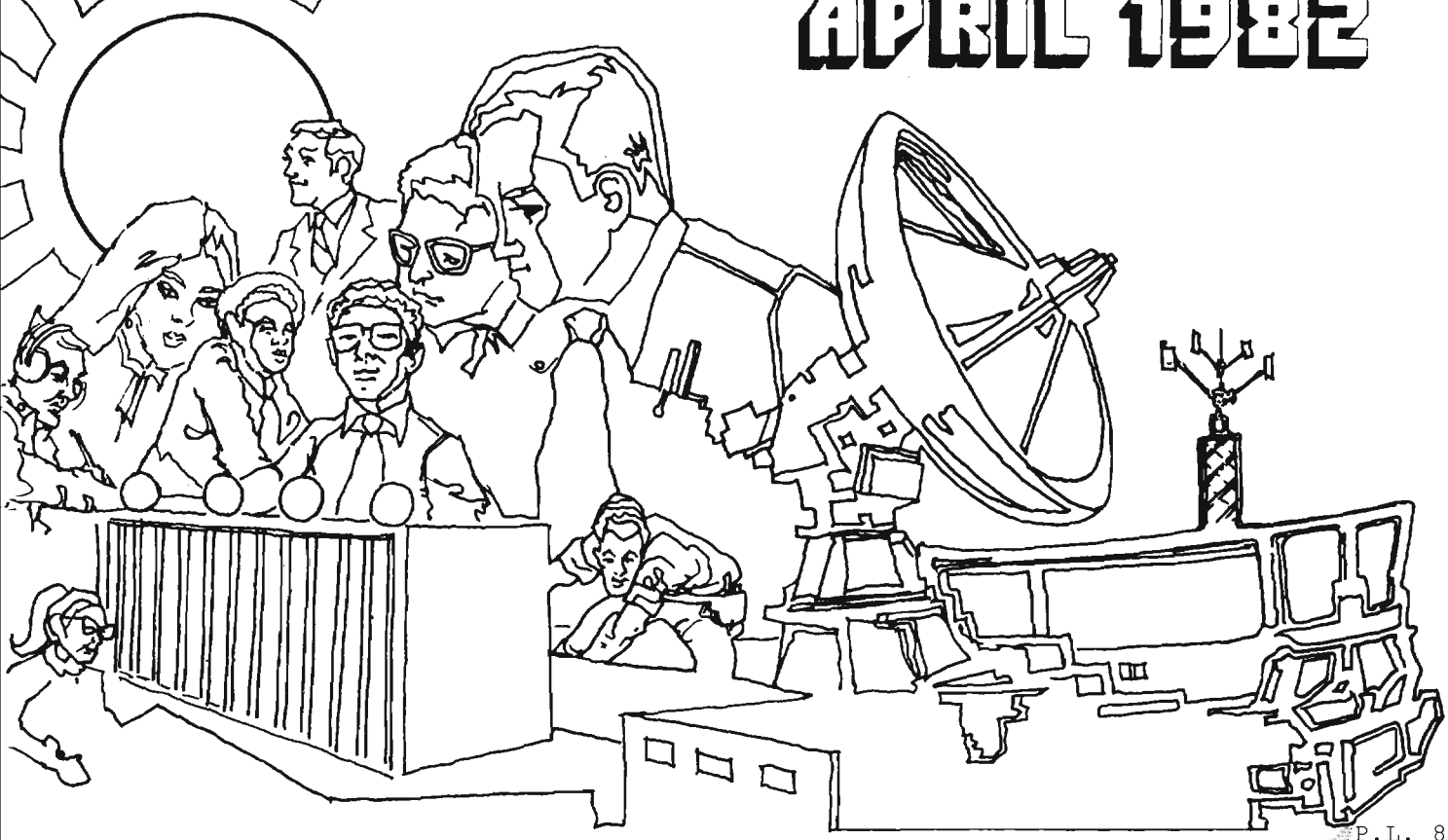
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Apr 2012~~

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

VOL. IX, No. 4 APRIL 1982

For individual (or organizational) subscriptions send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

By now it seems safe to announce that CRYPTOLOG is once again coming out on a monthly schedule. That was our objective back in October, but there were a lot of questions about whether it could be done.

We decided at the outset not to make any promises about publication schedules. These days there are so many people promising so much, and yesterday's promises have a way of fading unfulfilled beneath the flood of ever newer and more exciting promises. Maybe politicians and advertisers and hawkers of the new and better tomorrow don't think we remember those promises; at least they seem to operate as if we don't. But I think we do.

So, my inclination is not to add more promises to the glut, but rather to work on trying to deliver. We will try not to promise you some new development until we can show it to you. (At least one major space program works that way.)

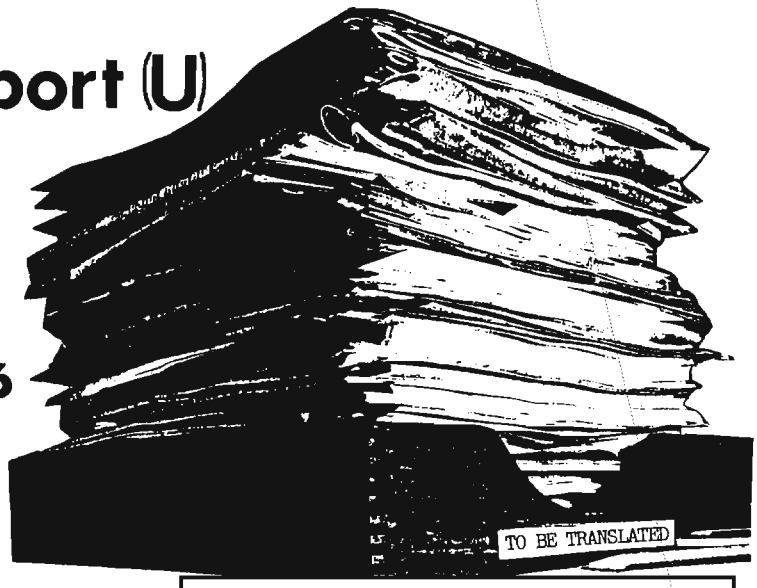
We have had lots of ideas about how to make the magazine more useful to its readers, but not all of them have worked out. Some of them sound great, but the doing of them leaves a lot to be desired. We will continue to try, and we will continue to experiment with various things. Some of the things we plan to try may surprise you, or irritate you, or even offend you. We hope not.

If there is something you think we ought to be doing, or something we are doing that we ought to stop or change, let us know.

P.L. 86-36

Partial Machine Translation: A Final Report (U)

[redacted] P16
and
[redacted] P16



Partial Machine Translation (PMT) is a word-for-word or phrase-by-phrase "translation" from one language to another. The quotations marks are placed around the word "translation" to show that a PMT is not exactly what most people consider a true (or full) translation, but the quotes are inserted reluctantly. Although it may be difficult to read the result, some information may be lost or misinformation added, the quality may be less in virtually every respect than that of a good human (or even machine) translation, a PMT can nevertheless convey to the sympathetic reader the import of the original; and that, after all, is a translation's primary purpose.

(U) The purpose of a PMT is to enable readers with little or no knowledge of the source language to decide on their own whether to request a standard translation or to move on to other texts of potentially greater interest. The alternative might be to burden a linguist with translating many useless texts, assuming adequate linguistic help is available. PMTs can be prepared reasonably cheaply, freeing the linguist from fruitless tasks; the linguist thereby concentrates on tasks of importance.

~~(SC)~~ To illustrate how fine the distinction is between PMT and "true" translation, here is a sample of each. Which is which?

[redacted]

~~(S-CCO)~~ At first glance there does not seem to be much difference between the two versions. The second version is the PMT. (Actually, certain PMT conventions not yet explained but which would quickly become second nature to users have been smoothed out of the version as given above. For example, "we will be" would appear "(we)will_be"; "N" is a garble for "NR" and would be translated "?"; the capitalizations in "Again", "Further", "Awaiting" are not made. Also the original had a garble which caused "interest"

to be received as two words; the first of these would be translated "interest", the second would get a "?".) The first version above is the sender's own translation.

II. Background (U)

(U) PMTs could doubtless have been prepared nearly three decades ago in the early days of Machine Translation, but researchers were convinced that much better translations could be made automatically. They were correct but, even with the expenditure of considerable linguistic and programming efforts, their most optimistic hopes have not yet been achieved. (In addition, the telegraphic and/or garbled texts for which PMT has been expressly designed are less amenable to translation than texts written in standard language.) PMTs can yield useful results after only a minimal computational and linguistic investment.

[redacted]

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

[redacted]

(U) A general consideration which for the most part has been left implicit in the discussion that follows is that a PMT does whatever must be done to produce output with a reasonable chance of being usable, together with whatever else can be easily and usefully done to enhance the final product. Fine points which could be handled with difficulty but which would rarely improve the quality of a PMT have usually been omitted. P.L. 86-36
EO 1.4.(c)

III. Russian PMT: Language Independent (SC)

(U) A PMT output consists of groups of three lines:

- a line of the original text,
- a second line with the PMT itself, and
- a blank line as a separator.

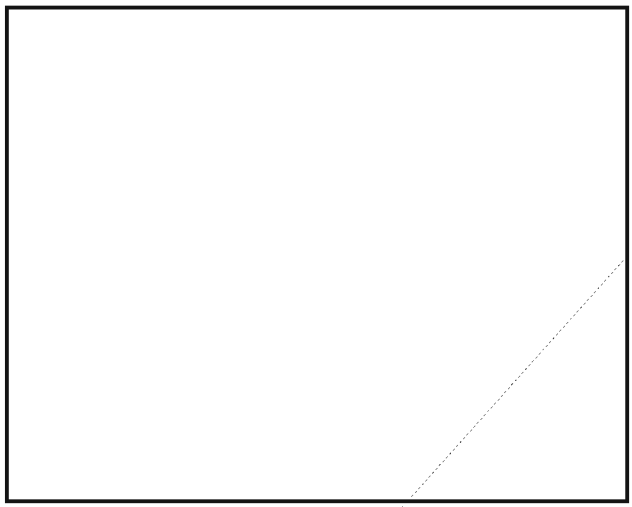
The words (or phrases) of the second line are aligned underneath the words (or phrases) of the first line to the extent possible by expanding spaces in the original text. (There seems to be little danger of misleading someone reading the original.) This three-line pattern continues to the end of the text.

(U) Some words (e.g., misspellings, proper names, and cognates that are not likely to cause problems for the reader) are not in the dictionary. When they appear in the text, they will be represented by "?" to distinguish them from words which are within phrases and translated as such. Numbers and punctuation that appear in the original are not copied into the PMT line to avoid cluttering it and to enable punctuation conventions (built into

the dictionary) to show more clearly just how the translation is to be interpreted.

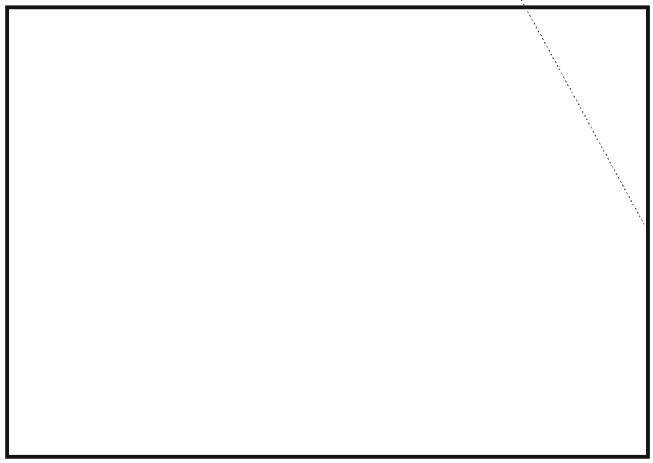
(U) The heart of any PMT effort is the dictionary. The person in charge of preparing and maintaining the dictionary will be called the lexicographer. The current dictionary is empirical, which means that it is based on actual texts. One is well advised to begin with a generous sample of texts to be translated and to compile therefrom a list of words in inverse frequency order. A KWIC (keyword in context) index will aid in determining the most apt translation, or gloss, and in deciding what phrases should become a part of the dictionary. The dictionary is then expanded by observing words and phrases that appear in subsequent texts without being translated or, even worse, with incorrect translations. (A few critical words, such as "plutonium", might be added just in case.)

(U) The current PMT algorithm can handle phrases (or idioms) whose individual words are contiguous, which includes a large number of useful cases, such as English "OF COURSE" or Russian "DO SIH POR". Phrases will normally be entered only when a word-for-word rendering is inadequate.



(U) For a heavily inflected language like Russian, it may be objected that words would have to be entered in all or many of their forms, a tedious job at best and a computer overload at worst. Fortunately, it has been observed that inflections may be ignored without severely diminishing a PMT's usefulness. An English example would be WALK%, standing for the forms WALK, WALKS, WALKED, WALKING (also WALKER, WALKERS, WALKWAY, etc., although entries such as WALKER% would take precedence over WALK% as appropriate). The %

represents all remaining letters to the end of the word. Most Russian words now require only one entry.



(U) It is wisest to include some common forms in full, such as SOOBQIM '(we)inform' and SOOBQITE '(you)inform', which will make many messages much clearer than the gloss given to SOOB%, 'inform'. Also, the participles of some verbs occur frequently enough to justify separate inclusion; POLUCHEN% 'received' is much clearer than POLUCH% 'receive'.

(U) Trimming can be done within idioms, as in JELEZ% DOROG% (for JELEZNAYA DOROGA) 'railroad. (The lexicographer must, however, be consistent. The full stem of the first word is JELEZN%, and if JELEZN% 'iron' is also an entry, the idiom will be missed.)

(U) If certain conventions are followed when entering glosses, the readability of the

output will be enhanced. Multiword glosses may usefully be joined by _, as in KONECHNO 'of_course'. Using lowercase for the English will be beneficial for implementations in which the case can be preserved (this is not true of the printer used now). Parenthesizing words which might be redundant is helpful, so that MY SOOBQIM becomes 'we (we)inform'; this convention is essential if the cleanup feature of Section IV is to be fully utilized.

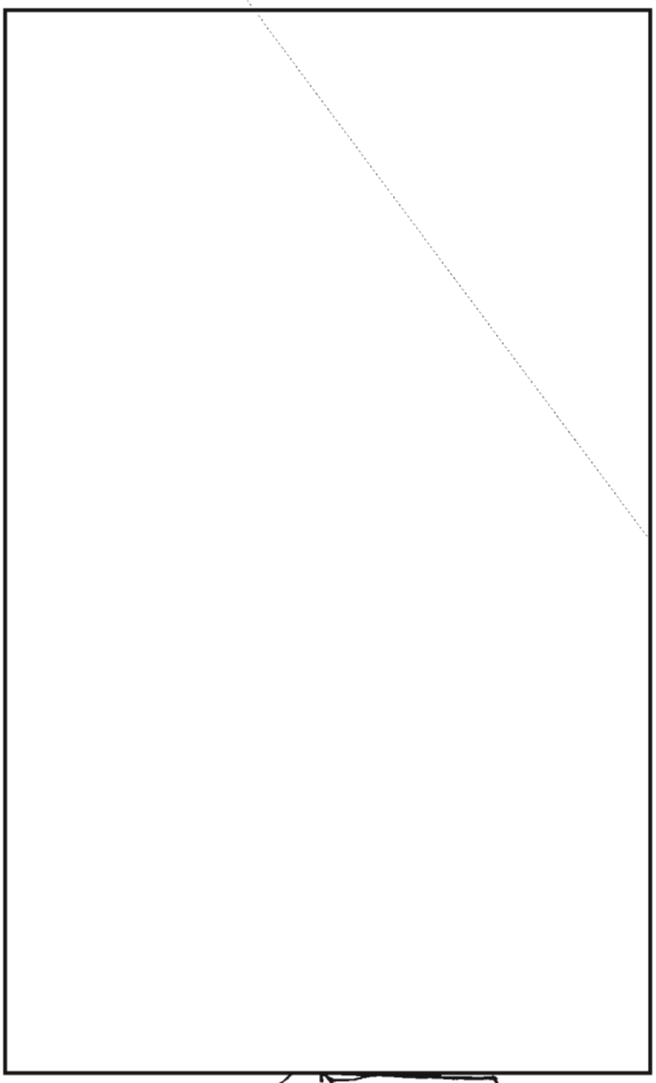
(U) Choosing the right gloss for a word with many meanings certainly can be a problem. One may:

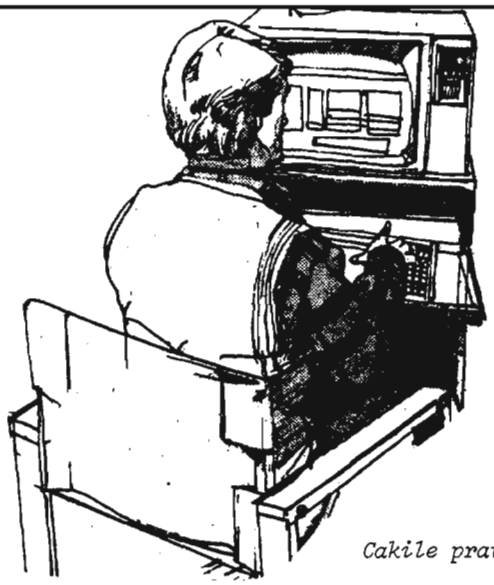
- choose the most likely meaning (REKLAMA = 'advertising', not 'publicity');
- take the most striking meaning (GRANAT% = 'grenade', although 'pomegranate' is more likely);
- separate two meanings by a conventional slash (CHTO = that/what) (overuse of this will clutter the output, so fewer than 10 glosses have it);
- prefix the gloss with a conventional question mark (as in BLOK% = '?pulley'), an especially useful convention when the unlisted meaning is a cognate, as in the example given.

(U) Prefixes may become entries in the dictionary, with resulting savings in computer storage and dictionary upkeep. If AVAILABLE is in the dictionary, as well as the prefix UN= (the suffixed = signals a prefix), then UNAVAILABLE can be glossed correctly even if it had not appeared in earlier traffic. (If the word UNION were not entered, a false prefix will be taken from it regardless of whether ION is an entry. Use of prefixes results in such situations often enough that it is recommended that prefix glosses end in = to alert the user to possible trouble. NEYASNYJ is therefore glossed 'un=clear'.) The prefix convention will find use in handling certain Russian compounds, as in GOSBANK 'state=bank'.

(U) Although Russian examples have been given up to now, virtually everything that has been said is applicable to other languages, so this version of the program has been called the "language-independent" version. You still need a separate dictionary for each language, of course, and it is possible that a given language will require some special handling.

~~(SC)~~ Indeed there is one section of code that must be added to the language-independent version in order to allow for reasonable Russian output without imposing a severe burden on the dictionary.





Cakile prattii

IV. Russian PMT: Language Dependent ~~(SC)~~

(U) A step up from the preceding version of the program requires morphological analysis. The semantic content of Russian is expressed in the morphology to a greater extent than in most languages. The programming required to analyze Russian morphology is essentially different from what would pertain to any other language, so this is the "language-dependent" version of PMT. Some of the principles involved would be relevant for other languages.

(U) The meaning of a Russian word-ending often depends on the class to which the word belongs. For example, -U on a feminine noun is usually the accusative case, on a nonfeminine noun usually dative, on verbs usually first person singular. Consequently, it is necessary to assign grammar codes to whatever dictionary entries are to be subject to morphological analysis. The codes in use are F, N, A, and V for feminine nouns, nonfeminine nouns, adjectives, and verbs. (The occasional use of P for prepositions will be explained later.) The code is stored in the rightmost of the positions allotted to the gloss in the lexicographer's dictionary. Absence of a code means that the entry is invariant or that, for one reason or another, analysis would tend to obscure the meaning or clutter the output. (For example, names of months receive no code because the typical usage '3 MARTA' is better glossed '3 March' than '3 (of)March'. This does mean that 'KONEC MARTA' comes out as 'end March'.)

(U) More codes could be used to distinguish masculines from neuters, nouns likely to occur in the plural from probable singulars, feminines of the soft declension, nouns with adjectival declensions, and so forth. Relatively little would be gained for the increased work expended by the programmer and lexicographer.

(U) Note that REKLAM% 'advertising' now probably requires three entries: REKLAM% (F), REKLAMN% (A), REKLAMIR% (V). On the other hand, participles and forms such as PROSIM and SOOBQITE no longer need separate entries.

~~(SC)~~ If a grammar code is present, the program may modify the gloss obtained from the dictionary depending on the ending of the Russian word involved. Feminine nouns offer a relatively simple example:

- if the ending is OJ, the case is instrumental, so '(with)' is preposed to the gloss (not only is 'with' the correct preposition for some pure instrumentals, but most often the preposition S which governs the instrumental

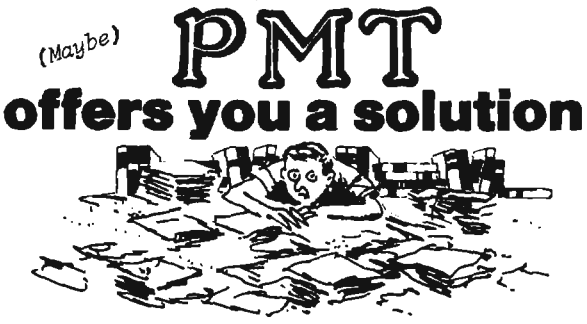
- if the ending is AM, the case is dative plural, so the English gloss is pluralized and '(to)' preposed;

- and so on for locative, genitive, and instrumental plural.

No modification to the gloss is required if the noun is nominative or accusative singular, so those endings are not tested. Nouns in the dative and locative singular have identical forms; the gloss could be modified by preposing '(to/in/of)' with 'of' reflecting the frequent omission of the preposition O which governs the locative, although this is not yet done due to the clutter. A genitive singular noun looks the same as a nominative or accusative plural: '(?of)' is preposed since the genitive is more common, with the hope that users can accommodate the times when a plural occurs.

(U) A small amount of syntactic analysis takes place in disambiguating certain adjectival forms. (Otherwise the unambiguous noun that follows might produce a preposition lying between the adjective and the noun.) For example, adjectives ending YM may be instrumental singular or dative plural. In the latter case, the following noun will generally end AM. The program looks ahead one word and examines the ending: if it is AM, '(to)' is preposed to the adjective's gloss; otherwise '(?with)' is preposed.

(U) Whenever adjectives acquire a preposition, the program prevents the following word (if it is a noun or another adjective in the same case) from acquiring a preposition as well.



(U) Participles represent a more complex situation. A Russian participle may be regarded as a verb stem plus a participial suffix plus an adjectival ending. Some adjectival endings coincide with verb endings (IM for example), so the presence of a participle must be tested before such endings are declared to be verbal. So if a verb ends with any of two dozen or so adjectival endings, the preceding few letters are examined. If they are SC, SCH, or Q, the word is almost certainly a present active participle, so the English suffix -ing is added to the gloss, and the word is treated as an adjective; as indicated earlier, the adjectival ending may cause a preposition to be added to the gloss. The other participial suffixes are treated similarly.

(U) The above does not exhaust the richness of Russian morphology; it merely serves as an indication of ways by which much semantic information may be extracted without unduly complicating the program or increasing its run time.

(U) English morphology is comparatively simple. The irregular verb 'be' is rendered 'is', 'was/were', and 'being' as in OTSUTSTVUET 'is_absent'. (Note that by convention it is the first word of a multiword gloss that is inflected.) Use of other irregular words is discouraged; the gloss 'come' should defer to the regular s verb 'arrive'. The program can handle the spelling changes exemplified by word like 'indicated', 'shipped', and 'cities', but there is no convenient way to get both words like 'considering' and words like 'referring' spelled correctly, so misspellings like 'refering' will be encountered from time to time.

[redacted]

[redacted]

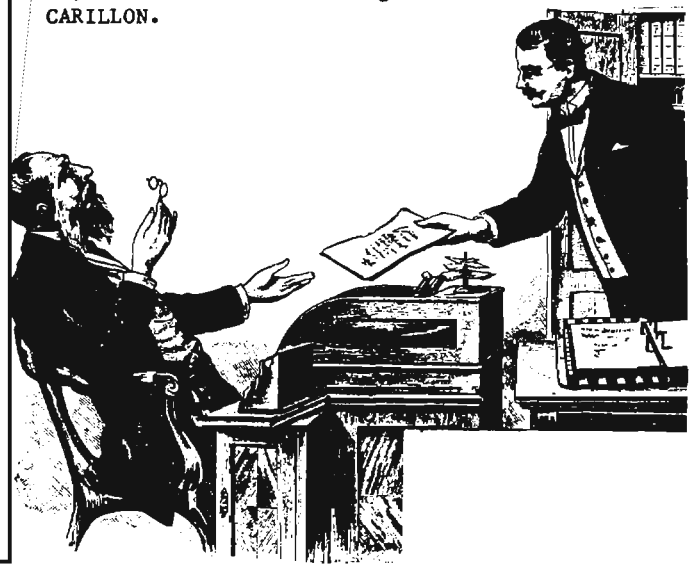
V. Russian PMT: Technical Details ~~(SC)~~

[redacted]

(U) Cleanup would achieve only minimal advantages if applied to the language-independent version, but it constitutes an integral part of this version.

[redacted]

(U) The lexicographer's copy of the dictionary resides on a CARONA file which can be updated using the Rand editor. This, however, is not a form which the main program (CAKILE) can use. Whenever the dictionary is modified, a program (UCDICT) must be run to restructure it, and store the resulting file on disc at CARILLON.



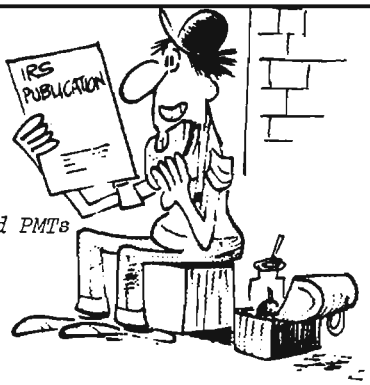
(U) The structure used is the Unary Chain Dictionary, which is completely described in [redacted] paper of the same name. Suffice it to say that this structure:

[redacted]

[redacted]

[redacted]

EO 1.4.(c)
P.L. 86-36



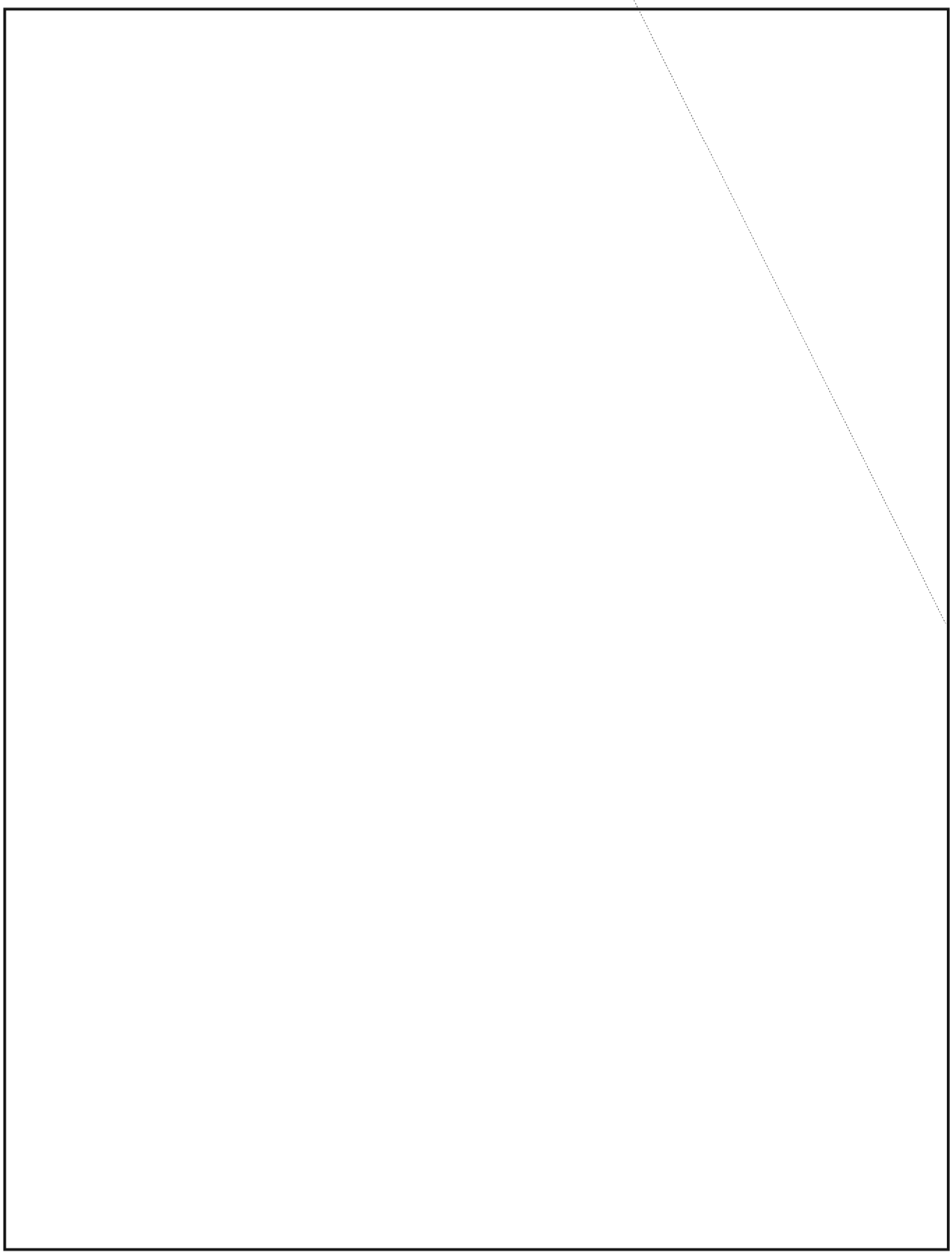
What else could PMTs help us with?

EO 1.4.(c)
P.L. 86-36

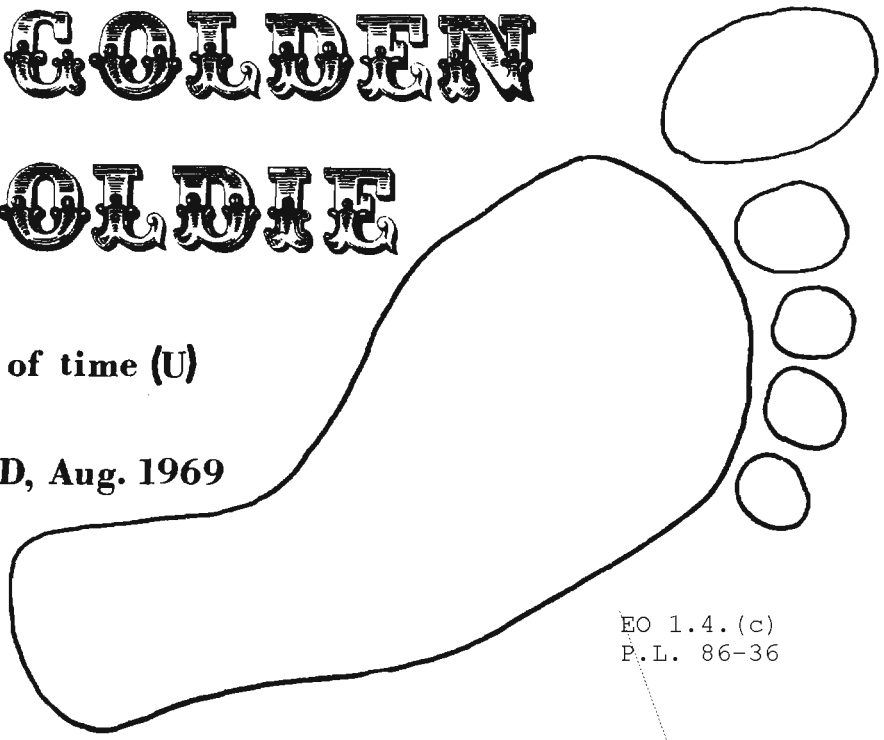
(U) Most of the programming effort needed for PMT has already been expended. The Russian PMT dictionary requires further expansion by a qualified linguist/analyst. For other languages, considerable linguistic effort must still be invested to produce usable output. It is up to potential users to evaluate the extent to which such an investment would yield profits in the form of more judicious use of linguistic resources.

P.L. 86-36
EO 1.4.(c)

VIII. Appendix



GOLDEN OLDIE



Tracks in the sands of time (U)
by Fred Mason
from COMMAND, Aug. 1969

Go, stalk the red deer o'er the heather,
Ride, follow the fox if you can!
But, for pleasure and profit together,
Allow me the hunting of Man, --
The chase of the Human, the search for the Soul
To its ruin, -- the hunting of Man.

The Old Shikarri
Rudyard Kipling

~~(SC)~~ In this game[1] we play, called TA, what matters is the target, not his spoor. Where <u>is</u> he <u>now</u>, who <u>is</u> he, what <u>is</u> he doing? To trail him by his aliases of otherwhen and plot him by his utterances of otherwhere is useful only if you are catching up.

(U) It is a terrible temptation to follow his red herrings, to watch the flutterings of a Mother Bird when you near the nest. And one of our major problems with computers is the relatively enormous storage capacity -- most of which contains old target spoor; not even his present evasions.

(U) One of the best ways of distracting our attention from here and now is to offer us more than we can assimilate -- and to tease us with patterns which change so often and so erratically that we lead ourselves off course -- we "hunt[2]."

~~(SC)~~ There are an infinite number of points[3] on a line and the target signal officer attempts now to draw our attention to as many of these points[4] as possible -- to distract us from the line.

[redacted]

(U) Sounds like the description of the human brain -- a finite number of cells with an almost infinite number of interconnections.

[redacted]

~~(SC)~~ Is all this necessary? Yes and no; depends on the target and the analytic purpose involved. Having a limited number of analysts, it is vital to our success in catching the target that we do not waste our time.

[redacted]

~~(C-CCO)~~ The only problem here is the <u>in between</u> situation: no continuity, but we still hope to achieve it. Old sets on which continuity has been lost (or never achieved) remain useful for this purpose over a limited period -- but very limited.

~~(SC)~~ The point of all this is to urge that we purge. Yes, we must deal with <u>all</u> of today's intercept -- sort it into homogeneous piles and distribute it properly -- milk it of its current content -- report it as <u>reflections of real units, here and now.</u>

[redacted]

Cope with today today and save only as much of the many yesterdays as you must -- preferably in summary form only. Don't be so bemused by old tracks that you have no time for those still hot -- get rid of the old ones.

As you ramble on through life, Brother,
Whatever be your goal,
Keep your eye upon the doughnut
And not upon the hole.

Anon.

---

1. And it is a game -- against a player at least as clever as you -- his life or death at stake (yours, too, if you are part of our team present in the arena).
2. Oscillate alternately to each side of a neutral point because of insufficient stability controls.

[redacted]

4. Or, he offers us trees in hopes that we won't notice the forest.

Everything's coming up roses...

A nostalgia piece by an unknown author, on music from the early part of this century. Have fun with Word R!

NSA-Crostic No. 39

1 U		2 G	3 J	4 D	5 K		6 Q	7 J	8 O	9 A	10 W		11 O	12 D										
13 A		14 F	15 J	16 O	17 C	18 W	19 L	20 S	21 G	22 R	23 K		24 M	25 N										
26 S	27 H		28 W	29 T	30 R		31 P	32 W	33 N	34 F	35 Q	36 G	37 E											
38 H	39 V	40 W		41 N	42 T	43 J	44 G	45 C	46 K	47 P		48 M	49 F	50 I										
51 T	52 G	53 H	54 J		55 K		56 U	57 V	58 M	59 T	60 C	61 A	62 F											
63 D	64 T	65 N	66 B		67 F	68 V	69 M		70 K	71 J	72 P	73 N		74 S										
75 A	76 T		77 C	78 I	79 M	80 G	81 O	82 Q		83 M	84 N	85 R	86 I	87 D										
	88 L	89 N	90 H		91 K	92 R		93 Q	94 W		95 J	96 H	97 O											
98 E	99 D	100 F	101 C	102 T	103 O	104 H	105 U	106 N	107 L		108 W	109 M	110 H	111 U										
	112 V	113 K	114 G	115 W		116 B	117 E	118 G	119 M	120 C		121 B	122 E											
123 T	124 F	125 P	126 N	127 Q		128 M	129 T	130 J	131 G	132 U	133 V		134 N	135 K										
136 V		137 A	138 M	139 P	140 F	141 G		142 D	143 R	144 M		145 F	146 P	147 S										
148 M		149 B	150 J	151 T	152 Q		153 M	154 I	155 O	156 B	157 V	158 P	159 C											
160 E	161 R	162 J		163 C	164 F	165 T	166 L	167 H	168 N	169 U	170 W		171 J	172 R										
173 C	174 K	175 V	176 H		177 U	178 B	179 Q	180 P	181 F		182 G	183 S	184 P	185D / 186L										

A. British composer (1763—1824), wrote "The Bay of Biscay"
13 75 61 137

B. Pseudo-Swedish popular song of 1939
178 156 66 116 121 149

C. American comedian; foreign capital
101 17 163 120 60 173 159 45 77

D. Musical of the early '30s, in which Bob Hope appeared
185 4 142 99 87 63 12

E. Singing family
37 98 160 117 122

F. Orchestral signal for brass instruments to play loudly
145 9 164 100 34 62 14 124 49 140 67 181

G. Razaf and Waller's Rose (1929)
44 21 131 52 182 141 80 36 2 118 114

H. Victor Herbert's Rose (1909) (2 wds)
96 38 104 90 176 27 53 167 110

I. He wanted to "get somewhere" with his girl, but alas, all he could do was "get out and get" this
78 154 50 86 15

J. Clarke and Hanley's Rose (1921)
54 130 43 71 95 162 150 7 3 171

K. Alcott's Rose (with "My'), 1899 (2 wds)
5 174 70 135 55 46 91 23 113

L. "Honey Boy" _____, minstrel of the turn of the century
107 166 88 19 186

M. Non-commercial, low-cost, often experimental drama; permises in which such dramas are presented (2 wds)
24 119 148 128 58 69 79 109 153 83 144 138 48

N. Song hit from "The New Yorkers" (1930) (3 wds)
106 134 168 73 84 25 41 33 65 89 126

O. Place for dancing, accoring to Dietz and Schwartz (2 wds)
97 11 16 155 81 8 103

P. "_____, will travel": want ad placed by a violinist (2 wds)
146 184 72 158 180 125 31 139 47

Q. George M cohan's Rosie (1923)
179 127 35 93 82 6 152

R. Is this a ballet dancer without her costume?
22 161 85 143 92 172 30

S. What the S-S B did at dawn (September 14, 1814)
74 147 26 183 20

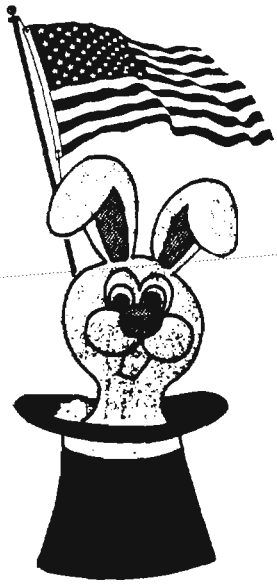
T. 20th century lyricist, often used the pseudonum Arthur Francis (2 wds)
42 165 123 51 151 102 76 64 129 59 29

U. American operatic tenor (1896—1960)
111 1 56 105 169 132 177

V. Elegy
112 68 157 57 175 39 136 133

W. Haunting melody from Word D
10 32 94 108 18 40 170 28 115

LOOKING AROUND with



P.L. 86-36

Review:

THE AMERICAN MAGIC (U)
by Ronald Lewin
Farrar, N.Y. 1982

(U) The Americans were more effective in producing COMINT against the Japanese, than in using it, in Ronald Lewin's opinion. His rather readable book skims over a lot of material, some of it recently declassified, some of it already well known, and some still classified, to give an overview of the development and use of COMINT against the Japanese before and during World War II. Pinches were important in getting started on the Naval codes in the 1920's. After that, continuity in message content, codes, cipher systems and especially in trained cryptanalytic and language personnel were critical to both the Army and Navy COMINT effort.

~~(TSC)~~ The book contains some ironies. Lewin denounces Yardley as disloyal for selling and publishing secret information that induced the Japanese to improve their cipher security. But he does not hesitate to publish Top Secret technical information about how the PURPLE machine was solved, leaked to him by one of his informants who knew about diplomatic cryptanalysis. Lewin also devotes an entire chapter, called "The Stab in the Back", to the risks and potential damage caused by the American press in revealing successes against German and Japanese ciphers. He deplores the inability of the U.S. legal system to conduct trials in camera even when the most crucial wartime secrets are at stake. He further deplores the permissiveness of U.S. society with its attitude of anything goes, "of which the FOIA is the most recent expression". None of this handwringing deterred Lewin from seeking out American and British cryptanalysts and intelligence people to get bits of "private information" to enhance the sales of his own book.

~~(TSC)~~ Lewin's book appears to have been written for a British audience, for it recounts some of the personalities and battles of the Pacific war which are fairly well known to Americans of that era. Inevitably he has serious omissions, for his sources seem to be primarily intelligence people rather than cryptanalysts, although Bundy, Filby, Raven and Tiltman are cited in acknowledgements. He does not know that in the weeks before Pearl Harbor, the main Japanese naval code JN25 was being read, but the resources were too limited to exploit it adequately. JN25 at that time would probably have given considerable insight into Japanese naval preparations. Lewin also fails to note the great importance of cryptanalysis immediately after Midway in reading the attack assessment given by the Japanese, when Nimitz was unable to get a battle report from his own subordinates. This point is clearly made in Potter's book on Nimitz. The Japanese enciphered code system was originally provided them in 1902 by the British Navy as part of the Anglo-Japanese Naval Alliance. Forty years later it was still a secure system, as delays and outages in reading the enciphered code of Army, Navy and Air Force showed. Even today it would be a difficult system. Lewin also fails to note that Royal Navy tactical doctrine, adopted by the Japanese, ordered contact reports and immediate damage reports, and these signals were very useful in monitoring and assessing sea battles. The analysis of the Japanese naval situation after the numerous clashes in the Solomon Islands depended on decrypting these prompt signals. Another point which Lewin apparently missed about Midway is that on 19 May 1942 the U.S. Navy asked the Royal Navy to send a carrier to strengthen the U.S. fleet at Hawaii, because of the loss of the Lexington, and the damage to Yorktown. The British

immediately inquired how the Americans knew that the Japanese fleet, whose whereabouts was a mystery to them, would attack Midway in June. Roskill's The War at Sea (V.2,p.37) recounts that Admiral King had to reveal that the U.S. was breaking into the JN25 traffic, although only in a limited way. The British did not send a carrier to Midway, but sent some cryptanalysts, including Tiltman, to Washington, to see if the U.S. Navy had actually broken the JN25 code. (When they were sure of the competence of the U.S. Navy cryptanalysts, the COMINT liason improved).

~~(S-CCO)~~ Lewin correctly gives substantial credit to U.S. traffic analysis which gave continuous intelligence on the Japanese Navy during the outages when Japanese cryptographic changes cut off ULTRA intelligence. He does not explain the long delay till mid 1943 in breaking into the traffic of the Japanese Army and Air Force, who adopted the same system in 1936 that the Navy used, as a result of a cipher compromise, nor does he touch upon the more important point that it was the higher level nets that were read, giving operational rather than low level tactical details.

~~(TSC)~~ The extraordinary wealth of military and technical information passing from Germany to Japan over the readable Japanese diplomatic and attaché ciphers is developed in Chapter 11, but the most important of this technical intelligence, viz. the details of the new German torpedoes, which allowed the Atlantic convoy escorts to utterly defeat WREN and its successors, is not mentioned. COMINT in early 1943 on German traffic warned of WREN and Royal Navy countermeasures made it ineffective in September 1943 when it was used tactically. The attaché traffic revealed all the technical features of new torpedoes, and other crucial facts about the Schnorkel and Type XXI U-Boat, which allowed prior countermeasures by the British Navy. The Germans misjudged the success of their new weapons and tactics and lost so many U-Boats that they were forced on the defensive, allowing the massive convoys and logistic buildup from mid 1943 till the end of the war without which the invasion of Italy and France would have been impossible.

~~(TSC)~~ Lewin raises a number of questions concerning the American use of the political intelligence from Japanese diplomatic and attaché links concerning Russian-German and Russian-Japanese peace negotiations, and gives an impression that a better political outcome to the war was possible from these insights, perhaps without the use of the Atomic bombs. This appears to overlook the strong interest in high policy circles in the U.S. for a friendly postwar relation with the Russians that tended to nullify the COMINT indications of Soviet military expansion.

~~(TSC)~~ The importance of plain voice COMINT during an air battle in the Marianas illustrates the opportunistic nature of COMINT, and the farsighted practice of carrying a voice gister on a major warship to exploit Japanese plain voice aircraft traffic (p.256). Conversely, the inability of COMINT to reveal the Japanese naval activities before the nearly disastrous battle of Leyte Gulf shows the extent to which even the best COMINT depends on what the target actually reveals in exploitable links. Lewin never mentions that the Flag Officers code was never read during the entire war, although it probably did contain the high level directions before Leyte.

~~(C)~~ The politics of wartime SIGINT in both Europe and the Pacific resulted from the basic fact that the traffic and the cryptanalysis had to be centralized in order to get enough related material to read the links. Inevitably, this gave the military and political people at the center of the war effort more information than the field commanders had, since they could control what was sent out. After some very dangerous compromises, including news stories identifying specific successes, Marshall and King put their personal authority into setting up and enforcing the stringent security that characterized all high level ULTRA COMINT. This not only protected the sources, but gave immense control to the two senior military commanders. In the field, security was much more uneven, for the Special Liason Units copied from the British were not welcomed in the Southwest Pacific where MacArthur sought to control all information flow. One byproduct of the secret SLU channels was a series of very frank reports by the SLU officers which came back to Washington without local censorship.

~~(TSC)~~ The most visible continuous COMINT success in which the intelligence was very well exploited was the merchant shipping traffic. Both Army and Navy cryptanalysts read the messages, and the conclusive success of the submarine war of attrition on unescorted merchant ships made the "island hopping" strategy feasible, and greatly reduced the cost of the war to the U.S. Other COMINT results were intermittent and scrappy until late in the war, when U.S. war production and the destruction of Japan's merchant navy had made the outcome inevitable. Lewin's extensive criticism of MacArthur seems to overlook the fact that a commander cannot be utterly trusting of the fragile and uncertain intelligence that codebreaking provided (or failed to provide) in the first half of the Pacific war. Because the lower level Japanese Army and Air Force nets used the same system of code plus additive, but did not send enough traffic to permit exploitation (so that it operated almost as one time pad), the detailed tactical information had to come from other sources. (The same was generally true in Europe). This lack of timely tactical intelligence, and the great difference between an operational order and the way it is carried out, created longstanding resistance by many operational commanders that devalued what COMINT there was.

~~(C)~~ Nimitz ranks high in Lewin's estimate as a commander and user of SIGINT, but the use of naval intelligence was inherently simpler than exploiting ground or air COMINT.

~~(S)~~ Except for Midway and the Coral Sea, COMINT gave little real help in the Pacific until 1943. The surprise at Pearl Harbor, the loss of the Phillipines, Singapore and Burma, and the unchallengable supremacy of the Japanese Navy until Midway show the ineffectiveness of American intelligence and also of Allied military forces. A point not illuminated is that Japanese military technology stood still from 1940, while U.S. weapons became much better, and with big advantages in quality and quantity, the U.S. was then able to make use of the COMINT it produced. Lewin never quite captures the inner environment of COMINT itself, and how it made itself the indispensable factor in Allied warfighting, because he deals primarily with the product, not the process. The fact that the intercepted traffic was sent by sea, or by aircraft at first, and often arrived months late, until major new radio teletype systems were put in place, is not mentioned, although this was a key factor in slow start against Japanese Army traffic. Another point missed was the role of Reischauer during 1943-45 in continuously interrupting the process oriented activities in Arlington Hall to snatch urgent intelligence from the rather inflexible assembly line of data processing. Reischauer, who held the rank of a G-2 Colonel, and his staff did the intelligence analysis from the raw decrypts inside Arlington Hall, rather than waiting for finished COMINT to arrive. Since less than ten percent of the mass of decrypts were actually useful for current intelligence, this highly informal plundering by a high ranking expert was essential to timeliness and correct selection.

~~(S)~~ The intense concern at high levels with security and secrecy, and the resistance and insubordination of the field commanders to these secrecy measures, is illuminated. The letter from Marshall to Dewey illustrates the fact that the success against the Japanese codes was the subject of national gossip, well outside Washington, all during the war. It is hard to imagine that the diplomats in Washington were not aware of these stories. The Americans were not only two years behind the British in defining doctrine about COMINT security that applied to operational commanders, but at Arlington Hall they had a massive turnover of staff because the clerical employees didn't like the work, and got other jobs. Interservice rivalry did provide some interest in secrecy, but it took several years and the imminent peril of losing their only reliable source of intelligence that invoked the imperious wartime diktats. In spite of this, literal decrypts found their way through

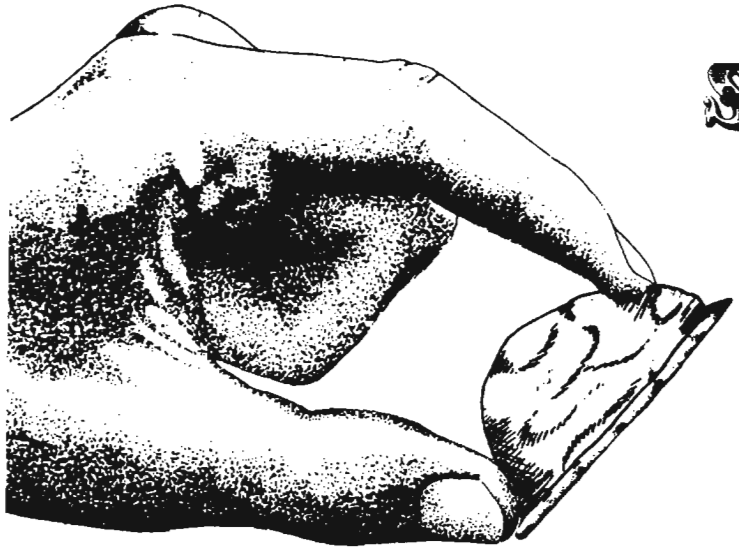
leaks and diplomatic channels into public media, revealing that specific Axis systems were being read. The military orders establishing security procedures apparently did not affect non-military elements.

~~(TSC)~~ Lewin repeats the well known stories of how all the German and Japanese messages about cipher security reported the conclusion that their crypto-security was beyond question, yet the fact is that the Germans knew Enigma was being read currently in 1943, correctly believed their Abwehr ciphers were being read in late 1941, and took numerous physical, personnel and cryptographic security measures to defeat enemy cryptanalysts, which were successful but too late to help them. The Japanese introduced a number of cipher and code changes on military and non military traffic, including the use of encipherment squares, but some of their changes were more insecure than the procedures they replaced. However, the changes were to the system, not just new crypto materials. The far flung Japanese had the special disadvantage of sending the cipher security changes over the radio links that were being read. Efforts to distribute new crypto materials to change the diplomatic and attaché ciphers were thwarted by Allied military action. These energetic and difficult cryptographic changes by the Axis indicate they were less complacent about cipher security than the self confident conclusions sent over the channels we were suspected of reading. It is probable that overall secrecy about COMINT successes was much less than the victors assume.

~~(TSC)~~ One of the most important points that Lewin seems to slight is the great difference in intelligence production from codes versus ciphers. The Japanese military and naval traffic was primarily in code, and when the books had to be recovered the intelligence was invariably much more scrappy and uncertain than with ciphers. Routine messages with little intelligence value would be the most completely decipherable, while non routine messages would contain mostly undefined groups for months. Recovered meanings change, e.g., today's Tokyo can become tomorrow's Yokohama, and this makes it impractical to exploit daily traffic without chaining backwards and forwards to other traffic. Of the huge volume of decrypts, less than ten percent was actually used for current intelligence. The bookbreaker was always the key person in the intelligence process, and the U.S., like the British, used professors of exceptional ability to get the combined problem of language, bookbreaking and intelligence analysis right. A codebook change was disastrous to intelligence continuity for weeks or months, unlike cipher machine key changes that gave up all their secrets, once solved. Captures were often the only way to make traffic currently exploitable, and they were planned and executed with murderous efficiency as the war progressed.

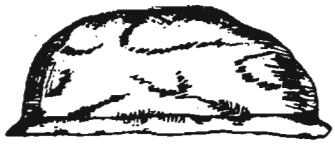
~~(TSC)~~ Whenever he can, Lewin points out the mistakes the Japanese made that allowed their systems to be broken and exploited. The difficulty of solving the attaché CORAL system is cited, with references to a 1981 letter from Raven. The importance of reencipherments and cribs in attacking PURPLE, and the crucial value of low level weather traffic in giving cribs into a high level system, are described. The fatal error of the messages giving successive ship noon positions, which allowed submarine ambush, is elucidated. Presumably Lewin wants to assure that no one will ever make those errors again. Declassification is probably the epitaph for future Naval COMINT.

(U) Summing up, Lewin's book is a readable but often specious commentary on the production and use of SIGINT against the Japanese. The classified and declassified official reports and histories written by both Americans and British during and after the war are better and more insightful. Lewin obviously applauds the American COMINT effort, but not being an insider he misses most of the color and "war stories" and contingent detail that would convey the intense commitment, rivalry and sense of mastery that were central to the success. Enjoy it, then seek out the real thing.



SHELL GAME (U)

W. E. S.



One of the more useful features about UNIX is the shell, which permits one to put together a file of commands and then execute them simply by naming the file. It is easy to use, and easy to change. Once the file is made (normally using the Rand or screen editor), the mode of the file is changed to make it executable (using the command chmod), or one simply types:

sh filename

and whatever commands are in the file called filename are executed, in whatever order they appear in the file.

In my early days of learning about UNIX, I learned more about it by prowling around through other people's shell files than by any other method. We have begun to get security conscious on the various systems, and so it is harder to poke through other people's directories and files. Nevertheless, it is still instructive to look over other people's shoulders. Therefore, we propose to set up an irregular feature called Shell Game, showcasing various shell files that actually work. (At the present time, it is probably a good idea to limit exhibits to Version 6 UNIX, since that is the most common version now being used here.) To begin the series, we offer two simple shell files.

CLEANUP is used to 'housekeep' by throwing away the many '.bak' files that tend to accumulate when one uses the Rand editor a lot. The name of the file is in capital letters, so that it comes at the head of the list when I type ls -l to look at my filenames. The file looks like this:

```
find /u2/wes -name "*.bak" -a -exec rm {} ";"
cp /dev/null /u2/wes/CLEAN.last
```

It contains only two lines. The first line uses the UNIX command find in the following way:

- find
  - UNIX command
- /u2/wes
  - tells the system where to start looking, i.e., begin here and work downward,
  - my directory is in filesystem u2, and my username is wes
- -name "*.bak"
  - look for any file whose name ends with .bak
- -a
  - and
- -exec rm {} ";"
  - execute the UNIX command rm (remove) to whatever is found.

The second line makes a copy of a system file called /dev/null, and names the new file /u2/wes/CLEAN.last.

The system file /dev/null is sometimes called "the bitbucket" because it is always empty. You can send an output to /dev/null and, in effect, throw the output away. Or, as in this shell, you can create an empty file. The empty file CLEAN.last is used as a place to record the time you last executed CLEANUP. When you type in ls -l one of the top lines should look something like this:

```
-rw-rw-rw- 1 wes      0 Mar  1 17:39 CLEAN.last
```

which would show you the date and time of the last CLEANUP.

The second file is called (in my directory) names. (You can, of course call it whatever you want in your directory.) Its purpose is to bring up to the screen the full names of anyone currently working on the system. It looks like this:

```
who
who | reform +t8 | rpl "^" "name " | sh
```

This shell was built to use as part of a demonstration of UNIX capabilities. The UNIX command who gives a display something like this:

```
lct      ttyj Mar  4 08:16
rsh      ttyG Mar  4 08:31
norm     ttyK Mar  4 08:52
sue      ttyL Mar  4 10:02
wes      ttyX Mar  4 08:10
```

The UNIX command name takes up to nine usernames and returns the full names of the users. For example,

```
name dlr wes
```

might return the following:

```
dlr     P14
wes     P14
```

The first line of the shell file simply sends the result of the 'who' command to the screen, in the usual way. The second line sends the output of the command 'who' through a pipe (|) to become the input of the command 'reform', which throws away (truncates) everything after the 8th position on each line.

The output of the 'reform' command is piped to become the input for the 'rpl' or replace command. Here the 'rpl' is used to insert the five characters "name " (including the space) at the beginning of the line. Although it won't make any difference in this example, the 'rpl' usually throws away any trailing blanks, i.e., any blanks at the end of the line - in this case, all blanks from the end of the username out to the 8th position.

Once more the output is piped, this time to the command 'sh' (UNIX shell). The input to 'sh' looks something like this:

```
name lct
name rsh
name norm
name sue
name wes
```

The command 'sh' will cause each line to be executed in turn, and since no output direction is indicated (i.e., no > is given), the output will come back to the screen.

One of the reasons for getting the output of 'who' onto the screen first is that 'name' is a bit uncritical: it takes the string of characters in the user name, and brings back any line containing that same string. For example, the command

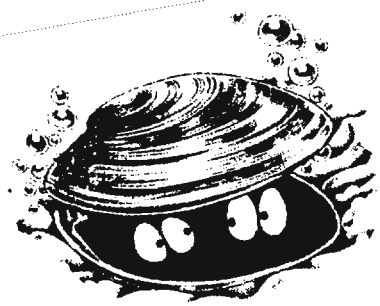
```
name wes
```

might bring back

```
wes     P14
 drl    Z43
```

one of which is the one we want.

P.L. 86-36



WORD PROCESSING IN A4(U)

by [redacted] A41

P.L. 86-36

The author wishes to thank [redacted] Without her encouragement and generous help, this article would certainly not have been written.

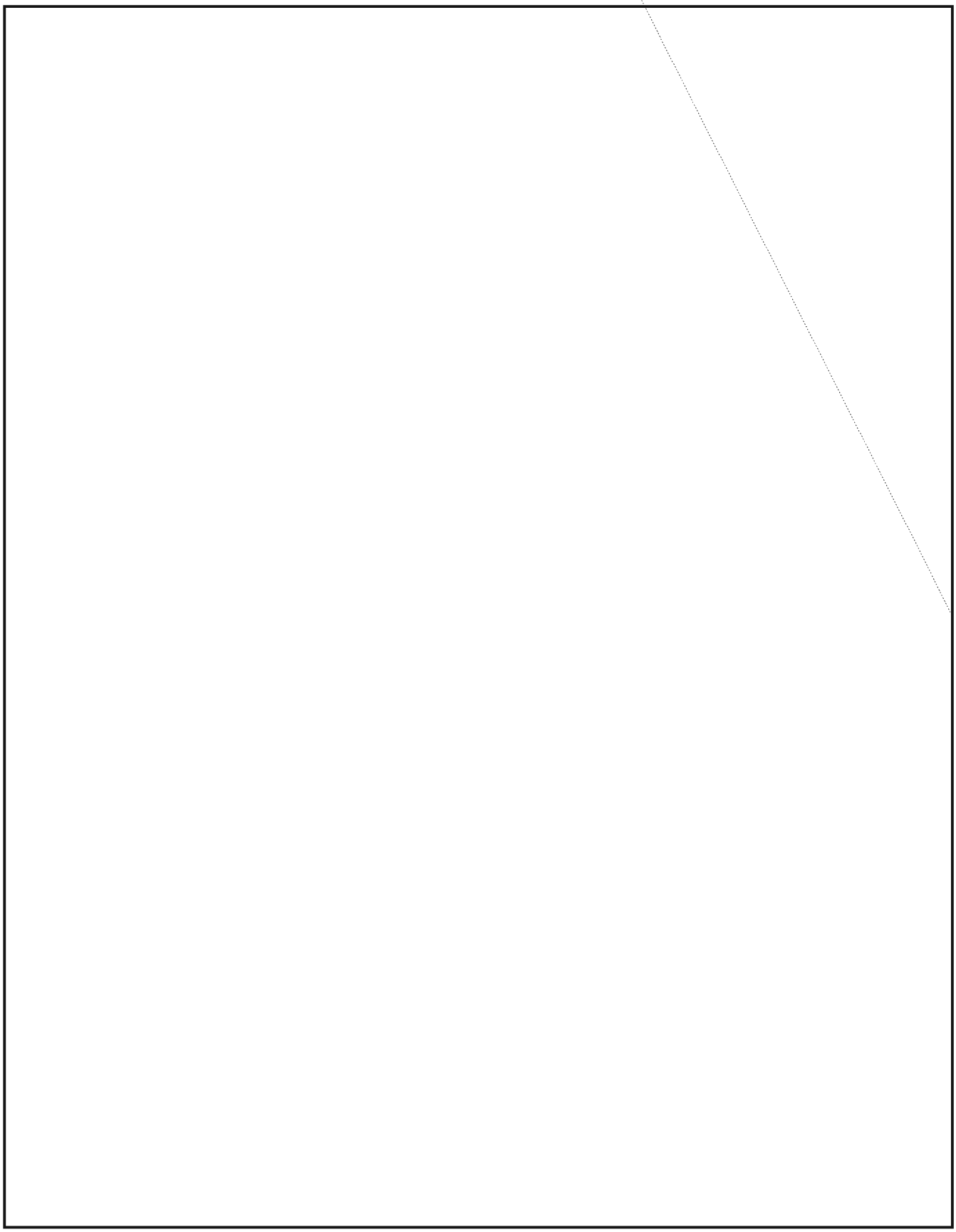
This report describes a study of document production by A41 personnel. Its purpose was to provide a basis for planning office automation ~~(FOUO)~~ efforts in A41, and the findings have been extended by extrapolation to cover all of A4.

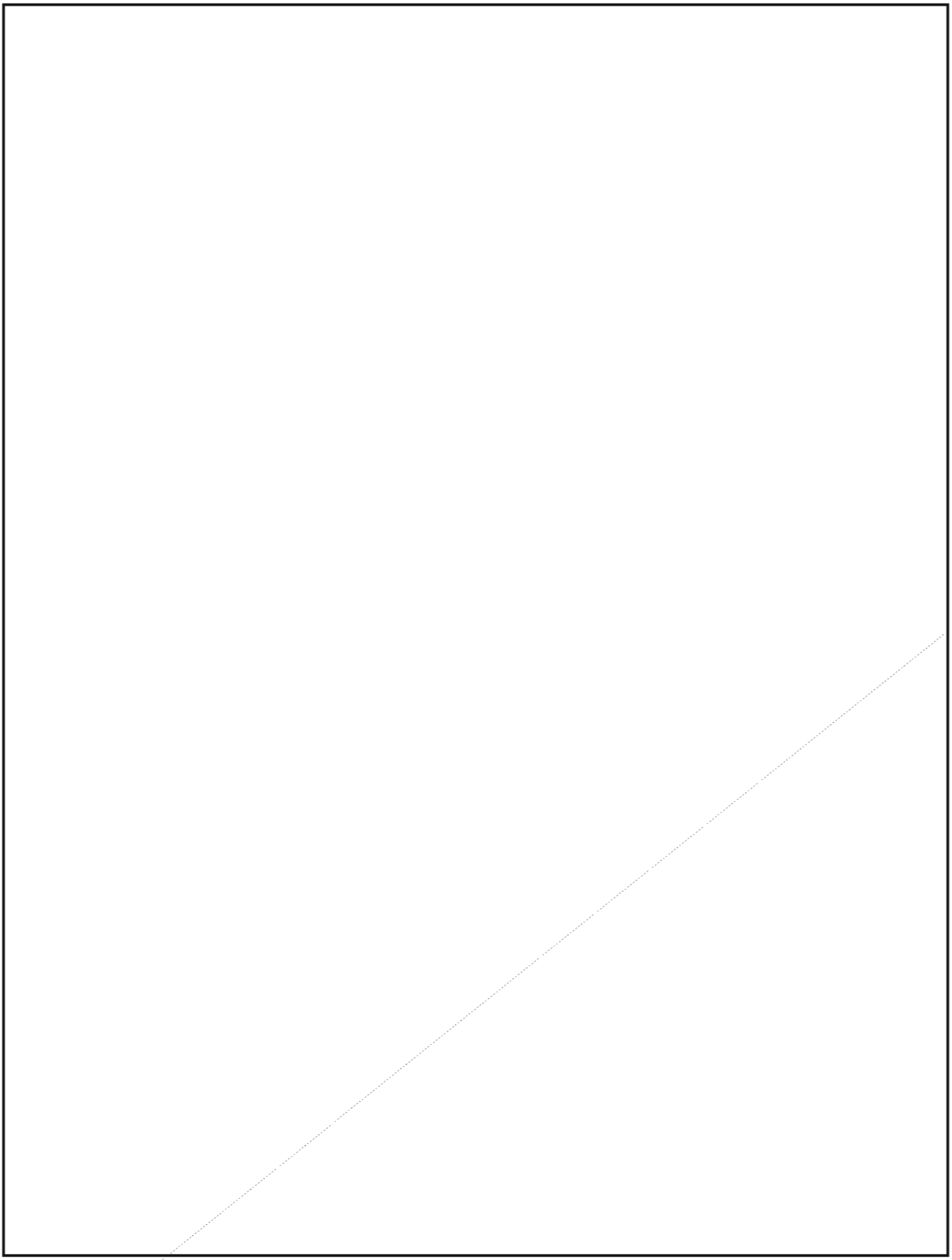
~~(C)~~ The results to be presented here relate directly to "putting words on paper," an activity which represents about one quarter of A41's productivity baseline. Document production was selected for initial study because it offers the simplest and most direct opportunity to improve productivity in an immediate time-frame.

[redacted]

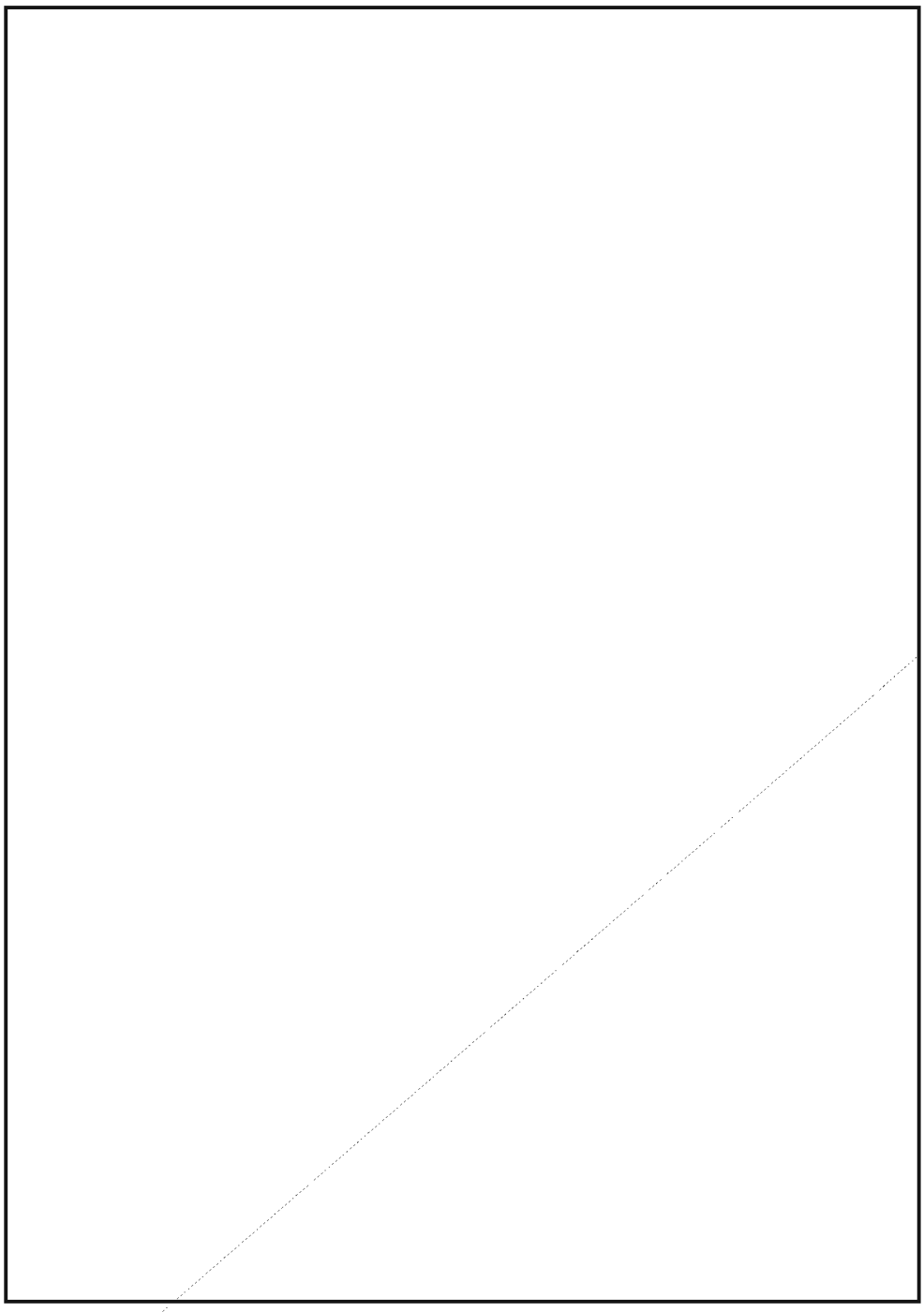
[redacted]

EO 1.4.(c)
P.L. 86-36





EO 1.4.(c)
P.L. 86-36



EO 1.4.(c)
P.L. 86-36

A4 WORD-PROCESSING REQUIREMENTS (U)

(U) The findings in this report were developed by extrapolation from the results of a survey of document production in A41 (above), supplemented by other estimates and computations. This summary was prepared in support of a request for word-processing equipment for A4. The data were collated and organized for use in documentation required by T443, entitled "Word Processing Requirements Workload and Resource Summary (Feasibility)".

[redacted]

[redacted]

(S) CURRENT DOCUMENT PRODUCTION RESOURCES AND COSTS. Full-time typists in A4 use automatic equipment for 50% of their document production and manual equipment for the other 50%. They do not use any overtime hours. Author/word generators spend 24.2% of their work hours in document production (10.1% in preparation, 1.4% in proofreading, and 12.7% in typing). They require 540 hours of overtime quarterly. Current cost of electric

[redacted]

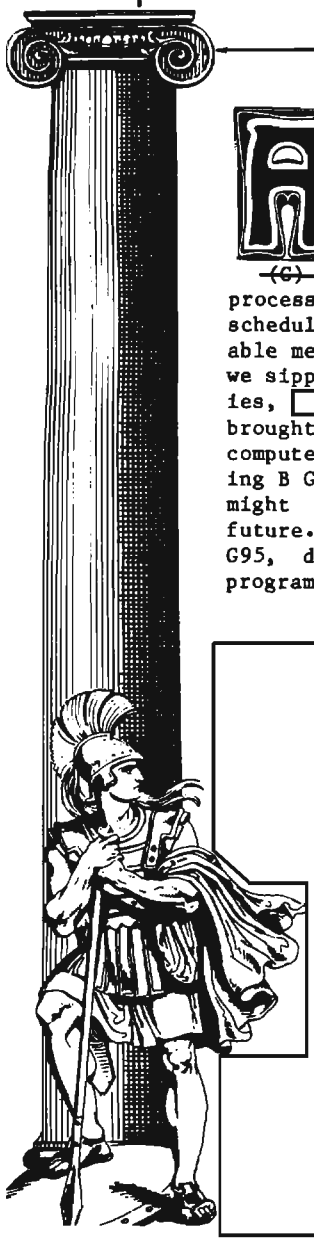
P.L. 86-36
EO 1.4.(c)

[redacted]

REFERENCE

1. "Guidance on Requirements Analysis for Office Automation Systems," NBS Special Publication 500-72, National Bureau of Standards, December 1980

BOOKBREAKERS' FORUM ON MACHINE AIDS



P.L. 86-36

[redacted] **P16**

A funny thing happened on the way to the Forum ... [redacted] USA, was waylaid ~~(C)~~ in the mustering-out process and didn't make it as scheduled. But we had a profitable meeting nevertheless. While we sipped tea and munched cookies, [redacted] Chief P13, brought us up to date on personal computers and how they are helping B Group analysts, and what we might look forward to in the future. [redacted] G95, described the bookbreaking programs he wrote on [redacted]

[redacted]

[redacted]

(U) [redacted] told us about a software package P13 bought which has been successfully applied to administrative files in P15 and B6. For details, call [redacted] on 3045s.

P.L. 86-36

~~(C)~~ Down the pike, Gene tells us, are very powerful personal computers which will allow bookbreaking to be done on all but the biggest codes. It's way off, so don't hold up work on a going problem waiting for it.

[redacted]

P.L. 86-36
EO 1.4.(c)

~~CONFIDENTIAL~~

[redacted]

~~(C)~~ Moving? Cleaning out?

Give your old code materials a good home. You can send them, including codebooks, runs, sample messages, write-ups, mag tapes, punched, cards, etc., to:

[redacted] T54, SAB 2 Door 3, 2268s,

or

[redacted] P16, 8A187, 1103s.

~~(C)~~ Notice to [redacted] users:

In mid-1983 RYE will be deactivated. That means that you will have to find some other means for processing your code messages. You really ought to start right now looking for a replacement program. If you wait too long, you may find that the plug has already been pulled, and that all your data is lost, including the codebook used for decoding the messages, and all your message files. I'll be glad to help you find an alternative way, if your support people don't have something that can be implemented in good time. The chances are very good that in some other area there's an operational program that can be adapted to your needs.

[redacted]
P16 x1103s

P.L. 86-36

Personal Computer Application (U)

P.L. 86-36

[redacted]

P13

One aspect of P13's mission is to investigate the use of personal computers for cryptanalysis and related functions. We make known the availability of these devices, show how they are being used in operational environments, and provide some ideas as to their future use. We provide demonstrations in conjunction with organizations such as the Bookbreaker's Forum, we participate in courses such as CA305, and we offer personal demonstrations for interested individuals or offices. These demonstrations provide us with the opportunity to show interested people a wide range of operational uses for personal computers at NSA. We demonstrate in house, custom built software applicable to specific cryptanalytic problems or to a wide variety of cryptanalytic problems, some potential uses for personal computers as cipher devices, and a wide variety of inexpensive, commercially available software encompassing managerial tools, data base management systems, and word processing.

~~(FOUO)~~ A problem recently presented to us was that of converting Universal Transverse Mercator grid coordinates to latitude and longitude. With the cooperation of the sponsoring organization and a good deal of investigation into past efforts in this area a program, written for the Radio Shack TRS 80 Model III, was produced for use with an operational problem in DDO. This program converts UTM coordinates to latitude and longitude for [redacted]

~~(FOUO)~~ A paper entitled "Conversion of Universal Transverse Mercator Grid Coordinates to Latitude and Longitude" has been published as P1 Informal Number 1, March 1982, #S-223,678 and is available to interested individuals or organizations.

~~CONFIDENTIAL~~

SOLUTION TO LAST MONTH'S

CRYPTIC CROSSWORD

ACROSS

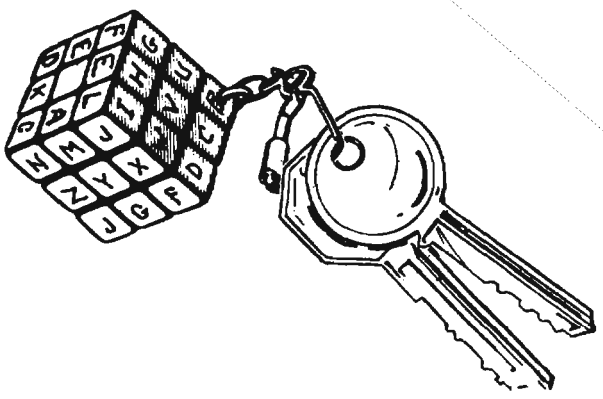
1. TRUMPET VINES
9. SECRETIVE (anag.)
10. GAUNT (gauntlet - let)
11. EMETIC (Believe me tick)
12. GATEPOST (anag.)
13. SULTAN (consult a nautical)
15. REPAIRED (rep + aired)
18. PIONEERS (pIONeers)
19. AGATHA (aGAThа)
21. REAPPEARS (reapPEARS)
23. IN A NET (anag.)
26. ELDER (el + der)
27. GLUTINOUS (anag.)

DOWN

1. TASTERS (t + asters)
2. UNCLE (double definition)
3. PREDICATE (pREDICate)
4. TWIN (t[o]win)
5. ICE WATER (anag.)
6. EAGLE (glee anag. + a)
7. AUTOCRAT (auto + car anag. + t)
8. STATED (sTATEd)
14. LEOPARDS (anag.)
16. ARGENTINA (a rain anag. + gent)
17. TRIANGLE (pun: try + angle)
18. PORTER (anag.)
20. ATTESTS (at + tests)
22. PERON (tipper once)
24. NAOMI (main anag. + o)
25. RUED (pun: rude)

SOLUTION TO 'A TOY PROBLEM'

[redacted] G9



OVERHEARD WHILE STANDING IN THE BURN-BAG LINE

"I heard a guy speaking in a briefing the other day -- and if he had been Pinocchio, he would never have gotten out of that room!"

"I haven't even thought about where. Who would ever want to eat a street map?"

HUMAN FACTORS

Have you noticed the articles and reviews about various aspects of Human Factors by [redacted] in recent issues of CRYPTOLOG? Does the subject interest you? Did you know that there is a lot going on in this field? Conferences, courses of study, publications, and societies, including a Special Interest Group of CISI: all these are active in the field of Human Factors.

If you want to know what is going on, you ought to subscribe to the Human Factors Letter, published by the Human Factors SIG of CISI. How? Call its editor, [redacted] on x8845s.

P.L. 86-36

~~TOP SECRET~~