRATING	A(8)A		SUSPICIONS
A(8)A	CO	NCILIATION	A(8)A		SUSPICIOUS
A(8)A	CO	NFIRMATION	A(8)A	AN	TIAIRCRAFT
A(8)A	CO	NFISCATION	A(8)A	EN	TANGLEMENT
A(8)A	CO	NFORMATION	A(9)A		AGRICULTURAL
A(8)A	CO	NSCRIPTION	A(9)A		CHRONOLOGICAL
A(8)A	CO	NSTITUTION	A(9)A		CIRCUMSTANCES

Table D-7—*Continued*

A(9)A	RE	CONNAISSANCE
A(9)A		DEMOBILIZED
A(9)A		DISAPPEARED
A(9)A		DISINFECTED
A(9)A	D	ECENTRALIZE
A(9)A	D	ECENTRALIZED
A(9)A		ENTERTAINMENT
A(9)A		ESTABLISHMENT
A(9)A		EXTERMINATE
A(9)A	C	IRCUMSTANTIAL
A(9)A		INVESTIGATION
A(9)A		INVESTIGATIONS
A(9)A	A	NTICIPATION
A(9)A	CO	NCENTRATION
A(9)A	CO	NSIDERATION
A(9)A	E	NTERTAINMENT
A(9)A	IDE	NTIFICATION
A(9)A	I	NAUGURATION
A(9)A	I	NSTALLATIONS
A(9)A	I	NTERDICTION
A(9)A	I	NTERRUPTION
A(9)A	I	NTERVENTION
A(9)A	I	NTRODUCTION
A(9)A		NONCOMBATANT
A(9)A	TRA	NSPORTATION
A(9)A	C	OMMUNICATION
A(9)A	C	ONCENTRATION
A(9)A	C	ONSIDERATION
A(9)A		ORGANIZATION
A(9)A	RE	ORGANIZATION
A(9)A		RANGEFINDER
A(9)A		RECONNOITER
A(9)A		RECONNOITERING
A(9)A	DI	SCREPANCIES
A(9)A	IN	STALLATIONS
A(9)A	IN	STANTANEOUS
A(9)A	MI	SCELLANEOUS
A(9)A	EN	TERTAINMENT
A(9)A	ES	TABLISHMENT
A(9)A		TRANSATLANTIC
A(9)A		TRANSPORTATION
A(9)A		UNSUCCESSFUL
A(10)A		COUNTERATTACK
A(10)A		DEMONSTRATED
A(10)A		DISORGANIZED
A(10)A		DISSEMINATED
A(10)A		INTERPRETATION
A(10)A		IRREGULARITIES
A(10)A	CE	NTRALIZATION
A(10)A	I	NVESTIGATION
A(10)A	I	NVESTIGATIONS
A(10)A		NORTHWESTERN
A(10)A		REVOLUTIONARY
A(10)A		SEARCHLIGHTS
A(10)A		SIMULTANEOUS
A(11)A		CORRESPONDENCE
A(11)A		DECENTRALIZED
A(11)A		DISTINGUISHED
A(11)A	R	ECONNAISSANCE
A(11)A	I	NTERPRETATION
A(12)A		NATURALIZATION
A(12)A		SPECIFICATIONS

APPENDIX E

UTILITY TABLES

Table E-1. Expected number of repetitions, polyalphabetic ciphers.

Number of letters	Expected number of digraphs occurring exactly x times								
	E(2)	E(3)	E(4)	E(5)	E(6)	E(7)	E(8)	E(9)	E(10)
100	6.21	0.298	0.011						
200	21.8	2.12	0.154	0.009					
300	42.5	6.23	0.683	0.060	0.004				
400	65.3	12.8	1.87	0.220	0.022	0.002			
500	88.1	21.6	3.97	0.582	0.071	0.008			
600	110	32.3	7.11	1.25	0.184	0.023	0.003		
700	129	44.3	11.4	2.35	0.403	0.059	0.008	0.001	
800	145	57.1	16.8	3.96	0.777	0.130	0.019	0.003	
900	158	70.1	23.2	6.16	1.36	0.257	0.043	0.006	0.001
1000	169	83.0	30.6	9.03	2.21	0.466	0.085	0.014	0.002

Number of letters	Expected number of trigraphs			Number of letters	Tetragraphs		Number of letters	Pentagraphs
	E(2)	E(3)	E(4)		E(2)	E(3)		E(2)
100	0.269	0.001		100	0.010		100	
200	1.10	0.004		200	0.043		200	0.002
300	2.48	0.014		300	0.096		300	0.004
400	4.40	0.033		400	0.171		400	0.007
500	6.85	0.064		500	0.270		500	0.011
600	9.81	0.111	0.001	600	0.389		600	0.015
700	13.3	0.175	0.002	700	0.530		700	0.021
800	17.3	0.261	0.003	800	0.693		800	0.027
900	21.8	0.371	0.005	900	0.877		900	0.034
1000	26.8	0.505	0.008	1000	1.08	0.001	1000	0.042

Table E-2. Expected values of ϕr, and ϕp.

N	ϕr	ϕp	N	ϕr	ϕp	N	ϕr	ϕp	N	ϕr	ϕp	N	ϕr	ϕp
11	4.23	7.34	**29**	31	54	**47**	83	144	**65**	160	277	**83**	262	454
12	5.08	8.80	**30**	33	58	**48**	87	150	**66**	165	286	**84**	268	465
13	6.00	10.4	**31**	36	62	**49**	90	157	**67**	170	295	**85**	275	476
14	7.00	12.1	**32**	38	66	**50**	94	163	**68**	175	304	**86**	281	488
15	8.08	14.0	**33**	41	70	**51**	98	170	**69**	180	313	**87**	288	499
16	9.23	16.0	**34**	43	75	**52**	102	177	**70**	186	322	**88**	294	511
17	10.5	18.1	**35**	46	79	**53**	106	184	**71**	191	331	**89**	301	522
18	11.8	20.4	**36**	48	84	**54**	110	191	**72**	197	341	**90**	308	534
19	13.2	22.8	**37**	51	89	**55**	114	198	**73**	202	351	**91**	315	546
20	14.6	25.3	**38**	54	94	**56**	118	205	**74**	208	360	**92**	322	558
21	16.2	28.5	**39**	57	99	**57**	123	213	**75**	213	370	**93**	329	571
22	17.8	30.8	**40**	60	104	**58**	127	221	**76**	219	380	**94**	336	583
23	19.5	33.8	**41**	63	109	**59**	132	228	**77**	225	390	**95**	343	596
24	21.2	36.8	**42**	66	115	**60**	136	236	**78**	231	401	**96**	351	608
25	23.1	40.0	**43**	69	120	**61**	141	244	**79**	237	411	**97**	358	621
26	25.0	43.4	**44**	73	126	**62**	145	252	**80**	243	422	**98**	366	634
27	27.0	46.8	**45**	76	132	**63**	150	261	**81**	249	432	**99**	373	647
28	29.1	50.4	**46**	80	138	**64**	155	269	**82**	255	443	**100**	381	660

Table E-3. Factor table.

NUMBERS 1—400

	1	Prime	**45**	3 5 9 15	**89**	Prime
	2	Prime	**46**	2 23	**90**	2 3 5 6 9 10 15 18 30 45
	3	Prime	**47**	Prime	**91**	7 13
	4	2	**48**	2 3 4 6 8 12 16 24	**92**	2 4 23 46
	5	Prime	**49**	7	**93**	3 31
	6	2 3	**50**	2 5 10 25	**94**	2 47
	7	Prime	**51**	3 17	**95**	5 19
	8	2 4	**52**	2 4 13 26	**96**	2 3 4 6 8 12 16 24 32 48
	9	3	**53**	Prime	**97**	Prime
	10	2 5	**54**	2 3 6 9 18 27	**98**	2 7 14 49
	11	Prime	**55**	5 11	**99**	3 9 11 33
	12	2 3 4 6	**56**	2 4 7 8 14 28	**100**	2 4 5 10 20 25 50
	13	Prime	**57**	3 19	**101**	Prime
	14	2 7	**58**	2 29	**102**	2 3 6 17 34 51
	15	3 5	**59**	Prime	**103**	Prime
	16	2 4 8	**60**	2 3 4 5 6 10 12 15 20 30	**104**	2 4 8 13 26 52
	17	Prime	**61**	Prime	**105**	3 5 7 15 21 35
	18	2 3 6 9	**62**	2 31	**106**	2 53
	19	Prime	**63**	3 7 9 21	**107**	Prime
	20	2 4 5 10	**64**	2 4 8 16 32	**108**	2 3 4 6 9 12 18 27 36 54
	21	3 7	**65**	5 13	**109**	Prime
	22	2 11	**66**	2 3 6 11 22 33	**110**	2 5 10 11 22 55
	23	Prime	**67**	Prime	**111**	3 37
	24	2 3 4 6 8 12	**68**	2 4 17 34	**112**	2 4 7 8 14 16 28 56
	25	5	**69**	3 23	**113**	Prime
	26	2 13	**70**	2 5 7 10 14 35	**114**	2 3 6 19 38 57
	27	3 9	**71**	Prime	**115**	5 23
	28	2 4 7 14	**72**	2 3 4 6 8 9 12 18 24 36	**116**	2 4 29 58
	29	Prime	**73**	Prime	**117**	3 9 13 39
	30	2 3 5 6 10 15	**74**	2 37	**118**	2 59
	31	Prime	**75**	3 5 15 25	**119**	7 17
	32	2 4 8 16	**76**	2 4 19 38	**120**	2 3 4 5 6 8 10 12 15 20 24 30 40 60
	33	3 11	**77**	7 11	**121**	11
	34	2 17	**78**	2 3 6 13 26 39	**122**	2 61
	35	5 7	**79**	Prime	**123**	3 41
	36	2 3 4 6 9 12 18	**80**	2 4 5 8 10 16 20 40	**124**	2 4 31 62
	37	Prime	**81**	3 9 27	**125**	5 25
	38	2 19	**82**	2 41	**126**	2 3 6 7 9 14 18 21 42 63
	39	3 13	**83**	Prime	**127**	Prime
	40	2 4 5 8 10 20	**84**	2 3 4 6 7 12 14 21 28 42	**128**	2 4 8 16 32 64
	41	Prime	**85**	5 17	**129**	3 43
	42	2 3 6 7 14 21	**86**	2 43	**130**	2 5 10 13 26 65
	43	Prime	**87**	3 29	**131**	Prime
	44	2 4 11 22	**88**	2 4 8 11 22 44		

Table E-3—*Continued*

132	2 3 4 6 11 12 22 33 44 66
133	7 19
134	2 67
135	3 5 9 15 27 45
136	2 4 8 17 34 68
137	Prime
138	2 3 6 23 46 69
139	Prime
140	2 4 5 7 10 14 20 28 35 70
141	3 47
142	2 71
143	11 13
144	2 3 4 6 8 9 12 16 18 24 36 48 72
145	5 29
146	2 73
147	3 7 21 49
148	2 4 37 74
149	Prime
150	2 3 5 6 10 15 25 30 50 75
151	Prime
152	2 4 8 19 38 76
153	3 9 17 51
154	2 7 11 14 22 77
155	5 31
156	2 3 4 6 12 13 26 39 52 78
157	Prime
158	2 79
159	3 53
160	2 4 5 8 10 16 20 32 40 80
161	7 23
162	2 3 6 9 18 27 54 81
163	Prime
164	2 4 41 82
165	3 5 11 15 33 55
166	2 83
167	Prime
168	2 3 4 6 7 8 12 14 21 24 28 42 56 84
169	13
170	2 5 10 17 34 85
171	3 9 19 57
172	2 4 43 86
173	Prime
174	2 3 6 29 58 87
175	5 7 25 35
176	2 4 8 11 16 22 44 88
177	3 59
178	2 89
179	Prime
180	2 3 4 5 6 9 10 12 15 18 20 30 36 45 60 90
181	Prime
182	2 7 13 14 26 91
183	3 61
184	2 4 8 23 46 92
185	5 37
186	2 3 6 31 62 93
187	11 17
188	2 4 47 94
189	3 7 9 21 27 63
190	2 5 10 19 38 95
191	Prime
192	2 3 4 6 8 12 16 24 32 48 64 96
193	Prime
194	2 97
195	3 5 13 15 39 65
196	2 4 7 14 28 49 98
197	Prime
198	2 3 6 9 11 18 22 33 66 99
199	Prime
200	2 4 5 8 10 20 25 40 50 100
201	3 67
202	2 101
203	7 29
204	2 3 4 6 12 17 34 51 68 102
205	5 41
206	2 103
207	3 9 23 69
208	2 4 8 13 16 26 52 104
209	11 19
210	2 3 5 6 7 10 14 15 21 30 35 42 70 105
211	Prime
212	2 4 53 106
213	3 71
214	2 107
215	5 43
216	2 3 4 6 8 9 12 18 24 27 36 54 72 108
217	7 31
218	2 109
219	3 73
220	2 4 5 10 11 20 22 44 55 110
221	13 17
222	2 3 6 37 74 111
223	Prime
224	2 4 7 8 14 16 28 32 56 112
225	3 5 9 15 25 45 75
226	2 113
227	Prime
228	2 3 4 6 12 19 38 57 76 114
229	Prime
230	2 5 10 23 46 115
231	3 7 11 21 33 77
232	2 4 8 29 58 116
233	Prime
234	2 3 6 9 13 18 26 39 78 117
235	5 47
236	2 4 59 118
237	3 79
238	2 7 14 17 34 119
239	Prime
240	2 3 4 5 6 8 10 12 15 16 20 24 30 40 48 60 80 120
241	Prime
242	2 11 22 121
243	3 9 27 81
244	2 4 61 122
245	5 7 35 49
246	2 3 6 41 82 123
247	13 19
248	2 4 8 31 62 124
249	3 83
250	2 5 10 25 50 125
251	Prime
252	2 3 4 6 7 9 12 14 18 21 28 36 42 63 84 126
253	11 23
254	2 127
255	3 5 15 17 51 85

Table E-3—*Continued*

256	2 4 8 16 32 64 128
257	Prime
258	2 3 6 43 86 129
259	7 37
260	2 4 5 10 13 20 26 52 65 130
261	3 9 29 87
262	2 131
263	Prime
264	2 3 4 6 8 11 12 22 24 33 44 66 88 132
265	5 53
266	2 7 14 19 38 133
267	3 89
268	2 4 67 134
269	Prime
270	2 3 5 6 9 10 15 18 27 30 45 54 90 135
271	Prime
272	2 4 8 16 17 34 68 136
273	3 7 13 21 39 91
274	2 137
275	5 11 25 55
276	2 3 4 6 12 23 46 69 92 138
277	Prime
278	2 139
279	3 9 31 93
280	2 4 5 7 8 10 14 20 28 35 40 56 70 140
281	Prime
282	2 3 6 47 94 141
283	Prime
284	2 4 71 142
285	3 5 15 19 57 95
286	2 11 13 22 26 143
287	7 41
288	2 3 4 6 8 9 12 16 18 24 32 36 48 72 96 144
289	17
290	2 5 10 29 58 145
291	3 97
292	2 4 73 146
293	Prime
294	2 3 6 7 14 21 42 49 98 147
295	5 59
296	2 4 8 37 74 148
297	3 9 11 27 33 99
298	2 149
299	13 23
300	2 3 4 5 6 10 12 15 20 25 30 50 60 75 100 150
301	7 43
302	2 151
303	3 101
304	2 4 8 16 19 38 76 152
305	5 61
306	2 3 6 9 17 18 34 51 102 153
307	Prime
308	2 4 7 11 14 22 28 44 77 154
309	3 103
310	2 5 10 31 62 155
311	Prime
312	2 3 4 6 8 12 13 24 26 39 52 78 104 156
313	Prime
314	2 157
315	3 5 7 9 15 21 35 45 63 105
316	2 4 79 158
317	Prime
318	2 3 6 53 106 159
319	11 29
320	2 4 5 8 10 16 20 32 40 64 80 160
321	3 107
322	2 7 14 23 46 161
323	17 19
324	2 3 4 6 9 12 18 27 36 54 81 108 162
325	5 13 25 65
326	2 163
327	3 109
328	2 4 8 41 82 164
329	7 47
330	2 3 5 6 10 11 15 22 30 33 55 66 110 165
331	Prime
332	2 4 83 166
333	3 9 37 111
334	2 167
335	5 67
336	2 3 4 6 7 8 12 14 16 21 24 28 42 48 56 84 112 168
337	Prime
338	2 13 26 169
339	3 113
340	2 4 5 10 17 20 34 68 85 170
341	11 31
342	2 3 6 9 18 19 38 57 114 171
343	7 49
344	2 4 8 43 86 172
345	3 5 15 23 69 115
346	2 173
347	Prime
348	2 3 4 6 12 29 58 87 116 174
349	Prime
350	2 5 7 10 14 25 35 50 70 175
351	3 9 13 27 39 117
352	2 4 8 11 16 22 32 44 88 176
353	Prime
354	2 3 6 59 118 177
355	5 71
356	2 4 89 178
357	3 7 17 21 51 119
358	2 179
359	Prime
360	2 3 4 5 6 8 9 10 12 15 18 20 24 30 36 40 45 60 72 90 120 180
361	19
362	2 181
363	3 11 33 121
364	2 4 7 13 14 26 28 52 91 182
365	5 73
366	2 3 6 61 122 183
367	Prime
368	2 4 8 16 23 46 92 184
369	3 9 41 123
370	2 5 10 37 74 185
371	7 53
372	2 3 4 6 12 31 62 93 124 186
373	Prime
374	2 11 17 22 34 187
375	3 5 15 25 75 125

Table E-3—*Continued*

376	2 4 8 47 94 188
377	13 29
378	2 3 6 7 9 14 18 21 27 42 54 63 126 189
379	Prime
380	2 4 5 10 19 20 38 76 95 190
381	3 127
382	2 191
383	Prime
384	2 3 4 6 8 12 16 24 32 48 64 96 128 192
385	5 7 11 35 55 77
386	2 193
387	3 9 43 129
388	2 4 97 194
389	Prime
390	2 3 5 6 10 13 15 26 30 39 65 78 130 195
391	17 23
392	2 4 7 8 14 28 49 56 98 196
393	3 131
394	2 197
395	5 79
396	2 3 4 6 9 11 12 18 22 33 36 44 66 99 132 198
397	Prime
398	2 199
399	3 7 19 21 57 133
400	2 4 5 8 10 16 20 25 40 50 80 100 200

Table E-4. Table of Primes up to 2000.

1	139	337	557	769	1013	1249	1493	1741
2	149	347	563	773	1019	1259	1499	1747
3	151	349	569	787	1021	1277	1511	1753
5	157	353	571	797	1031	1279	1523	1759
7	163	359	577	809	1033	1283	1531	1777
11	167	367	587	811	1039	1289	1543	1783
13	173	373	593	821	1049	1291	1549	1787
17	179	379	599	823	1051	1297	1553	1789
19	181	383	601	827	1061	1301	1559	1801
23	191	389	607	829	1063	1303	1567	1811
29	193	397	613	839	1069	1307	1571	1823
31	197	401	617	853	1087	1319	1579	1831
37	199	409	619	857	1091	1321	1583	1847
41	211	419	631	859	1093	1327	1597	1861
43	223	421	641	863	1097	1361	1601	1867
47	227	431	643	877	1103	1367	1607	1871
53	229	433	647	881	1109	1373	1609	1873
59	233	439	653	883	1117	1381	1613	1877
61	239	443	659	887	1123	1399	1619	1879
67	241	449	661	907	1129	1409	1621	1889
71	251	457	673	911	1151	1423	1627	1901
73	257	461	677	919	1153	1427	1637	1907
79	263	463	683	929	1163	1429	1657	1913
83	269	467	691	937	1171	1433	1663	1931
89	271	479	701	941	1181	1439	1667	1933
97	277	487	709	947	1187	1447	1669	1949
101	281	491	719	953	1193	1451	1693	1951
103	283	499	727	967	1201	1453	1697	1973
107	293	503	733	971	1213	1459	1699	1979
109	307	509	739	977	1217	1471	1709	1987
113	311	521	743	983	1223	1481	1721	1993
127	313	523	751	991	1229	1483	1723	1997
131	317	541	757	997	1231	1487	1733	1999
137	331	547	761	1009	1237	1489		

APPENDIX F

CRYPTANALYSIS SUPPORT PROGRAM

F-1. Program Support

This program supports the development of FM 34-40-2, Basic Cryptanalysis. It gives the capability to encipher and decipher messages in monoalphabetic and polyalphabetic substitution systems, produce a variety of statistical data about the encrypted messages, and print the results or save them to disk. Because of its limited purpose, the program does not support on-screen analysis. The printed results can be used off-line to aid in analysis, however. The program should be particularly useful in preparing examples and exercises for training cryptanalytic techniques.

F-2. On-screen Analysis

The logical structure is present in the program to support on-screen analysis, if desired. The coding that now sends results to disk or printer can be modified to display on screen as well. Lines 6060 through 6780 provide the basis for this. This code together with the alphabet entry subroutines in lines 3920 through 5760 can be used to enter partial trial recoveries and see the results for both monoalphabetic and polyalphabetic systems.

F-3. Program Format

The listing has been specially formatted to make it easy to follow the program logic. Each statement in multiple statement numbered lines has been printed on a separate line with each follow-on statement indicated by the statement separator (colon) at the beginning of the line. FOR-NEXT commands have been indented to show the level and structure of each. Similarly, the parts of IF...THEN...ELSE statements have been printed on separate lines and then indented to show their structure clearly. If the program is typed in by hand, the statements in a single numbered line should be entered continuously, not on separate lines in most versions of BASIC. Indentation of FOR-NEXT structures can be preserved, if desired, but not for IF...THEN...ELSE statements.

```
100   ' CRYPTANALYSIS SUPPORT PROGRAM
120   ' Version 1.0
140   ' 4 October 1988
160   '
180   ' Developed in support of FM 34-40-2, Basic Cryptanalysis to provide
200   ' accurate encryption, decryption, frequency counts, and statistics for use
220   ' in the manual. It can be used for other applications.
240   '
260   ' The program was written in GW-BASIC.
280   ' It is readily adaptable to any computers that run
300   ' GW-BASIC. It can easily be converted to run in other BASIC languages.
320   '
340   ' As written, the program will print on a dot matrix printer with the name
360   ' PRN1 that uses standard Epson control codes. If necessary, change the
380   ' values in the *** Printer Setup *** section for the particular printer
400   ' to be used.
420   '
440   ' *** Printer Setup ***
460   PRINTER$=“PRN1”
480   FORMFEED$=CHR$(12)
500   CRLF$=CHR$(13)+CHR$(10) ' (not used in 1.0)
520   CONDENSED$=CHR$(15) ' (not used in 1.0)
540   DC2$=CHR$(18) ' Cancels condensed mode (not used in 1.0)
560   ELITE$=CHR$(27)+“M” ' (not used in 1.0)
580   PICA$=CHR$(27)+“P” ' (not used in 1.0)
600   '
620   ' *** Initialize Variables ***
640   DIM PTEXTD$(25), PTEXTI$(25), CTEXTD$(25), CTEXTI$(25)
660   ' Plain and ciphertext may be stored in two forms: display and internal.
680   ' Display forms (PTEXTD$() and CTEXTD()) are as typed with spaces.
700   ' Internal forms (PTEXTI$() and CTEXTI$()) have spaces, and nonliteral
720   ' characters stripped away. All frequency counts and ICs are performed on
740   ' CTEXTI$() strings. Up to 25 lines of text are allowed, as written.
760   ' Additional lines of text may be used if all uses of “25” are increased
780   ' in the DIM statement in line 640.
800   DIM MFREQ(26), PFREQ(20,27), DIFREQ(26,26), PHIMONO,PHIPERI(20), PHIDIG,
      PMIXFREQ(20,27), SET 1(26), SET 2(27), MATCH (27), PERPHISUM(20), PERTOTLTR(20)
820   ' Sets up monographic, periodic, and digraphic frequency, IC tables. Up
840   ' to 20 alphabets are allowed for periodic frequencies, as written. The
860   ' number of alphabets can be increased by increasing all uses of “20” in
880   ' the DIM statements in line 800.
900   DIM PCOMP$, CCOMP$(200) ' Variables for plain and cipher components with up
920   ' to 200 cipher component sequences for long running key aperiodics. The
940   ' length of the key may be increased by increasing the “200” in the DIM
960   ' statement in line 900.
1000  '
1020  KEY OFF ' Turns off prompts on bottom of screen.
1040  '
```

```
1160  ' *** Main Menu ***
1180  CLS
1200  PRINT "          CRYPTANALYSIS SUPPORT PROGRAM"
1220  PRINT
      :PRINT
1240  PRINT "      1. Enter text ";STATUS$(1)
1260  PRINT "      2. Encipher text ";STATUS$(2)
1280  PRINT "      3. Decipher text ";STATUS$(3)
1300  PRINT "      4. Print text ";STATUS$(4)
1320  PRINT "      5. Save text to disk ";STATUS$(5)
1340  PRINT "      6. Calculate frequency counts, ICs ";STATUS$(6)
1360  PRINT "      7. Print frequency counts, ICs ";STATUS$(7)
1380  PRINT "      8. Save frequency counts, ICs to disk ";STATUS$(8)
1400  PRINT "      9. Find repeats ";STATUS$(9)
1420  PRINT "     10. Quit"
1440  PRINT
      :PRINT
1460  '
1480  ' *** Main Menu Control ***
1500  INPUT  " Enter your choice: ",SELECTION
1520  ON SELECTION GOSUB 1600,3000,3480,6080,6380,6840,8600,9960,10240,10980
1540  GOTO 1180
1560  '
1580  ' *** Text Entry Subroutine ***
1600  CLS
1620  PRINT "          TEXT ENTRY MENU"
1640  PRINT
      :PRINT
      :PRINT
1660  PRINT "     1. Enter plaintext from disk
1680  PRINT "     2. Enter ciphertext from disk
1700  PRINT "     3. Enter plaintext from keyboard
1720  PRINT "     4. Enter ciphertext from keyboard
1740  PRINT "     5. Return to Main Menu
1760  PRINT
      :PRINT
1780  INPUT “Enter your choice:   ”, CHOICE
1800  ON CHOICE GOTO 1860,2040,2220,2440,2600
1820  '
1840  ' *** Plaintext Disk Entry ***
1860  INPUT “Enter input filename, for example, A:SAMPLE.TXT    ”,INFILE$
1880  OPEN INFILE$ FOR INPUT AS #1
1900  NRLINES=0
1920  NRLINES=NRLINES+1
1940  INPUT #1, PTEXTD$(NRLINES)
1960  IF EOF(1)
        THEN STATUS$(1)="     (PLAINTEXT ENTERED)"
       :CLOSE #1
       :RETURN
```

```
1980  GOTO 1920
2000  '
2020  ' *** Ciphertext Disk Entry ***
2040  INPUT "Enter input filename, for example, A:SAMPLE.TXT   ",INFILE$
2060  OPEN INFILE$ FOR INPUT AS #1
2080  NRLINES=0
2100  NRLINES=NRLINES+1
2120  INPUT #1,CTEXTD$(NRLINES)
2140  IF EOF(1)
        THEN CLOSE #1
       :STATUS$="      (CIPHERTEXT ENTERED)"
       :GOTO 2660 ' Branches to internal text preparation.
2160  GOTO 2100
2180  '
2200  ' *** Plaintext Keyboard Entry ***
2220  PRINT "Type a line of text. Use lower case letters only."
2240  PRINT "Use no commas in the text. When you are through,"
2260  PRINT "type END on a new line."
2280  NRLINES=0
2300  LINE INPUT T$
2320  IF T$="END" OR T$="end"
        THEN STATUS$(1)="      (PLAINTEXT ENTERED)"
       :RETURN
2340  NRLINES=NRLINES+1
2360  PTEXTD$(NRLINES)=T$
2380  GOTO 2300
2400  '
2420  ' *** Ciphertext Keyboard Entry ***
2440  PRINT "Type a line of text. Use CAPITAL letters only."
2460  PRINT "When you are through, type END on a new line."
2480  NRLINES=0
2500  INPUT T$
2520  IF T$="END" OR T$="end"
        THEN STATUS$(1)="      (CIPHERTEXT ENTERED)"
       :GOTO 2660
2540  NRLINES=NRLINES+1
2560  CTEXTD$(NRLINES)=T$
2580  GOTO 2500
2600  RETURN
2620  '
2640  ' *** Preps Ciphertext in Internal Format ***
2660  FOR TEXTLINE=1 TO NRLINES
2680        T$=CTEXTD$(TEXTLINE)
2700        POSN=0
2720        POSN=POSN+1
           :IF POSN>LEN(T$)
              THEN 2800
2740        C$=MID$(T$,POSN,1)
```

```
2760        IF (ASC(C$)<65 OR ASC(C$)>90) AND C$<>“.”
              THEN GOSUB 2900
2780        GOTO 2720
2800        CTEXTI$(TEXTLINE)=T$
2820   NEXT TEXTLINE
2840   RETURN
2860   '
2880   ' *** Subroutine to Strip Nonliteral Characters From Ciphertext ***
2900   T$=MID$(T$,1,POSN-1)+MID$(T$,POSN+1,LEN(T$)-POSN)
2920   POSN=POSN-1
2940   RETURN
2960   '
2980   ' *** Encipherment Subroutine ***
3000   GOSUB 3940
3020   CYCLEPOS=0
3040   FOR LNE=1 TO NRLINES
          :CTEXTD$(LNE)=”
          :KTEXTD$(LNE)=”
      :NEXT LNE
3060   FOR LNE=1 TO NRLINES
3080     FOR CHARPOS=1 TO LEN(PTEXTD$(LNE))
3100       PCHAR$=MID$(PTEXTD$(LNE),CHARPOS,1)
3120       IF PCHAR$=" "
             THEN CCHAR$=" "
             :KCHAR$=" "
             :GOTO 3320
3140       CYCLEPOS=CYCLEPOS+1
          :IF CYCLEPOS>PERIOD
             THEN CYCLEPOS=1
3160       KCHAR$=MID$(REPEATKEY$,CYCLEPOS,1)
3180       IF ASC (PCHAR$) >64 AND ASC(PCHAR$)<91
               THEN PCHAR$=CHR$(ASC(PCHAR$)+32)
3200       IF ASC(PCHAR$)<97 OR ASC(PCHAR$)>122
               THEN PCHAR$=“.”
3220       IF PCHAR$=“.”
               THEN CCHAR$=“.”
              :GOTO 3320
3240       FOR ALPHCHAR=1 TO 26
3260         IF PCHAR$=MID$(PCOMP$,ALPHCHAR,1)
               THEN CCHAR$=MID$(CCOMP$(CYCLEPOS),ALPHCHAR,1)
              :GOTO 3320
3280       NEXT ALPHCHAR
3300       CCHAR$=“.”
3320       CTEXTD$(LNE)=CTEXTD$(LNE)+CCHAR$
         :KTEXTD$(LNE)=KTEXTD$(LNE)+KCHAR$
3340     NEXT CHARPOS
3360   NEXT LNE
3380   GOSUB 2660
```

```
3400  STATUS$(2)="     (ENCIPHEREMENT COMPLETED)"
3420  RETURN
3440  '
3460  ' *** Decipherment Subroutine ***
3480  GOSUB 3940
3500  CYCLEPOS=0
3520  FOR LNE=1 TO NRLINES
        :PTEXTD$(LNE)=" ":
      NEXT LNE
3540  FOR LNE=1 TO NRLINES
3560    FOR CHARPOS=1 TO LEN(CTEXTD$(LNE))
3580      CCHAR$=MID$(CTEXTD$(LNE),CHARPOS,1)
3600      IF CCHAR$="   "
            THEN PCHAR$="   "
            :GOTO 3780
3620      CYCLEPOS=CYCLEPOS+1:
          IF CYCLEPOS>PERIOD
            THEN CYCLEPOS=1
3640      IF ASC(CCHAR$)>96 AND ASC(CCHAR$)<123
            THEN CCHAR$=CHR$(ASC(CCHAR$)-32)
3660      IF ASC(CCHAR$)<65 OR ASC(CCHAR$)>96
            THEN CCHAR$="."
3680      IF CCHAR$="."
            THEN PCHAR$="."
            :GOTO 3780
3700      FOR ALPHCHAR=1 TO 26
3720        IF CCHAR$=MID$(CCOMP$(CYCLEPOS),ALPHCHAR,1)
              THEN PCHAR$=MID$(PCOMP$,ALPHCHAR,1)
              :GOTO 3780
3740      NEXT ALPHCHAR
3760      PCHAR$="."
3780      PTEXTD$(LNE)=PTEXTD$(LNE)+PCHAR$
3800    NEXT CHARPOS
3820  NEXT LNE
3840  GOSUB 2660
3860  STATUS$(3)="     (DECIPHERMENT COMPLETED)"
3880  RETURN
3900  '
3920  ' *** Alphabet Entry Subroutine ***
3940  PCOMP$="abcdefghijklmnopqrstuvwxyz"
3960  CCOMPO$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
3980  RKEY$="AAAAAAAAAAAAAAAAAAAA"
4000  PERIOD=1
4020  CLS
4040  PRINT "Select type of system:"
     :PRINT
4060  PRINT "     1. Monoalphabetic uniliteral"
4080  PRINT "     2. Periodic polyalphabetic"
4100  PRINT "     3. Aperiodic polyalphabetic"
```

```
4120  PRINT
     :PRINT
4140  INPUT “Enter your choice:   ”, SELECTION
4160  ON SELECTION GOSUB 4240,4860,6020
4180  RETURN
4200  '
4220  ' *** Monoalphabetic Alphabet Entry Subroutine ***
4240  CLS:PLFAG=0:CIFLAG=0:DONEFLAG=0
4260  PRINT TAB(5);“Present alphabet is--”:PRINT
4280  PRINT TAB(10);“P: ”;
     :FOR N=1 TO 26
        :PRINT MID$(PCOMP$,N,1);“   ”;
     :NEXT N
4300  PRINT TAB(10);“C:   ”;
     :FOR N=1 TO 26
       :PRINT MID$(CCOMPO$,N,1);“   ”;
     :NEXT N
4320  PRINT
     :PRINT
4340  PRINT TAB(20);“1.  Change plain component”
4360  PRINT TAB(20);“2.  Change cipher component”
4380  PRINT TAB(20);“3.  Change specific key”
4400  PRINT TAB(20);“4.  Accept alphabet as shown”
4420  PRINT
     :PRINT TAB(18);“Enter your choice:   ”;
4440  INPUT CHOICE
4460  ON CHOICE GOSUB 4520,4580,4640,4500
4480  IF DONEFLAG=1
        THEN CCOMP$(1)=CCOMPO$
       :RETURN
      ELSE GOTO 4240 ' Exit if done
4500  DONEFLAG=1
     :RETURN
4520  ROW=3
     :COLUMN=11
     :PLFAG=1
     :GOSUB 5640
4540  PCOMP$=COMP$
4560  RETURN
4580  ROW=4
     :COLUMN=11
     :CIFLAG=1
     :GOSUB 5640
4600  CCOMPO$=COMP$

4620  RETURN
4640  LOCATE 11,10:X=SCREEN (3,13):
      PRINT “Type the specific key: ”;CHR$(X-32);
      “      of plaintext = ? of ciphertext.”
4660  LOCATE 11,50,1
```

```
4680  X$=INKEY$
     :IF X$=" "
        THEN 4680
4700  IF ASC(X$)>96 AND ASC(X$)<123
         THEN X$=CHR$(ASC(X$)-32)
4720  FOR N=1 TO 26:
         IF X$=MID$(CCOMPO$,N,1)
            THEN 4780
4740  NEXT N
4760  PRINT “CHARACTER NOT FOUND IN CIPHER COMPONENT”
     :GOTO 4640
4780  TCOMP$=RIGHT$(CCOMPO$,27-N)+LEFT$(CCOMPO$,N-1)
     :CCOMPO$=TCOMP$
4800  RETURN
4820  '
4840  '     *** Periodic and Aperiodic Alphabet Entry Subroutine ***
4860  CLS
     :DONEFLAG=0
     :PLFLAG=0
     :CIFLAG=0
4880  PRINT TAB(5);“Plain component is--”
4900  PRINT TAB(10);“P:   ”;
     :FOR N=1 TO 26
        :PRINT MID$(PCOMP$,N,1);“   ”;
     :NEXT N
     :PRINT
4920  PRINT TAB(5);“Cipher component is--”
4940  PRINT TAB(10);“C:   ”;
     :FOR N=1 TO 26
        :PRINT MID$(CCOMPO$,N,1);“   ”;
     :NEXT N
     :PRINT
     :PRINT
4960  IF AFLAG=0
         THEN PRINT TAB(5);“Length of period is:   ”;PERIOD
      ELSE PRINT TAB(5);“Length of key is:   ”;PERIOD
4980  X=SCREEN(2,13)
5000  IF AFLAG=0
         THEN REPEATKEY$=LEFT$(RKEY$,PERIOD)
5020  IF AFLAG=0
         THEN PRINT TAB(5);“Repeating key is   ”;CHR$(X-32);” of
         plaintext = ”;REPEATKEY$
        :PRINT
     :ELSE PRINT TAB (5);“Long running key is:   ”;REPEATKEY$
     :PRINT
5040  PRINT
     :PRINT
5060  PRINT TAB(20);“1. Change plain component”
5080  PRINT TAB(20);“2. Change cipher component”
```

```
5100  IF AFLAG=0
         THEN PRINT TAB (20);"3. Change repeating key"
      ELSE PRINT TAB(20);"3. Generate long running key"
5120  IF AFLAG=0
         THEN PRINT TAB(20);"4. Show complete matrix"
      ELSE PRINT TAB(20);"4. Accept alphabets"
5140  PRINT
     :PRINT TAB(18);"Enter your choice:   ";
5160  INPUT CHOICE
5180  ON CHOICE GOSUB 5220,5260,5300,5420
5200  IF DONEFLAG=1
         THEN RETURN
      ELSE GOTO 4860
5220  ROW=2
     :COLUMN=11
     :PLFLAG=1
     :GOSUB 5640
5240  PCOMP$=COMP$
     :RETURN
5260  ROW=4
     :COLUMN=11
     :CIFLAG=1
     :CMIXFLAG=1
     :GOSUB 5640
5280  CCOMPO$=COMP$
     :RETURN
5300  IF AFLAG=1
         THEN 5820
      ELSE LOCATE 7,39
     :INPUT RKEY$
5320  PERIOD=LEN(RKEY$)
5340  FOR N=1 TO PERIOD:
         FOR P=1 TO 26
            :IF MID$(RKEY$,N,1)=MID$(CCOMPO$,P,1)
               THEN 5380
5360     NEXT P
5380     CCOMP$(N)=RIGHT$(CCOMPO$,27-P)+LEFT$(CCOMPO$,P-1)
     :NEXT N
5400  RETURN
5420  CLS
     :IF AFLAG=1
        THEN 4500
5440  PRINT TAB(9);"P:   ";
     :FOR N=1 TO 26
        :PRINT MID$(PCOMP$,N,1);"   ";
     :NEXT N
     :PRINT
     :PRINT TAB(13);"---------------------------------------------------"
5460  FOR P=1 TO PERIOD
```

```
5480     PRINT TAB(9);“C”;CHR$(48+P);“:  ”;
        :FOR N=1 TO 26
          :PRINT MID$(CCOMP$(P),N,1);“   ”;
        :NEXT N
        :PRINT

5500  NEXT P
5520  PRINT TAB(20);“1.  Change matrix”
5540  PRINT TAB(20);“2.  Accept matrix”
5560  INPUT“                Enter your choice:   ”;CHOICE
5580  ON CHOICE GOTO 4860,4500
5600  '
5620  ' *** Reads in Edited Plain or Cipher Component From Screen ***
5640  LOCATE ROW, COLUMN
     :INPUT DUMMY$   ' DUMMY$ is not used as text is read from screen
5660  COMP$=" "
5680  FOR N=13 TO 63 STEP 2
        :X=SCREEN(ROW,N)
        :COMP$=COMP$+CHR$(X)
5700     IF PLFLAG=1 AND (X<96 OR X>122) AND X<>46
           THEN BEEP
          :GOTO 5640
5720     IF CIFLAG=1 AND (X<65 OR X>90)
           THEN BEEP
       :GOTO 5640
5740  NEXT N
5760  RETURN
5780  '
5800  ' *** Aperiodic Long-Running Key Generation Subroutine ***
5820  CLS
5840  RANDOMIZE
5860  INPUT “Enter the number of alphabets (up to 200):   ”;PERIOD
5880  FOR N=1 TO PERIOD
5900  LRK$=LRK$+CHR$(INT(RND*26)+65)
5920  NEXT N
5940  REPEATKEY$=LRK$
     :RKEY$=LRK$
5960  GOTO 5340
5980  '
6000  ' *** Sets Flag Indicating Long-Running Key System ***
6020  AFLAG=1
     :GOTO 4806
6040  '
6060  ' *** Text Print Subroutine ***
6080  CLS
6100  PRINT “IS PRINTER READY (Y/N)?   ”
6120  X$=INKEY$
     :IF X$=" "
        THEN 6120
```

```
6140  IF X$=“N” OR X$=“n”
        THEN RETURN
6160  OUTFILE$=PRINTER$
6180  GOSUB 6440
6200  PRINT #1,FORMFEED$;FORMFEED$
6220  CLOSE #1
6240  STATUS$(4)=“      (TEXT PRINTED)”
6260  IF PRINTER$<>“CON”
        THEN 6320
6280  PRINT “PRESS ANY KEY TO CONTINUE”
6300  GO$=INKEY$
     :IF GO$=″ ″
       THEN 6300
6320  RETURN
6340  '
6360  ' *** Text Save to Disk Subroutine ***
6380  CLS
6400  PRINT “Enter complete disk filename for the save text, for example,”
6420  INPUT “A:MYSAVE.TXT   ”;OUTFILE$
6440  OPEN OUTFILE$ FOR OUTPUT AS #1
6460  TEXTCOUNT=0
6480  FOR N=1 TO NRLINES
6500    PRINT #1,PTEXTD$(N)
6520    PRINT #1,CTEXTD$(N)
6540    PRINT #1,KTEXTD$(N)
6560    TEXTCOUNT=TEXTCOUNT+LEN(CTEXTI$(N))
6580    PRINT +1,
6600  NEXT N
6620  IF PERIOD>20
        THEN 6720
6640  PRINT#1,PCOMP$
6660  FOR N=1 TO PERIOD
6680    PRINT #1,CCOMP$(N)
6700  NEXT N
6720  IF OUTFILE$=PRINTER$ OR FILEFLAG=1 THEN RETURN
6740  CLOSE #1
6760  IF OUTFILE$<>PRINTER$ THEN STATUS$(5)=“      (TEXT SAVED)”
6780  RETURN
6800  '
6820  ' *** Frequency Count, IC Subroutine ***
6840  CLS
6860  PRINT “Select the routine you want to run:”
6880  PRINT:PRINT
6900  PRINT ″      1. Monographic frequencies and ICs″+STAT$(1)
6920  PRINT ″      2. Digraphic frequencies and ICs″+STAT$(2)
6940  PRINT ″      3. Periodic frequencies and ICs″+STAT$(3)
6960  PRINT ″      4. Chi test″+STAT$(4)
6980  PRINT ″      5. RETURN TO MAIN MENU″
7000  INPUT ″          Your choice: ″,CHOICE$
```

```
7020  IF ASC (CHOICE$)<49 OR ASC(CHOICE$)>53
        THEN 7000
7040  ON (ASC(CHOICE$)-48) GOSUB 7120,7440,7900,11120, 1180
7060  GOTO 6840
7080  '

7100  ' *** Monographic Frequency and IC Subroutine ***
7120  FOR LINE=1 TO NRLINES
7140    FOR CHARPOS=1 TO LEN(CTEXTI$(LNE))
7160      NXTLTR$=MID$(CTEXTI$(LNE),CHARPOS,1)
7180      Z=ASC(NXTLTR$)-64
7200      MFREQ(Z)=MFREQ(Z)+1
7220    NEXT CHARPOS
7240  NEXT LNE
7260  FOR Z=1 TO 26
7280    TOTLTRS=TOTLTRS+MFREQ(Z)
7300    PHISUM=PHISUM+(MFREQ(Z)*(MFREQ(Z)-1))
7320  NEXT Z
7340  PHIMONO=26*PHISUM/(TOTLTRS*(TOTLTRS-1))
7360  MFLAG=1
     :STAT$(1)=" (COMPLETED)"
     :STATUS$(6)="      (COMPLETED)"
7380  RETURN
7400  '

7420  ' *** Digraphic Frequency and IC ***
7440  FOR LNE=1 TO NRLINES
7460    IF (LEN(CTEXTI$(LNE))/2-INT(LEN(CTEXTI$(LNE))/2))=0
          THEN 7520
7480    CARRY$=RIGHT$(CTEXTI$(LNE),1)
       :CTEXTI$(LNE)=LEFT$(CTEXTI$(LNE),LEN(CTEXTI$(LNE))-1)

7500    CTEXTI$(LNE+1)=CARRY$+CTEXTI$(LNE+1)
7520  NEXT LNE
7540  FOR LNE=1 TO NRLINES
7560    FOR DIG=1 TO INT(LEN(CTEXTI$(LNE))/2)
7580      LTR1=ASC(MID$(CTEXTI$(LNE),DIG*2-1,1))-64
         :LTR2=ASC(MID$(CTEXTI$(LNE),DIG*2,1))-64

7600      IF LTR1=-18 OR LTR2=-18
            THEN 7640
7620      DIFREQ(LTR1,LTR2)=DIFREQ(LTR1,LTR2)+1
7640    NEXT DIG
7660  NEXT LNE
7680  FOR ROW=1 TO 26
7700    FOR COLUMN=1 TO 26
7720      TOTDIG=TOTDIG+DIFREQ(ROW,COLUMN)
7740      DIPHISUM=DIPHISUM+(DIFREQ(ROW,COLUMN)*(DIFREQ(ROW,COLUMN)-1))
7760    NEXT COLUMN
7780  NEXT ROW
7800  PHIDIG=676*DIPHISUM/(TOTDIG*(TOTDIG-1))
```

```
7820  DFLAG=1:
     :STAT$(2)=" (COMPLETED)"
     :STATUS$(6)="  (COMPLETED)"
7840  RETURN
7860  '
7880  ' *** Periodic Frequency, IC Subroute ***
7900  CYCLEPOS=0
7920  INPUT “What period do you want to use? ",PERIOD
7940  FOR N=1 TO PERIOD
7960    FOR M=1 TO 26
7980      PFREQ(N,M)=0
8000    NEXT M
8020    PERPHISUM(N)=0
       :PERTOTLTR(N)=0
8040  NEXT N
8060  FOR N=1 TO NRLINES
8080    FOR M=1 TO LEN(CTEXTI$(N))
8100      CYCLEPOS=CYCLEPOS+1
8120      IF CYCLEPOS>PERIOD
            THEN CYCLEPOS=1
8140      NXTCHAR$=MID$(CTEXTI$(N),M,1)
8160      Z=ASC(NXTCHAR$)-64
8180      IF Z=-18 THEN Z=27
8200      PFREQ(CYCLEPOS,Z)=PFREQ(CYCLEPOS,Z)+1
8220    NEXT M
8240  NEXT N
8260  FOR M=1 TO PERIOD
8280    FOR N=1 TO 26
8300      PERTOTLTR(M)=PERTOTLTR(M)+PFREQ(M,N)
8320      PERPHISUM(M)=PERPHISUM(M)+(PFREQ(M,N)*(PFREQ(M,N)-1))
8340    NEXT N
8360    PHIPERI(M)=26*PERPHISUM(M)/(PERTOTLTR(M)*(PERTOTLTR(M)-1))
8380  NEXT M
8400  PFLAG=1
     :STAT$(3)="  (COMPLETED)"
     :STATUS$(6)="  (COMPLETED)"
8420  IF CMIXFLAG=0
        THEN 8540 ' skips mixed alphabet routine if std sequence
8440  FOR M=1 TO PERIOD
8460    FOR N=1 TO 26
8480      PMIXFREQ(M,N)=PFREQ(M,ASC(MID$(CCOMPO$,N,1))-64)
8500    NEXT N
8520  NEXT M
8540  RETURN
8560  '
8580  ' *** Mixed Alphabet Periodic Stat Print ***
8600  ALPH$=" A B C D E F G H I J K L M N O P Q R S T U
      V W X Y Z"
8620  CLS
```

```
8640  OUTFILE$=PRINTER$
8660  GOSUB 6440
8680  IF MFLAG=1
        THEN GOSUB 8880
8700  IF DFLAG=1
        THEN PRINT #1,FORMFEED$
       :GOSUB 9080
8720  IF PFLAG=1
        THEN PRINT #1,FORMFEED$
       :GOSUB 9360
8740  IF CMIXFLAG=1
        THEN PRINT #1,FORMFEED$
       :GOSUB 9580
8760  PRINT #1,FORMFEED$
8780  PRINT #1,FORMFEED$
8800  CLOSE #1
8820  RETURN
8840  '
8860  ' *** Print Monographic Stats ***
8880  PRINT #1,
     :PRINT #1,
8900  PRINT #1,ALPH$
8920  FOR N=1 TO 26
8940    PRINT #1,USING "###";MFREQ(N);
8960  NEXT N
8980  PRINT #1,
     :PRINT #1,
9000  PRINT #1,"TOTAL LETTERS =";TOTLTRS;"   MONOGRAPHIC IC =";PHIMONO
9020  RETURN
9040  '
9060  ' ** Print Digraphic Stats **
9080  PRINT #1,
     :PRINT #1,
9100  PRINT #1, "  ";ALPH$
9120  FOR N=1 TO 26
9140    PRINT #1,CHR$(N+64);
9160    FOR M=1 TO 26
9180    PRINT #1,USING "###";DIFREQ(N,M);
9200    NEXT M
9220    PRINT #1,
9240  NEXT N
9260  PRINT #1,
     :PRINT #1,
9280  PRINT #1, "TOTAL DIGRAPHS =";TOTDIG;"   DIGRAPHIC IC=";PHIDIG
9300  RETURN
9320  '
9340  ' *** Print Monographic Stats ***
9360  PRINT #1,
     :PRINT #1,
9380  FOR N=1 TO PERIOD
9400    PRINT #1,ALPH$
9420    FOR M=1 TO 26
9440      PRINT #1,USING "###";PFREQ(N,M);
9460    NEXT M
9480    PRINT #1,
9500    PRINT #1,"TOTAL LETTERS =";PERTOTLTR(N);"        IC=";PHIPERI(N)
9520    PRINT #1,
       :PRINT #1,
9540  NEXT N
9560  RETURN
9580  PRINT#1,
     :PRINT #1,
9600  FOR M=1 TO PERIOD
9620    ALPHMIX$(M)=" "
9640    FOR N=1 TO 26
9660      ALPHMIX$(M)=ALPHMIX$(M)+"   "+MID$(CCOMPO$,N,1)
9680    NEXT N
9700  NEXT M
9720  FOR M=1 TO PERIOD
9740    PRINT #1,ALPHMIX$(M)
9760    FOR N=1 TO 26
9780      PRINT #1,USING "###";PMIXFREQ(M,N);
9800    NEXT N
9820    PRINT #1,
9840    PRINT #1, "TOTAL LETTERS =";PERTOTLTR(M);"        IC =";PHIPERI(M)
9860    PRINT #1,
       :PRINT #1,
9880  NEXT M
9900  RETURN
9920  '
9940  ' *** Statistics Save to Disk Subroutine ***
9960  ALPH$=" A B C D E F G H I J K L M O P Q R S T U
      V W X Y Z"
9980  CLS
10000  PRINT "Enter the complete disk filename for the saved statistics, for example,"
10020  INPUT "A:MYSTAT.TXT ";OUTFILE$
10040  FILEFLAG=1
10060  GOSUB 6440
10080  IF MFLAG=1
         THEN GOSUB 8880
10100  IF DFLAG=1
         THEN GOSUB 9080
10120  IF PFLAG=1
         THEN GOSUB 9360
10140  IF CMIXFLAG=1
         THEN GOSUB 9580
10160  CLOSE #1
10180  RETURN
```

```
10200 '
10220 ' *** Subroutine to Find Repeats ***
10240 INPUT "What is the shortest length repeat you want listed?",RPTLEN
10260 OUTFILE$=PRINTER$
10280 OPEN OUTFILE$ FOR OUTPUT AS #1
10300 IF RPTLEN<2
        THEN 10240
10320 FOR TLINE=1 TO NRLINES-1
10340   FOR ALTR=1 TO LEN(CTEXTI$(TLINE))
10360     IF TLINE<>NRLINES
            THEN CT$=CTEXTI$(TLINE)+CTEXTI$(TLINE+1)
          ELSE CT$=CTEXTI$(TLINE)
10380     A$=MID$(CT$,ALTR,RPTLEN)
10400     FOR BLTR=ALTR+2 TO LEN(CTEXTI$(TLINE))+2
            :BLINE=TLINE
            :CTB$=CT$
10420       IF BLTR>LEN(CTEXTI$(TLINE))
              THEN 10480
10440       B$=MID$(CTB$,BLTR,RPTLEN)
10460       IF A$=B$
              THEN GOSUB 10800
10480     NEXT BLTR
10500     IF TLINE=NRLINES
            THEN 10660
10520     FOR BLINE=TLINE+1 TO NRLINES
10540       IF BLINE<>NRLINES
              THEN CTB$=CTEXTI$(BLINE)+CTEXTI$(BLINE+1)
            ELSE CTB$=CTEXTI$(BLINE)
10560       FOR BLTR=1 TO LEN(CTEXTI$(BLINE))
10580         B$=MID$(CTB$,BLTR,RPTLEN)
10600         IF A$=B$
                THEN GOSUB 10800
10620       NEXT BLTR
10640     NEXT BLINE
10660   NEXT ALTR
10680 NEXT TLINE
10700 PRINT #1, FORMFEED$,FORMFEED$
10720 CLOSE #1
10740 RETURN
10760 '
10780 ' *** Subroutine to Check Length of Repeat and Print It ***
10800 LONGER=RPTLEN
10820 PRINT A$
10840 LONGER=LONGER+1
10860 IF MID$(CT$,ALTR,LONGER)=MID$(CTB$,BLTR,LONGER)
        THEN 10840 ' Try it longer
10880 LONGER=LONGER-1 ' Nope, too long
10900 PRINT #1,MID$(CT$,ALTR,LONGER);" AT LINE";TLINE;", LETTER";ALTR;
      " AND AT LINE";BLINE;", LETTER";BLTR
```

```
10920  RETURN
10940  '
10960  ' *** Quit Subroutine ***
10980  CLS
11000  INPUT “Are you sure you want to quit (Y/N)? ”,CHOICE$
11020  IF CHOICE$ <>″Y″ AND CHOICE$ <> ″y″
         THEN 1180
11040  KEY ON ' restores bottom of screen prompts
11060  END
11080  '
11100  ' *** Chi Test Subroutine ***
11120  PRINT “Do you want to print results or save to disk as text file?”
11140  INPUT “Enter P for printer, D for disk, or Q to quit.”,S$
11160  IF S$=“P” OR S$=“p”
         THEN OUTFILE$=PRINTER$
        :GOTO 11240
11180  IF S$=“Q” OR S$=“q”
         THEN RETURN
11200  IF S$<>“D” AND S$<>“d”
         THEN 11140
11220  INPUT “Enter the complete disk filename. ”,OUTFILE$
11240  OPEN OUTFILE$ FOR OUTPUT AS #1
11260  PRINT “Which of the ”;PERIOD;“alphabets do you want to match?”
11280  PRINT
11300  INPUT “      Enter number of 1st alphabet to be matched: ”,ALF1
11320  INPUT “      Enter number of 2nd alphabet to be matched: ”,ALF2
11340  PRINT “MATCHING ALPHABET”;ALF1;“AND ALPHABET”;ALF2
11360  PRINT #1,“MATCHING ALPHABET”;ALF1;“AND ALPHABET”;ALF2
11380  FOR N=1 TO 26
11400    IF CMIXFLAG=1
           THEN SET1(N)=PMIXFREQ(ALF1,N)
         ELSE SET1(N)=PFREQ(ALF1,N)
11420    IF CMIXFLAG=1
           THEN SET2(N)=PMIXFREQ(ALF2,N)
         ELSE SET2(N)=PFREQ(ALF2,N)
11440  NEXT N
11460  FOR M=1 TO 26
11480    FOR L=1 TO 26
11500      PRINT #1,″   ″MID$(CCOMPO$,L,1);  ' Print first sequence
11520    NEXT L
11540    PRINT #1,
11560    FOR L=1 TO 26
11580      PRINT #1, USING ″###″;SET1(L); ' Print first sequence frequencies
11600    NEXT L
11620    PRINT #1,
11640    FOR L=0 TO 25
11660      LTRPOS=M+L
          :IF LTRPOS>26
               THEN LTRPOS=LTRPOS-26
```

```
11680       PRINT #1, "   ";MID$(CCOMPO$,LTRPOS,1); ' Print second sequence
11700     NEXT L
11720     PRINT #1,
11740     MATCH(M)=0
11760     FOR N=1 TO 26
11780       MATCH(M)=MATCH(M)+(SET1(N)*SET(N))
11800       PRINT #1, USING "###";SET2(N); ' Print second sequence frequencies
11820     NEXT N
11840     PRINT #1,
11860     IF M/2-INT(M/2)<>0
            THEN PRINT TAB(1) “MATCH”;M;“:”;MATCH (M);
          ELSE PRINT TAB(40) “MATCH”;M;“:”;MATCH (M);
11880     PRINT #1,“       MATCH”;M;“:”;MATCH (M)
         :PRINT #1,
11900     SET2(27)=SET2(1)
11920     FOR N=1 TO 26
11940       SET2(N)=SET2(N+1):
          NEXT N
11960   NEXT M
11980   IF OUTFILE$=PRINTER$
          THEN PRINT #1,FORMFEED$
12000   INPUT “ANOTHER MATCH (Y/N)?”,Q$
12020   IF Q$=“Y” OR Q$=“y”
          THEN 11300
12040   IF OUTFILE$=PRINTER$
          THEN PRINT #1,FORMFEED$
12060   CLOSE #1
12080   RETURN
```

GLOSSARY

ASCII	American standard code for information interchange
C	ciphertext
CEOI	Communications-Electronics Operation Instructions
COMINT	communications intelligence
CR	carriage return
DA Pam	Department of the Army Pamphlet
EBDA	encipher below, decipher above
ERDL	encipher right, decipher left
FIG	figure
FM	field manual
IC	index of coincidence
LF	line feed
LTR	letter
MOS	military occupational specialty
NO	number
P	plaintext
SOI	Signal Operation Instructions
TM	technical manual
TRADOC	United States Army Training and Doctrine Command
USAISD	United States Army Intelligence School, Fort Devens
z	Zulu

Readings Recommended

These readings contain relevant supplemental information.

Army Correspondence Course Program

DA Pam 351-20 Army Correspondence Course Program Catalog. 22 July 1988

NOTE:
For enrollment in either a course or the individual subcourses, complete DA Form 145, Army Correspondence Course Enrollment Application and send it to:

Army Institute for Professional Development
US Army Training Support Center
Newport News, VA 23628-0001

INDEX

This is a topical index organized alphabetically. Citations are to paragraph numbers.

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

THOMAS F. SIKORA
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11E, requirements for FM 34-40-2, Basic Cryptanalysts, (Qty rqr block no. 4607) and FM 34-3, Intelligence Analysis (Qty rqr block no, 1119).

☆ U.S. GOVERNMENT PRINTING OFFICE; 1990-729/952