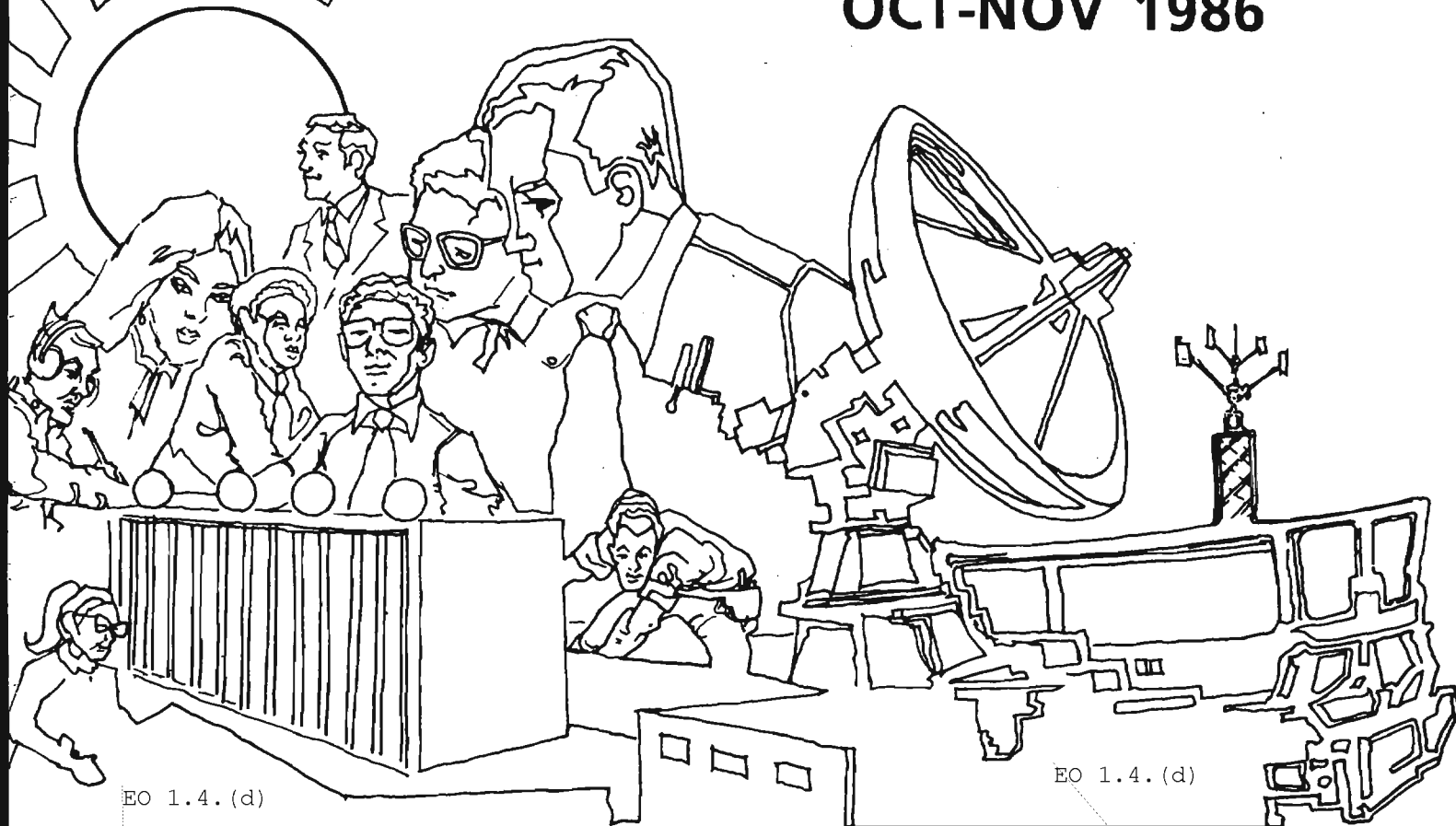


**NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND**

CRYPTOLOG

OCT-NOV 1986



EO 1.4.(d)

EO 1.4.(d)

[REDACTED]	[REDACTED]1
A NEW KIND OF JAPANESE (U)	[REDACTED]9
SIREN No. 5 (U)	[REDACTED]12
A SUMMER LANGUAGE COURSE (U)	[REDACTED]13
ON THE LIGHTER SIDE (U)	[REDACTED]15
THE REPRESENTATION OF PREFIXES	[REDACTED]16
CONFERENCE REPORT (U)	N.C. Gerson17
TECHNICAL LITERATURE REVIEW (U)	[REDACTED]19
SOFTWARE REVIEW (U)	[REDACTED]23
BULLETIN BOARD (U)	[REDACTED]8, 14, 22
LETTERS (U)	[REDACTED]27
FROM THE PAST	[REDACTED]31
RESULTS OF READERS' SURVEY (U)	[REDACTED]32
PUZZLE (U)	[REDACTED]33

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL NOT RELEASABLE TO CONTRACTORS~~

~~TOP SECRET~~

P.L. 86-36

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 10-11 October-November 1986

PUBLISHER [redacted]

BOARD OF EDITORS

- Editor [redacted] (963-1103)
- Collection [redacted] (963-5877)
- Computer Systems [redacted] (963-1103)
- Cryptanalysis [redacted] (963-5238)
- Cryptolinguistics [redacted] (963-1596)
- Index [redacted] (963-5292)
- Information Science [redacted] (972-2268)
- Information Security George F. Jelen (859-1211b)
- Intelligence Research [redacted] (963-3845)
- Language [redacted] (963-3057)
- Mathematics [redacted] (963-5566)
- Puzzles [redacted] (963-6430)
- Science and Technology [redacted] (968-8075)
- Special Research Vera R. Filby (968-8014)
- Traffic Analysis Robert J. Hanyok (963-5734)

Illustrators [redacted] (963-3057)
..... [redacted] (963-6211)

SHARE THE WEALTH! (U)

Even in the best of times, not everyone who could profit from it has been able to go to conferences. Partly it's because there's never that much money. But it's also because we can't shut down a whole operation for a conference -- someone has to mind the store.

Nowadays money is very tight. So people who are lucky enough to get to go to a conference ought to share the wealth, and write it up for CRYPTOLOG in addition to the customary trip report.

Why write it up again, when you can specify the distribution of each trip report and reach the right people? Because the probability is very great that there are people who should be informed that you don't know about. The Agency has gotten very large, and a good number of employees going to conferences haven't been around long enough to have a feel for who might be doing what. Also, our endeavors are becoming more complex and interdisciplinary, and the logical distribution may miss some key projects that are related. Only the fictional Mycroft Holmes could keep on top of things all by himself!

So, write it up for CRYPTOLOG, and increase the probability that your trip reports reach the people who would benefit. And the chances are that you'll get something out of it too -- making connections with people on similar projects or with like concerns.



To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

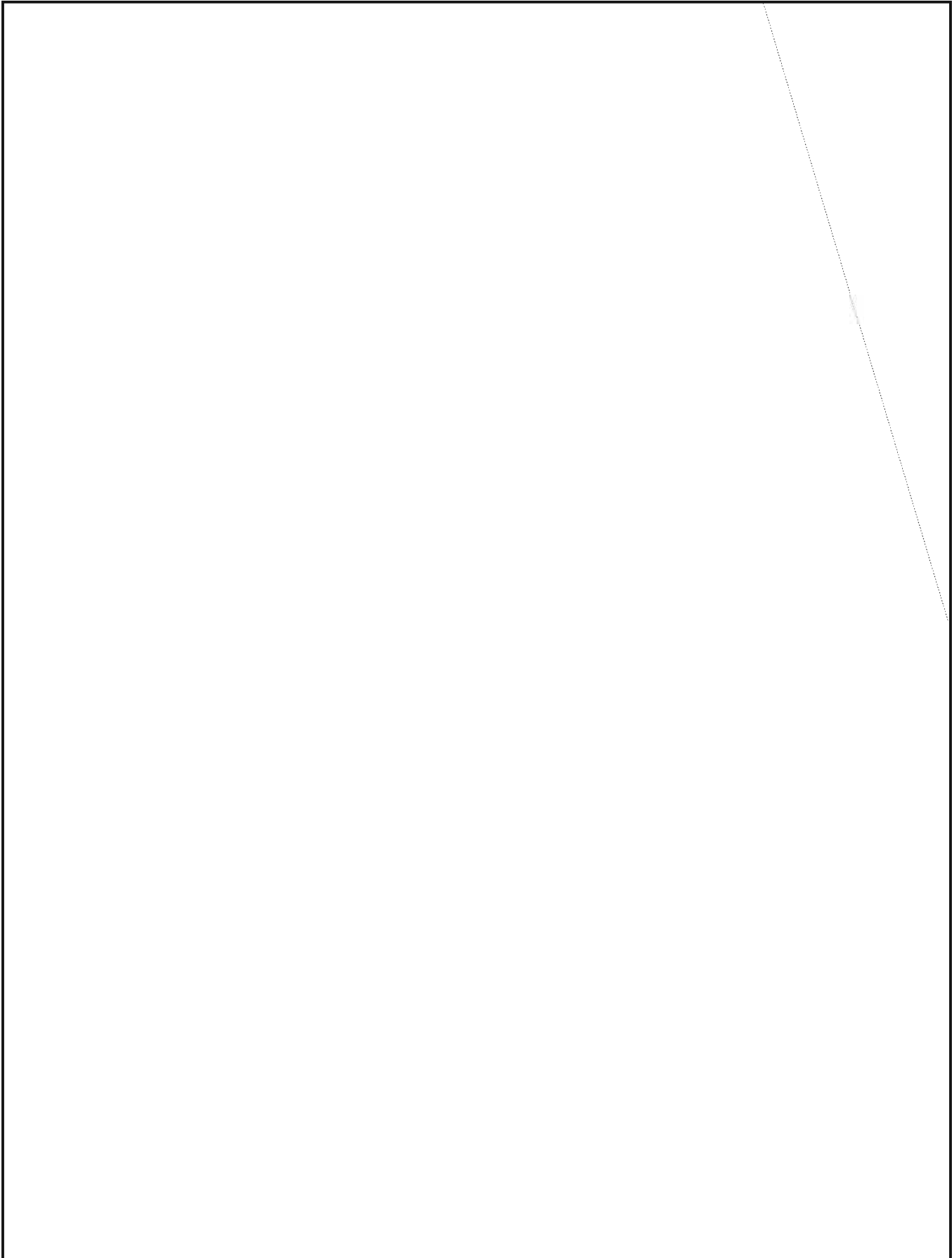
For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1
Please do not phone.

■ CORRECTIONS ■

- The caveat **NO CONTRACT** should be placed on the covers of the Aug-Sep 1986 issue.
- The article titled "Collection Management" in the same issue should be classified **CONFIDENTIAL** rather than **CONFIDENTIAL CCO**.

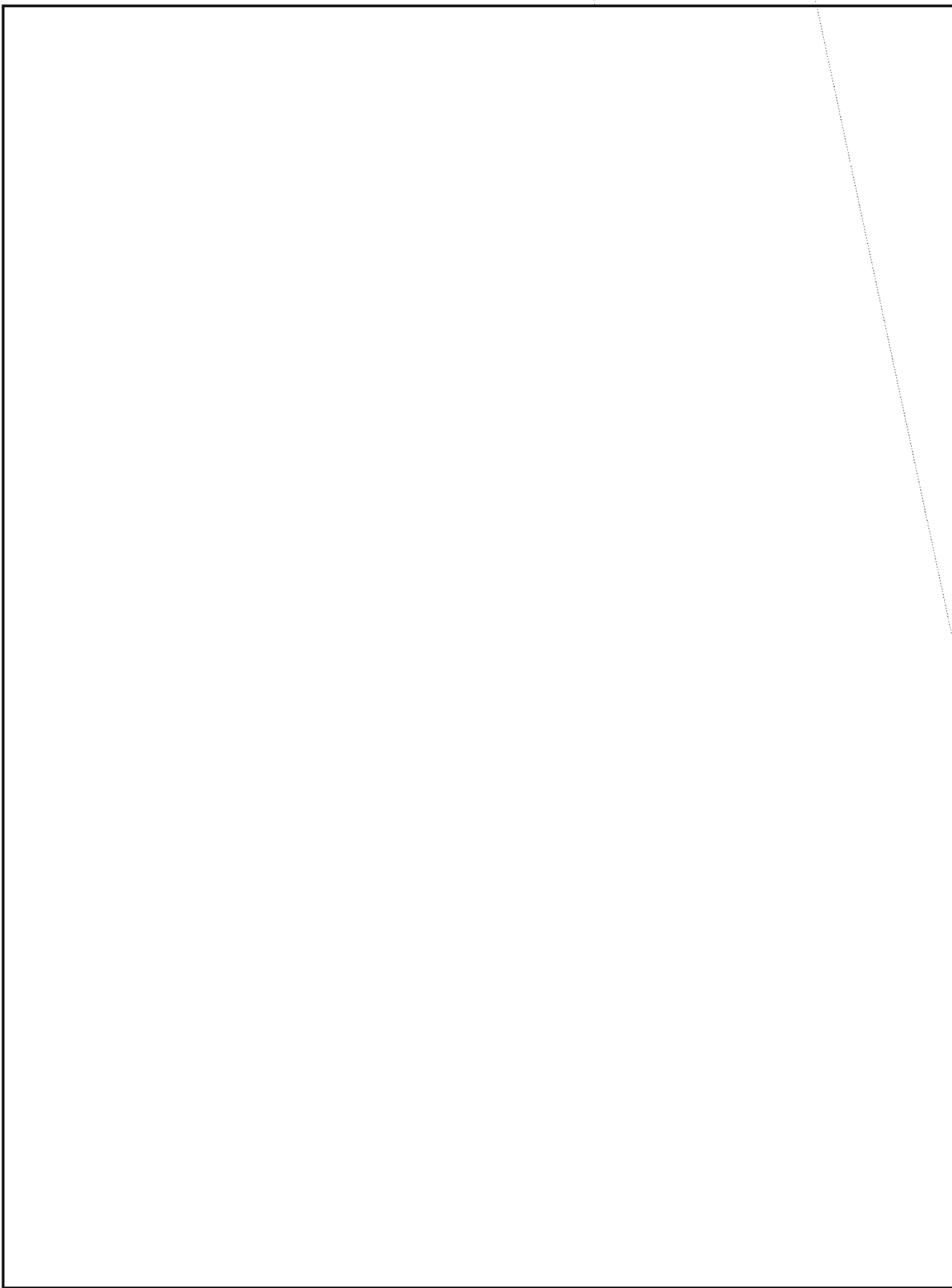
Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

~~SECRET SPOKE~~



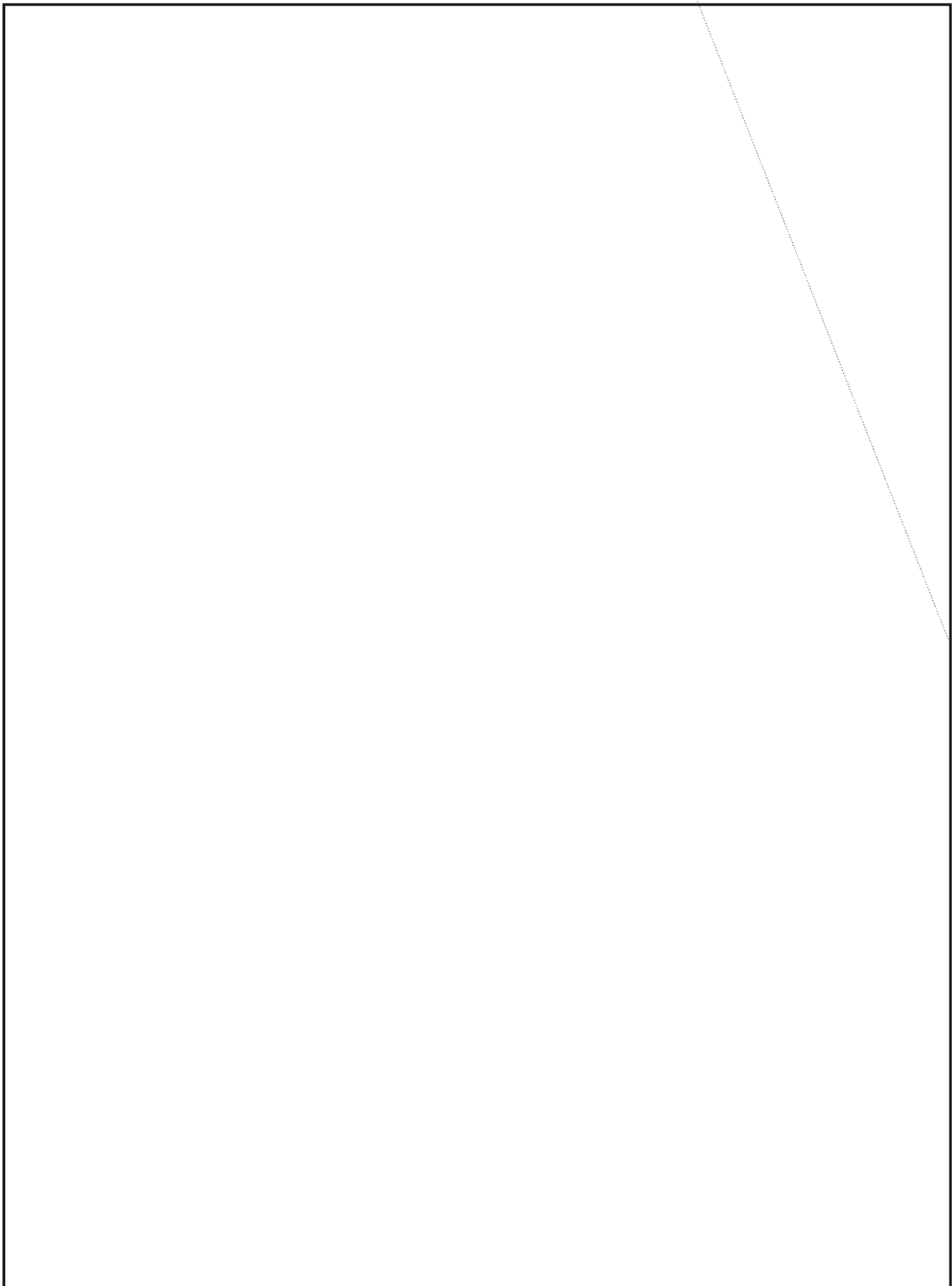
~~SECRET SPOKE~~

~~SECRET SPOKE~~



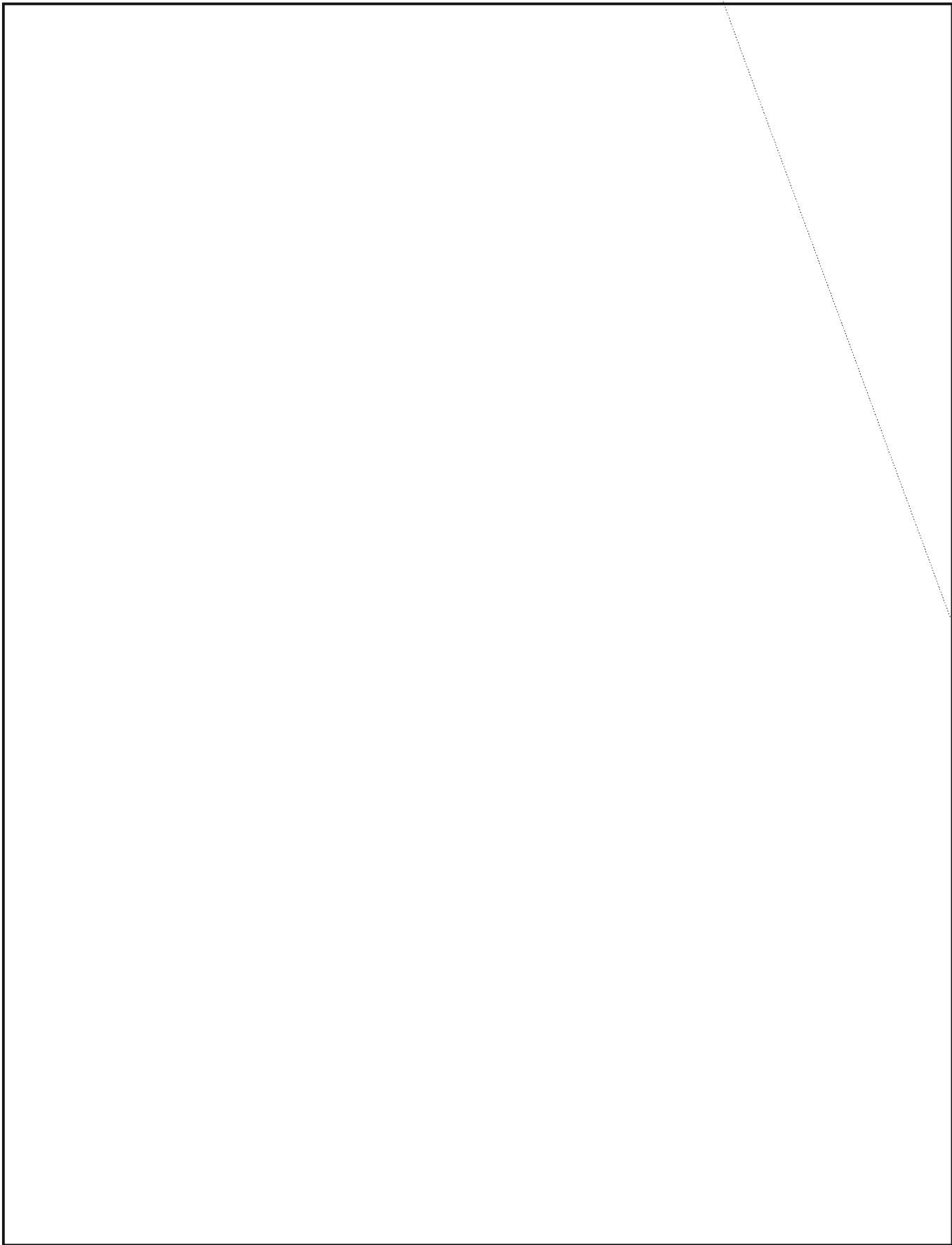
~~SECRET SPOKE~~

~~SECRET SPOKE~~



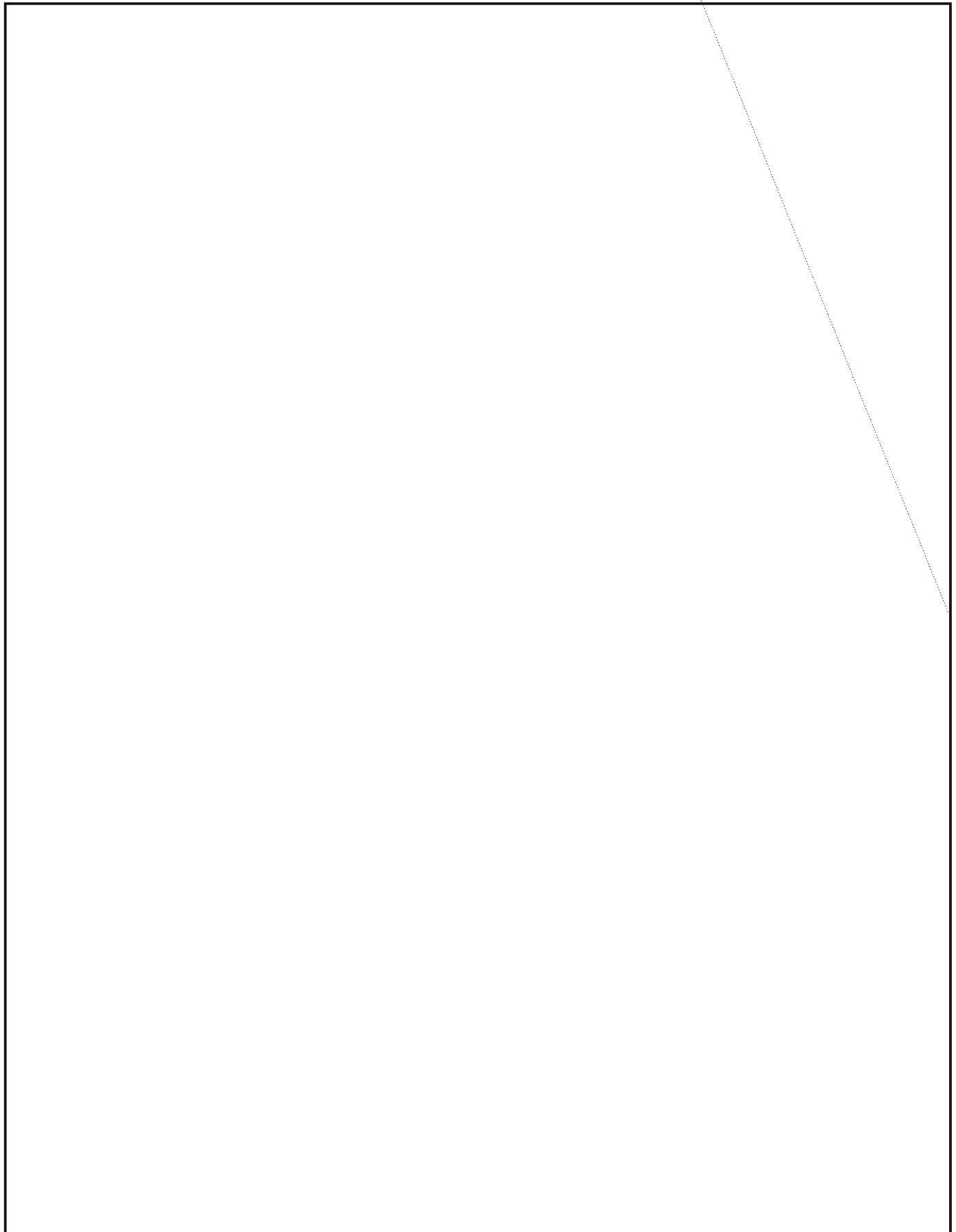
~~SECRET SPOKE~~

~~SECRET SPOKE~~



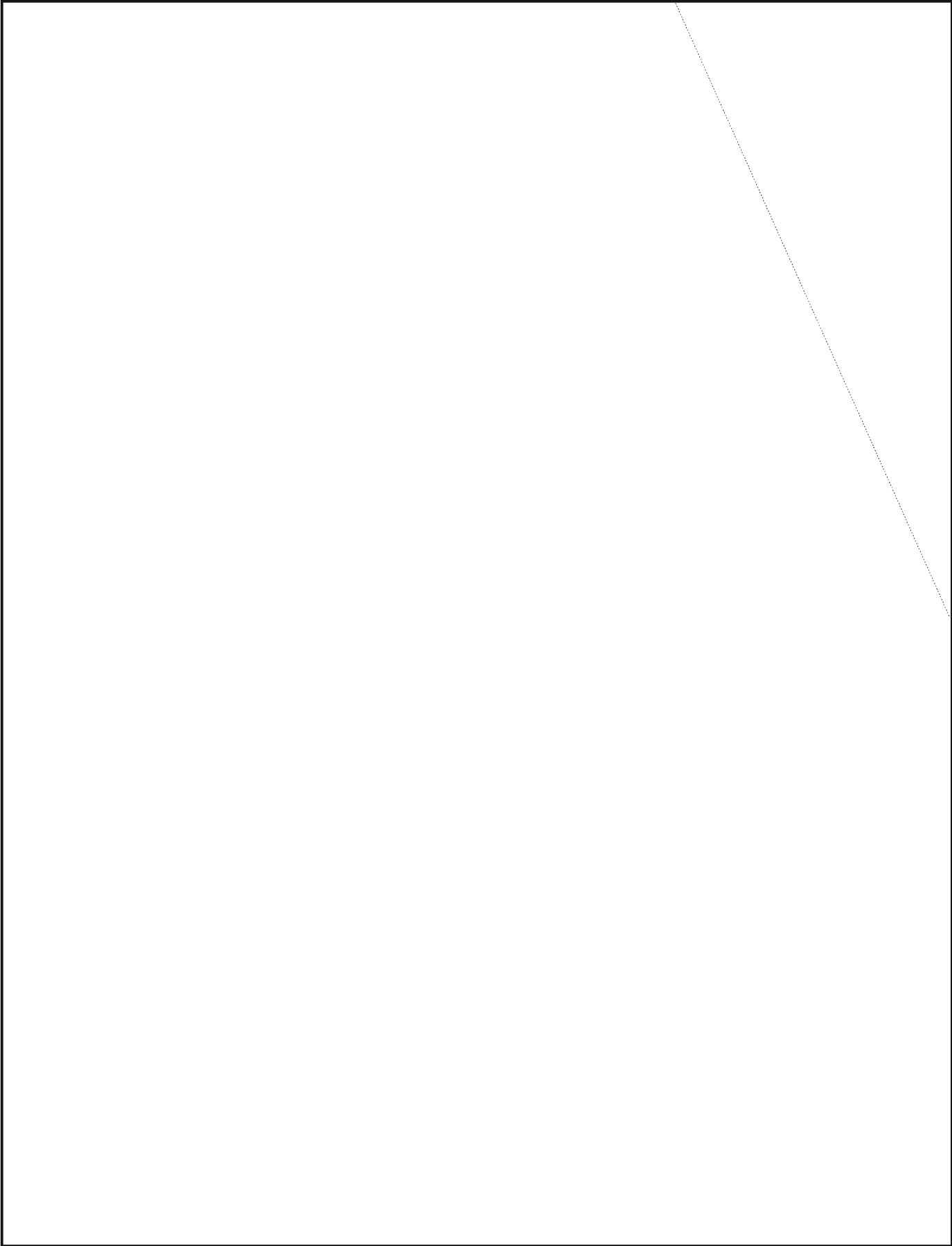
~~SECRET SPOKE~~

~~SECRET SPOKE~~



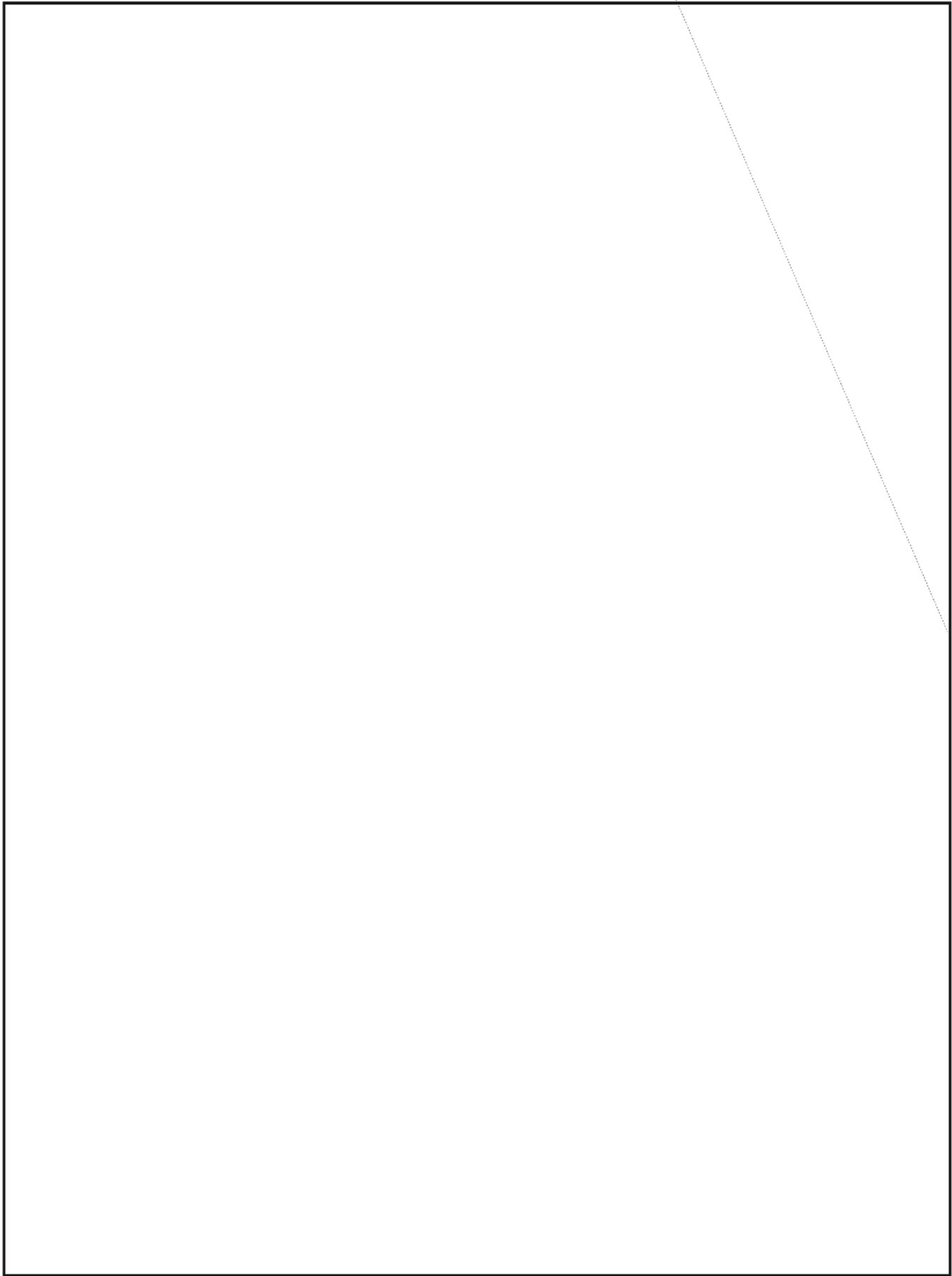
~~SECRET SPOKE~~

~~SECRET SPOKE~~



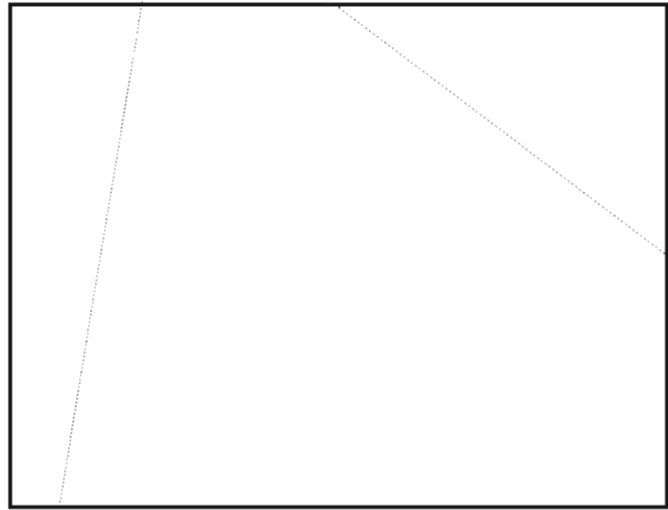
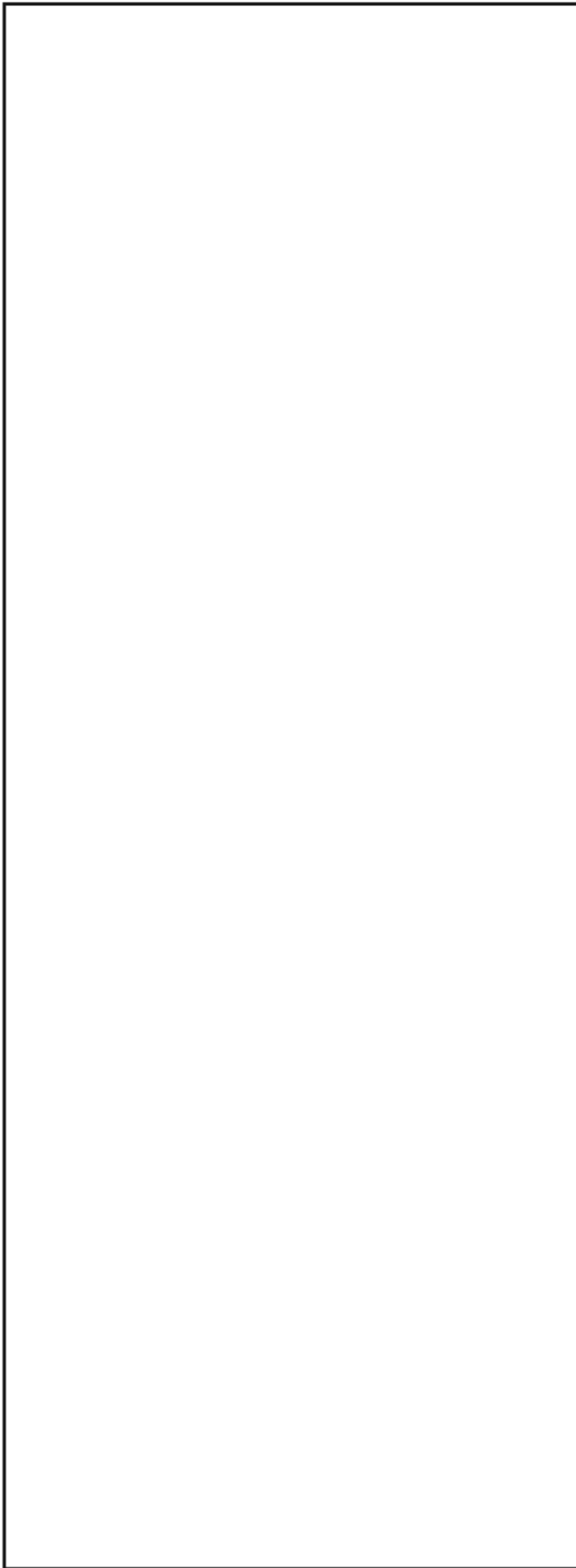
~~SECRET SPOKE~~

~~SECRET SPOKE~~



~~SECRET SPOKE~~

~~SECRET SPOKE~~



BULLETIN BOARD

DATA CONVERSION (U)

~~(FOUO)~~ The Data Conversion Center, formerly known as JOBBER, can convert your hard copy to machine-readable form using an optical scanner or a keyboard. At the same location, the Magnetic Media Conversion Center can also, in most cases, convert data from one machine-readable form to another. For information about specific conversion pairs call

T1431, 963-4777.

FORMATION OF HP3000 USERS' GROUP (U)

(U) In response to many requests an NSA Users' Group for the HP-3000 is being formed. Programmers as well as end users are invited to join. For information please call

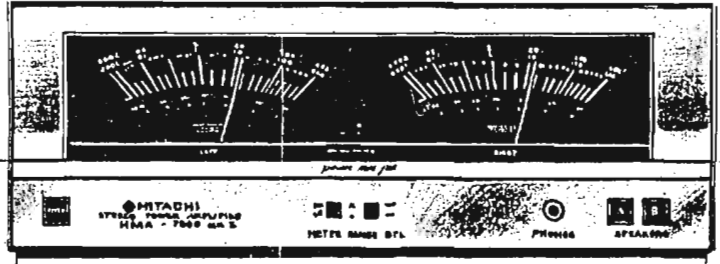
T2136, 968-8748.

P.L. 86-36



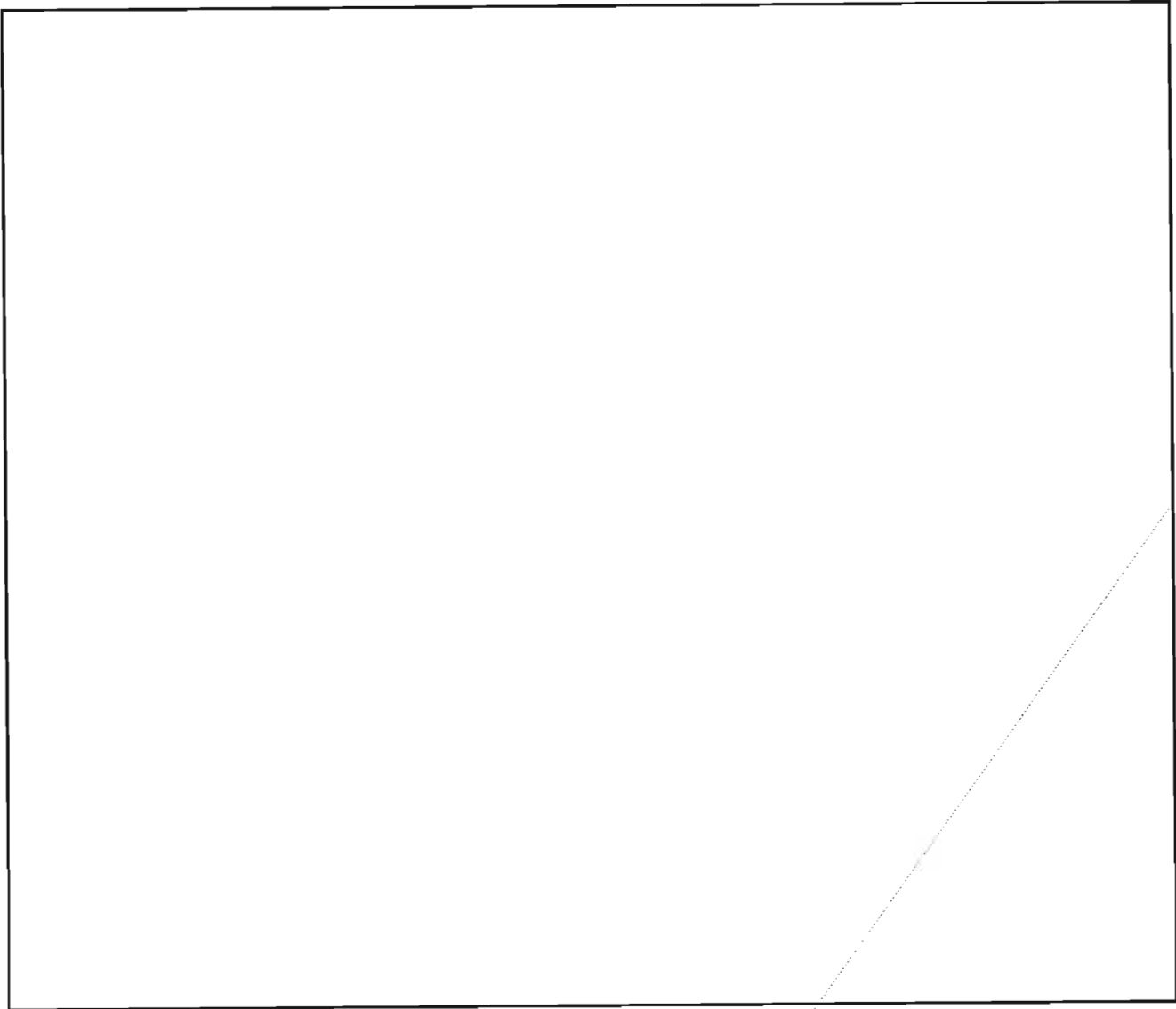
~~SECRET SPOKE~~

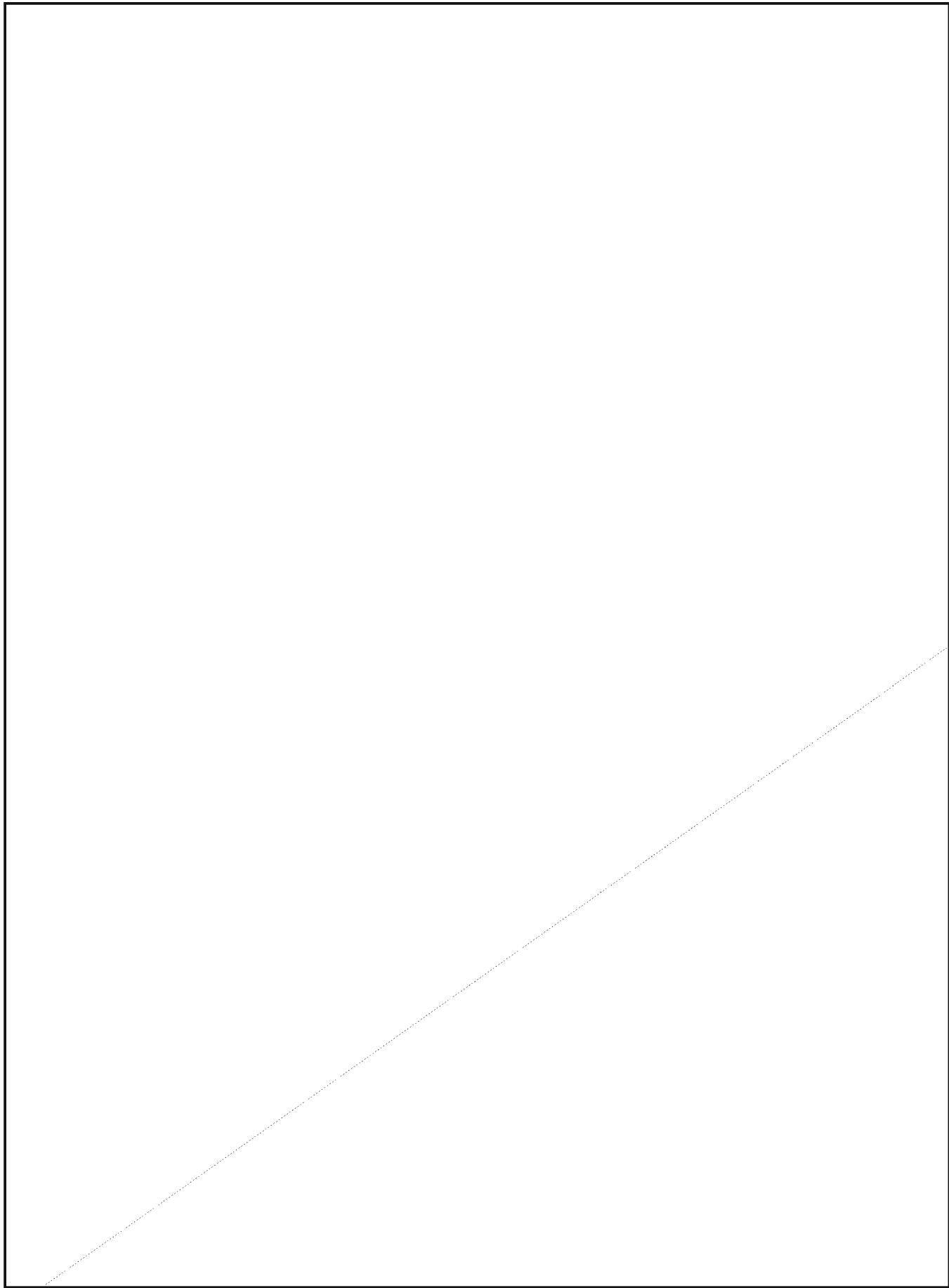
A NEW KIND OF JAPANESE (U)

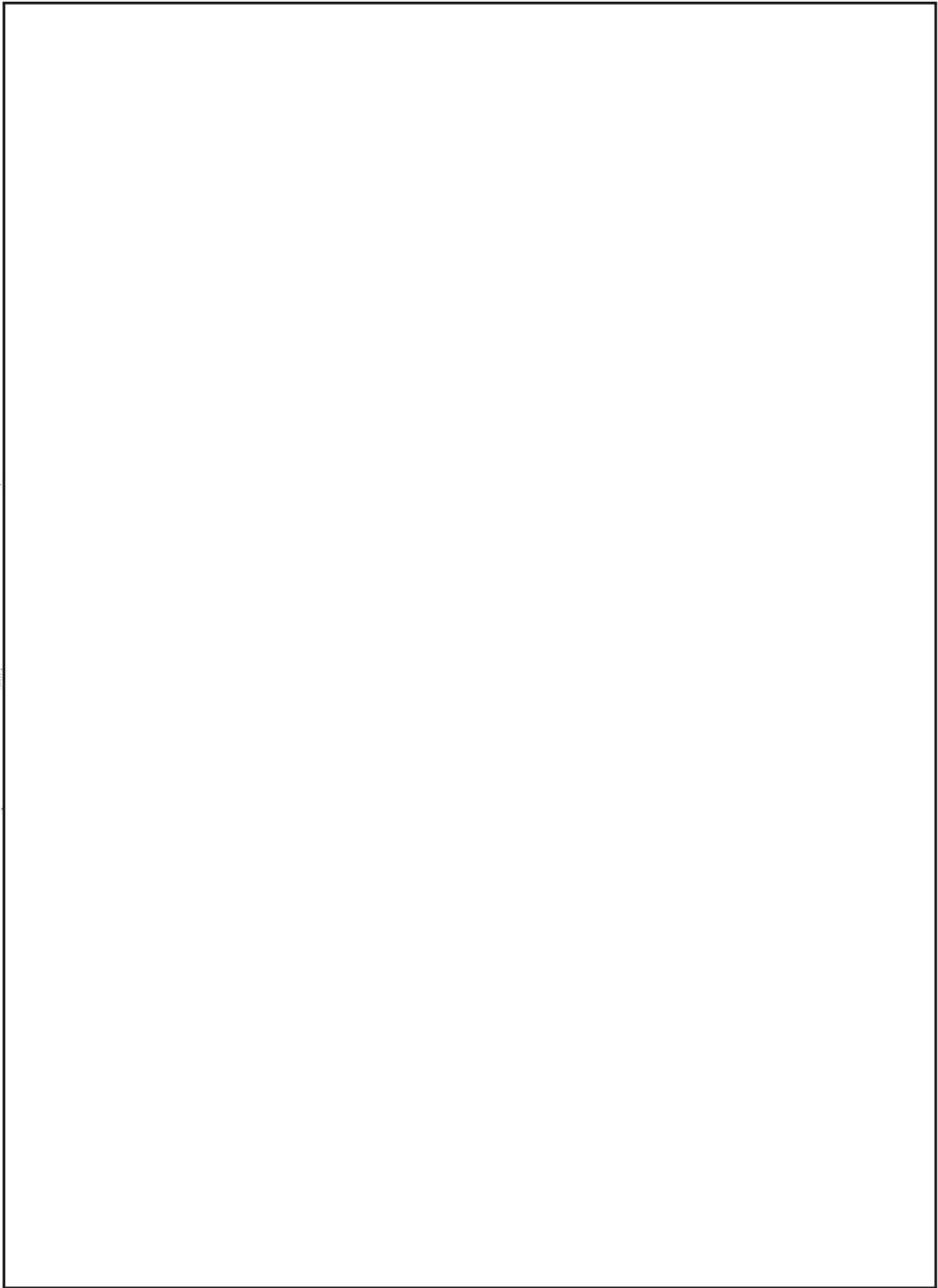


P.L. 86-36

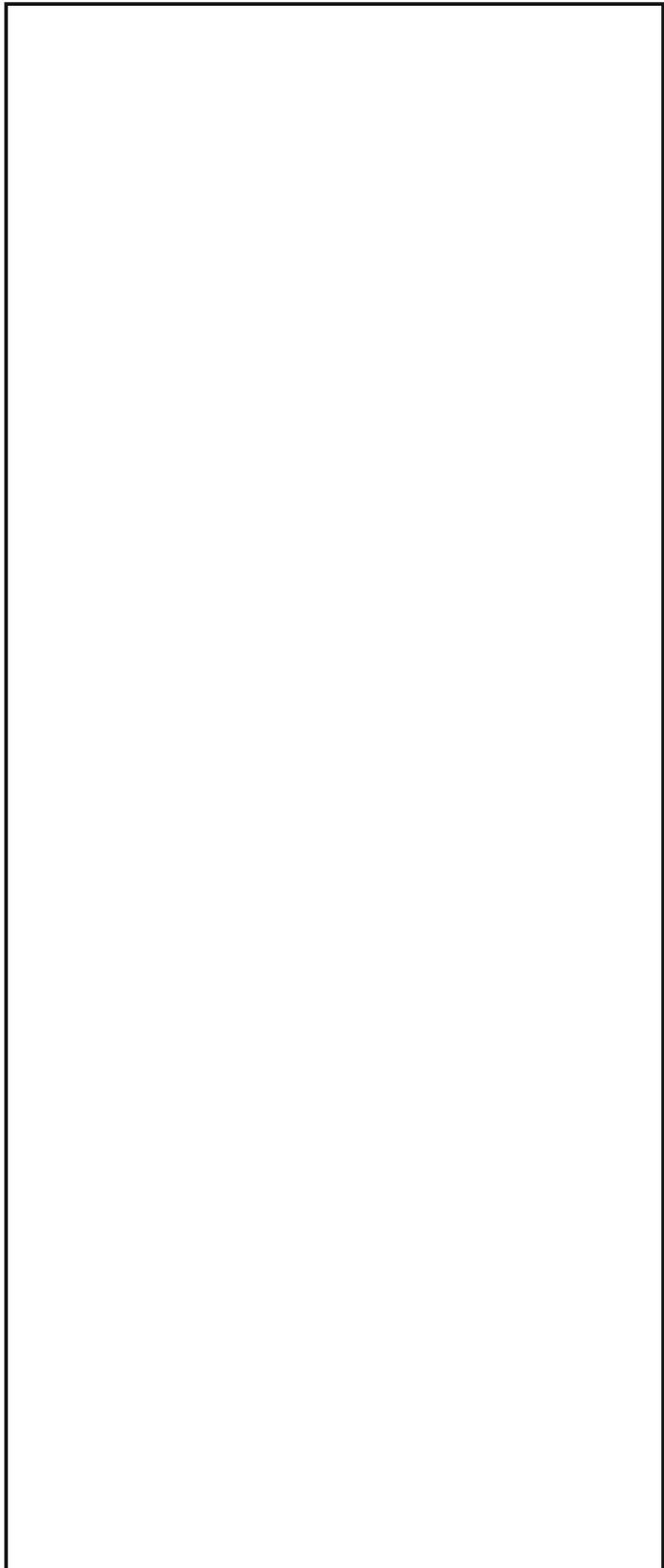
[Redacted] G72







~~SECRET~~



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

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

A SUMMER LANGUAGE COURSE (U)



P.L. 86-36

(U) I have just returned from a great experience. I was at the Indiana University campus in Bloomington in an intensive Chinese language program. It was a fantastic two months.

~~(FOUO)~~ The opportunity came about rather suddenly in May while I was working as a clerical assistant in B61. I came to the agency as a Senior Clerical Assistant in 1985, but with a desire to get into a language program. It did not take long. In the second week of May a memo came into the office about an intensive East Asian Summer Language program being offered in Indiana. I knew this was exactly what I was looking for. I thought my chances were slim, but after talking to the chief and the deputy chief of my division, I decided to submit my name. After about two weeks I was told that there was a very good possibility that I would be able to go. During the last week of May I was informed that I was going to Indiana to begin an intensive Chinese language course on June 13.

(U) When I arrived at the university, I was overwhelmed by the size of the campus. It was beautiful. I went straight to the dorm to check in. All of the language students stayed in the same dorm, the women on one floor and the men on another. It was one of only two dorms on campus that was air-conditioned. This was nice in the middle of the summer. I was told there were television, movie, and exercise facilities available in the dorm. I do not know if this is true because after the first day there was no time for any of these things.

(U) I met the other girls who would be in my class that afternoon and we all became fast friends. At

dinner that night I met the guys that would be in my class. There were 12 of us all together in the beginning class. All the Chinese students and teachers ate at special tables. The Japanese and Korean students also had their own tables. This was a great opportunity to talk to the teachers and practice Chinese as time went on.

(U) Classes started on Friday morning. We had four classes a day, each an hour long, with an hour between classes. That hour between classes was usually spent studying for the next hour's class. The two-hour lunch also was usually spent studying. The dorm cafeteria offered sack lunches so we did not have to waste time walking 20 minutes each way for lunch.

(U) At the end of the day we would all walk back to the dorm. It was a 20 minute walk along tree lined paths, over wooden bridges, and along a stream. This was an excellent way to relax after a day of classes. After dinner and about half an hour of relaxation and reading the newspaper, we resumed studying, about four hours a night. One of our native Chinese teachers had the room two doors down from mine. If anyone had a question, anytime, she was always eager to help. The teachers seemed to be truly interested in each student's progress. They were always around when someone had a question or a problem. They had office hours in the evening when the students could go and ask questions or just sit and talk. It was nice to be able to sit and use Chinese one-on-one with the teacher.

(U) All of our time was not spent studying, though. Every morning at 0630 there was Tai Qi (Chinese shadow boxing) for anyone who wanted to learn.

There was also a Chinese drama class, calligraphy and drawing, and singing. There were Chinese movies (with English subtitles for beginners) on Friday nights. Occasionally there was a party after the movie where we could relax and dance after a hard week of study. Saturdays were usually spent doing all the things a person did not have time to do during the week. There were trips to the store to get away from campus for a while, laundry, cleaning, and studying. There were volleyball games between the different classes. Sundays were usually spent studying all day. Every second or third Sunday the teachers tried and do something special. Since there was no dinner served at the dorm on Sunday, they cooked their own Chinese food and we would have a picnic, or just get together and talk. Then it was back to the dorm to study.

(U) I kept a diary while I was there. When I look at it now I see that just about every other word is "study." But for every "study" there is a "fun," and that is what I remember most. Although there was a lot of hard work, the teachers and students made it all fun.

~~(S)~~ [Redacted]

But at this time I am unable to do much. I still have a few years of study before I become effective in my job. But I look forward to it because it is definitely much more interesting and more challenging than being a secretary. I think I am going to like this.

~~(FOUO)~~ I found out when I returned to work that sending a beginner to Indiana was an experiment on the Agency's part. I was the first person to go there to take a beginning course. I think the experiment was a success because there is talk of sending more students next summer. I hope this is true because it would be great to see more people have the experience I did. And I must admit that I hope it is true because I would like to go back next year and take a more advanced course. I think even if the Agency does not send me next summer, I will go on my own for a long vacation spent studying and having fun. □

BULLETIN BOARD

SLAVIC TERMINOLOGY (U)

~~(FOUO)~~ Now in distribution is the third printing of the ever-popular *Comparative Bulgarian, Russian, Polish, and Czech Terminology* (S-203,185, P1 Language Publications No. 1, January 1972) compiled by [Redacted]

The multilingual format provides a base for a comparative method of solving translation problems. [Redacted]

For a copy write to:

[Redacted] P16, HQ 8A187. Phone orders are not accepted.

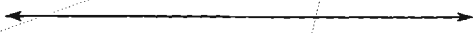
P.L. 86-36

1987 LINGUISTIC INSTITUTE (U)

(U) The Linguistic Society of America, the Association for Computational Linguistics and the American Association for Artificial Intelligence are co-sponsoring the 1987 Linguistic Institute at Stanford University from June 29 to August 7, 1987. The theme is "Contextual and Computational Dimensions of Language." The Institute includes conferences and seminars of various lengths, from a few days to 6 weeks, with intensive courses in African languages, Arabic morphology, and linguistic and language processing courses on syntax, semantics, and phonetics. The aim of the conference is to integrate linguistic theory with artificial intelligence, psycholinguistics, discourse analysis and computational linguistics.

For further information contact [Redacted]

[Redacted] P16, 963-1103. □



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

P.L. 86-36

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

ON THE LIGHTER SIDE (U)



A test paper making the rounds in the National Cryptologic School is rolling them in the aisles. Unlike most funny exams, the answers were right. You too might enjoy reading the unorthodox responses of an RU-15A student, to questions on Russian History.

Question 1. Describe the reign of the following Russian Tsars. What did they do which was significant for Russia, and what events took place?

P.L. 86-36

- A. Ivan IV.
- B. Peter I.
- C. Alexander I.
- D. Alexander II.
- E. Nicholas II.

Answer:

A. Ivan IV (The Terrible). One hard-core tsar. He got the landowners, boyars, and the church to fork over some cash to help run the country.

Created a 6,000-man political police force to help "persuade" his populace to follow the straight and narrow. Freaked out and killed his son during a tantrum.

B. Peter I (The Great). Tall dude who liked the West. Modernized the army and created a navy. He was a tsar who knew how to profit from Western technology. But no liberal was he. He did nothing that would weaken his absolute rule. Serfs remained chattel.

C. Alexander I. Napoleon came, saw, and barely escaped with his brandy intact.

Alexander's troops beat him back to France and made Russia a European power to be reckoned with. Only head of state that showed up at the Congress of Vienna. But still your basic tsar on the homefront.

D. Alexander II. (The Tsar Liberator). Freed the serfs (technically) in 1861. Real liberal guy, he tried to push through a bunch of reforms but it wasn't fast enough and some hot-headed terrorists blew him to smithereens.

E. Nicholas II. The last tsar. This poor slob was hen-pecked by a warhorse of a wife. Wanted to be big and tough like his dad, but it was no go. Blundered into WW I. After a few uprisings he gave up some power, forming the Duma. But it was too little, too late. Overthrown in 1917, he and his family met an untimely end. (See "Anastasia" starring Ingrid Bergman.)

Question 2. Why was Lenin successful in the October Revolution when all other revolutions failed? What was the shortcoming of the Provisional Government?

Answer: The Germans secretly shipped Lenin into Russia to get the Russians off their backs. It worked. The provisional Government and Kerensky didn't pull Russia out of WW I (which was probably why the October Revolution took place in the first place). AWOL soldiers, workers, and your basic Joe Blowsky didn't take kindly to going back to the front and so Lenin moved in, and with the treaty of Brest-Litovsk got Russia out of the war.

Question 3. What was the New Economic Policy and what was its effect on the Soviet Union?

Answer: In 1922, after the Civil War, the Soviet Union's economy was a shambles. So Lenin devised this new economic plan which was nothing less than a good strong dose of capitalism. It worked, and in 1927 everything was back to its pre-Civil War level.

Question 4. What steps were taken by Stalin to set the country back on the road to socialism? What problems were encountered? What effect did the purges of the 1930's have?

Answer: Stalin came in and ended the NEP, and put socialism back on its dreary path. Not too many people liked that. So he got rid of them. Exiled and/or killed millions. Decimated

the officer corps, so that when WW II came around his leadership cadre was wanting. Serves him right.

Question 5. What were the major events during Khrushchev's regime?

Answer: Let's see. There's the denunciation of Stalin that put the Soviets in a tizzy and really upset the Chinese. His "Virgin Lands" project to expand agriculturally into the vast regions of eastern Russia was a big flop. Gary Francis Powers took a nose dive in his U-2 and with that and so did relations with the U.S. And in 1962 he tried to sneak missiles to Fidel and blinked when Kennedy stared him down. Banged his shoe at the U.N. Visited Disneyland and was shocked by Shirley Maclaine on the set of Can-Can in Tinsel Town. □

REPRESENTATION OF PREFIXES (u)

Provided by P13D P.L. 86-36

REPRESENTATION

PREFIX	Factor by Which Unit is Multiplied	International Symbol (Common Use Symbol)	FORM I	FORM II	II
			(Double Case)	(Single Case, Lower)	(Single Case, Upper)
exa	10 ¹⁸	E	E	ex	EX
peta	10 ¹⁵	P	P	pe	PE
tera	10 ¹²	T	T	t	T
giga	10 ⁹	G	G	g	G
mega	10 ⁶	M	M	ma	MA
kilo	10 ³	k	k	k	K
hecto	10 ²	h	h	h	H
deka (deca)	10 ¹	da	da	da	DA
deci	10 ⁻¹	d	d	d	D
centi	10 ⁻²	c	c	c	C
milli	10 ⁻³	m	m	m	M
micro	10 ⁻⁶	μ	μ	u	U
nano	10 ⁻⁹	n	n	n	N
pico	10 ⁻¹²	p	p	p	P
femto	10 ⁻¹⁵	f	f	f	F
atto	10 ⁻¹⁸	a	a	a	A

CONFERENCE REPORT:

TALC 1986

Target

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

Aquisition and

Location

Conference

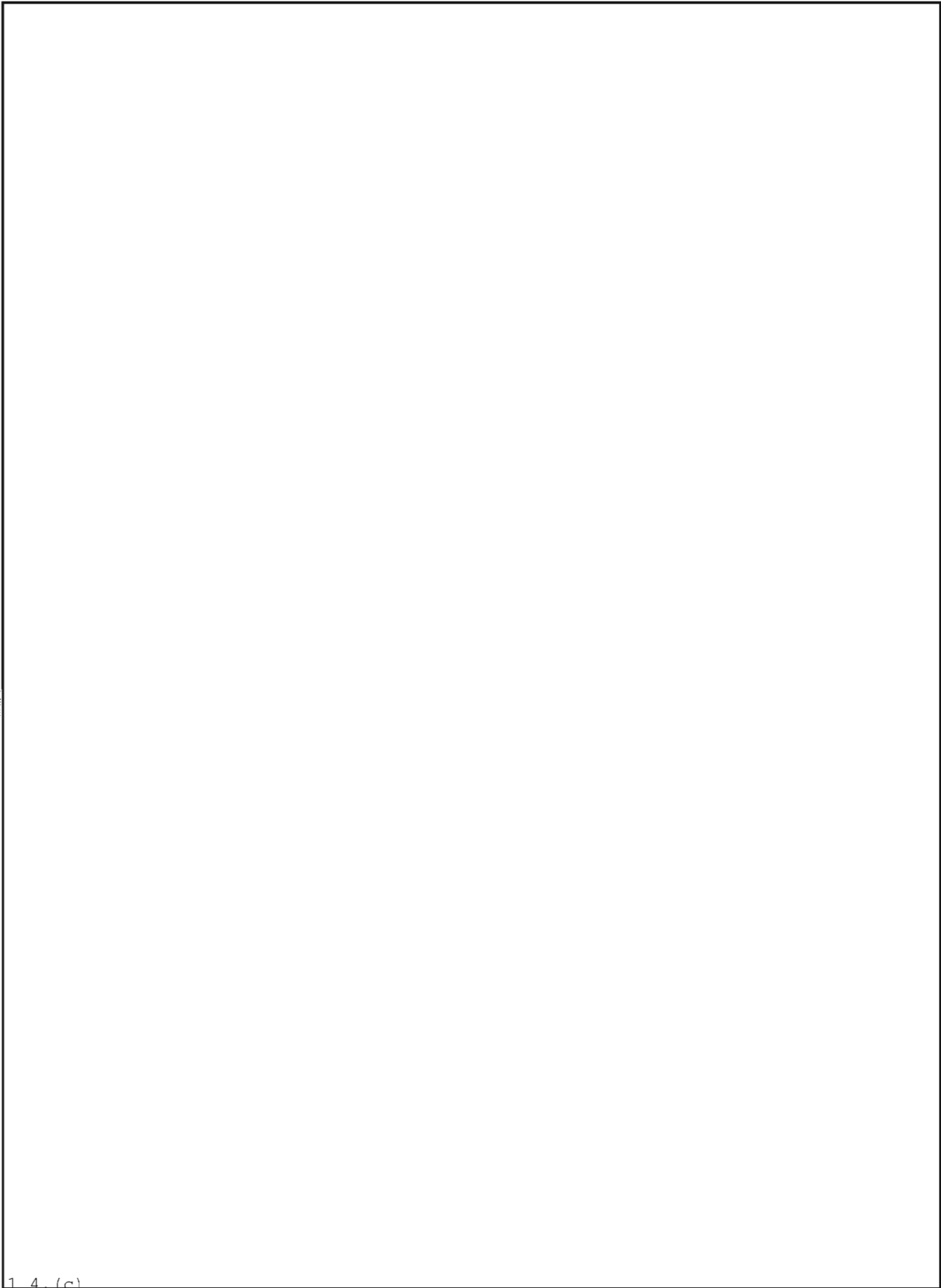


86 ~~(S-ECO)~~

N. C. Gerson, W3

~~This article is classified SECRET HVCCO in its entirety.~~





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

Technical Literature Review



"A Trigraphic Cipher with a Short Key for Hand Use" by Joseph R. Kruskal. *Cryptologia*, July 1985

P.L. 86-36 Reviewed by P12

In this article the author presents a simple Playfair-like cipher which is, as he states, easily used for manual enciphering and is genuinely trigraphic.

I. THE SYSTEM

This segment of the review is unclassified

The author's scheme requires that the number of rows (m) and the number of columns (n), are both odd. As an example let us take $m = n = 5$, combining J with I, and construct a Playfair square with an appropriate keyword:

C	R	Y	P	T	00	01	02	03	04
O	L	G	A	B	10	11	12	13	14
D	E	F	H	I	20	21	22	23	24
K	M	N	Q	S	30	31	32	33	34
U	V	W	X	Z	40	41	42	43	44

The second square shows the row and column coordinates of the 25 alphabetic characters. Both the plain and cipher components are alphabetic; the coordinates will however be useful in calculations.

If the coordinates of an on-cut plaintext trigraph are (r_1, c_1) , (r_2, c_2) , (r_3, c_3) , then the

corresponding ciphertext trigraph has coordinates

$$(r_2 + r_3 - r_1, c_2 + c_3 - c_1), (r_1 + r_3 - r_2, c_1 + c_3 - c_2), \\ (r_1 + r_2 - r_3, c_1 + c_2 - c_3),$$

where the calculations of the components are carried out mod (m, n) . To illustrate, if the plaintext trigraph REF is to be enciphered, we write $R = (0,1)$, $E = (2,1)$, $F = (2,2)$ and calculate the ciphertext coordinates as

$$(2+2-0, 1+2-1), (0+2-2, 1+2-1), (0+2-2, 1+1-2)$$

which mod $(5,5)$ is $(4,2)$, $(0,2)$, $(0,0)$, resulting in the ciphertext trigraph WYC.

The deciphering procedure is only a little more complicated. If the ciphertext trigraph is

$$(R_1, C_1), (R_2, C_2), (R_3, C_3)$$

then the transformation, which is inverse to the enciphering transformation, produces the plaintext

$$\left(\frac{1}{2}(R_2 + R_3), \frac{1}{2}(C_2 + C_3)\right), \left(\frac{1}{2}(R_1 + R_3), \frac{1}{2}(C_1 + C_3)\right), \\ \left(\frac{1}{2}(R_1 + R_2), \frac{1}{2}(C_1 + C_2)\right),$$

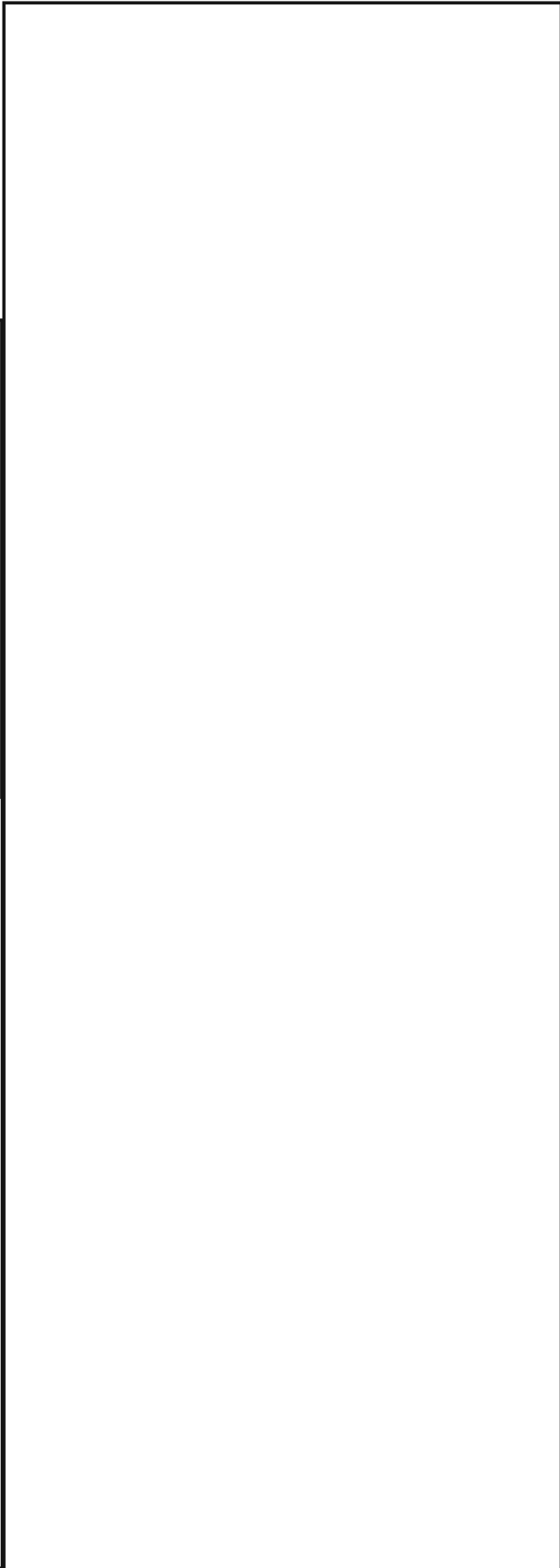
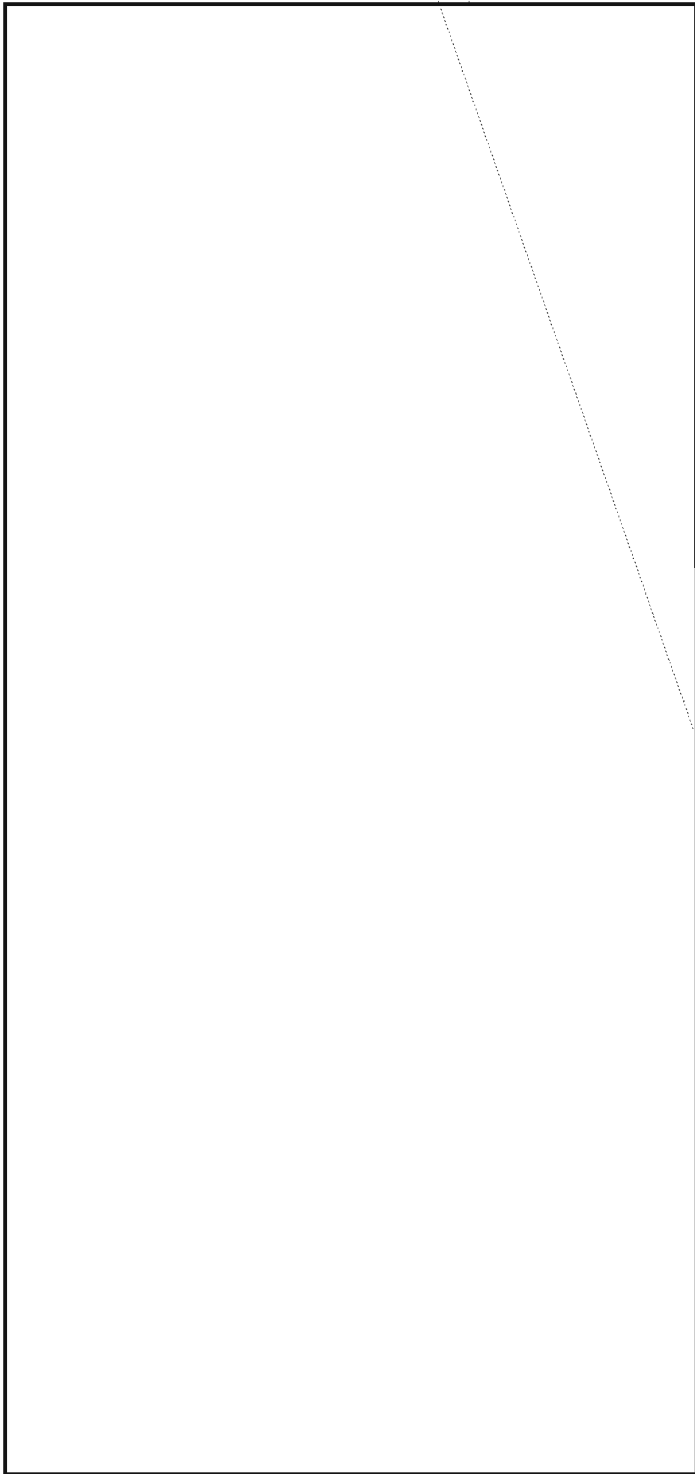
as can readily be checked. For example

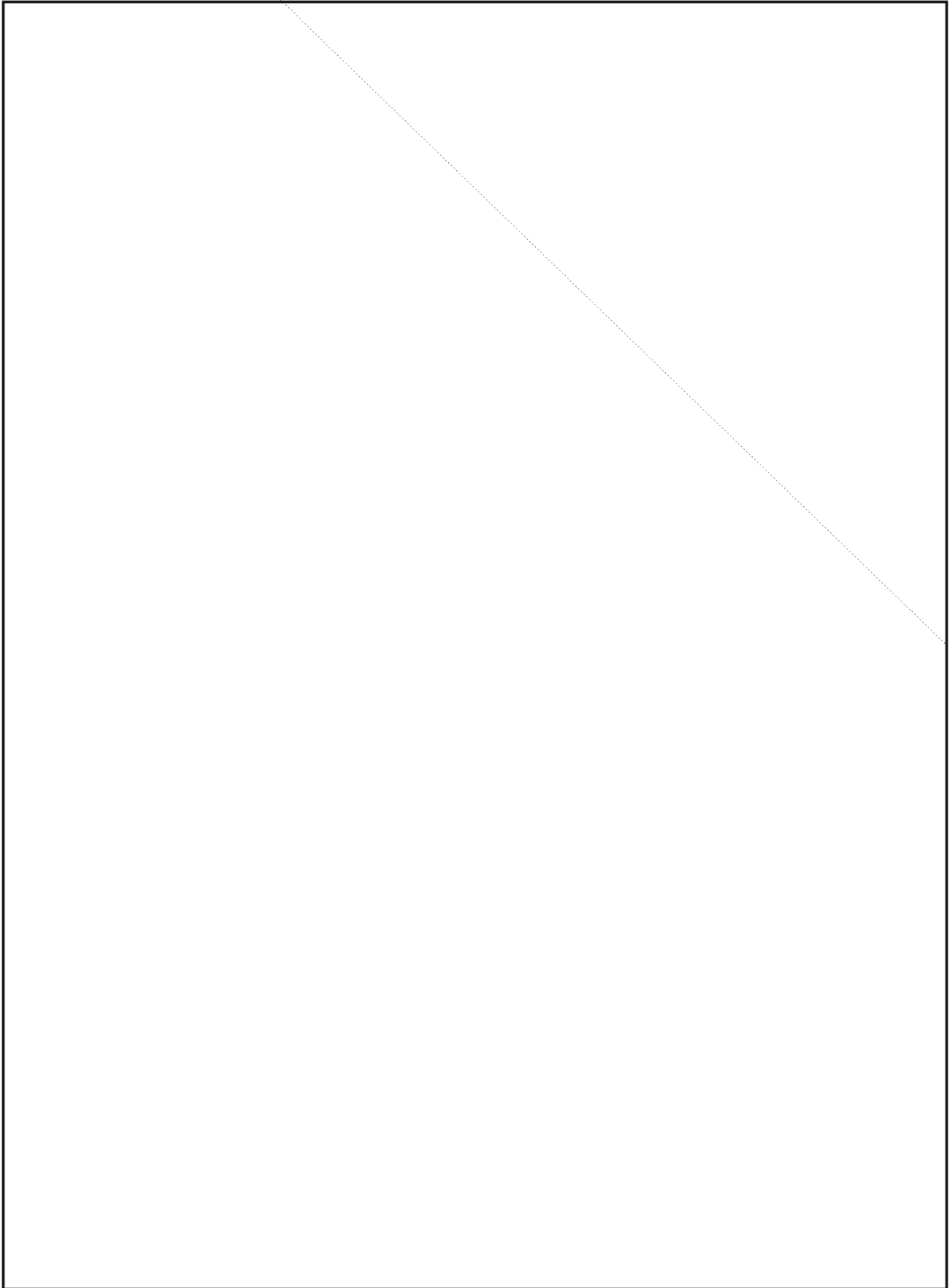
$$\frac{1}{2}(R_2 + R_3) = \frac{1}{2}((r_1 + r_3 - r_2) + (r_1 + r_2 - r_3)) = r_1$$

The form of the decryption operation shows why it is that we must insist that both m and n are odd. If m were even, then $\frac{1}{2}$ would have no meaning. But for m odd, $\frac{1}{2}$ makes perfectly good sense: $\frac{1}{2}$ is that number which when

multiplied by 2 yields 1 mod m. So for instance if $m = 5$, then $\frac{1}{2} = 3$, since $3 \cdot 2 = 6 = 1 \text{ mod } 5$.

Kruskal remarks that if plain ABC corresponds to cipher XYZ, then we also have correspondences between the pairs BCA and YZX, CAB and ZXY, CBA and ZYX, BAC and YXZ, and ACB and XZY.





BULLETIN BOARD**FORMATION OF XEROX USERS' GROUP (U)**

(U) A Users' Group is being formed at NSA for users of the Star, Viewpoint, and XDE.

Interested persons should call [REDACTED]
Y44, 972-2345.

P.L. 86-36

FOREIGN LANGUAGE VIDEOS (U)

~~(FOUO)~~ Videotapes in Russian and German are shown every Thursday at lunchtime in a conference room. They feature news and documentaries. Russian tapes are shown 11:00-12:00, and German tapes, from Austria and East and West Germany, are shown 12:00-1300.

(U) Programs and meeting rooms are posted on the CLO Bulletin Board on the north wall by the escalators near the entrance to the cafeteria.

~~(FOUO)~~ For other information about the German videos call [REDACTED] P16, 963-1103, and about the Russian videos, [REDACTED] A2COG, 963-1180.

P.L. 86-36

TERMINOLOGIES (U)

~~(FOUO)~~ Several terminologies and glossaries in SIGINT and related specialties are being compiled by P13D. For a list of publications in the planning stage or already completed, call or write [REDACTED] P13D, 968-8161.

P.L. 86-36



~~TOP SECRET~~

P.L. 86-36

SOFTWARE REVIEW:

P13

FOUR PC-BASED EXPERT SYSTEM SHELLS (U)

- ▶ ExSys
- ▶ Personal Consultant
- ▶ Guru
- ▶ Expert-Ease.



(U) Are any of the many "expert system" packages advertised really useful? Is even the best PC package suitable for building expert systems for NSA applications?

(U) In general, one might expect:

- ▶ cheap, easy to use products providing roughly the same set of features as in Mycin (an expert system research project of the 1970s) with the rule capacity limited by the PC's memory and disk storage;
- ▶ limited processing speed and either no extensibility or very limited extensibility
- ▶ a variety of user interfaces
- ▶ generally poor documentation.

(U) In the four packages tested I found:

- ▶ more features and a greater variety than I expected, though some of the "basic" Mycin features were not available in some packages,
- ▶ better user interfaces, but disappointingly, some aspects of the user interfaces seemed needlessly complex or difficult;
- ▶ generally more capacity than I had believed possible;
- ▶ documentation in some cases even worse than I had expected.

~~(FOUO)~~ Overall, I found that all the PC-based expert system shells have some potential for NSA applications. With the abundance of ASTWs in NSA and at its field sites, expert system shells have considerable potential for assisting both junior and senior analysts with complex analytical decisions. Greater potential exists in areas where personnel rotation creates a training problem and round-the-clock operations make it difficult for even an expert to keep track of the myriad of constantly changing detail. Field sites, NSOC, and DEFSMAC are excellent candidates for expert systems which assist with important time-sensitive decisions about analysis and reporting of observed phenomena, particularly when there are conflicting data from multiple sources.

(U) Following are specific comments on the individual packages.

ExSys (\$300)

(U) ExSys is the easiest to use of the four expert system shells I tried, and it has some powerful features as well, though it does have some limitations.

(U) When you start to build an expert system with ExSys, the first activity is to define a rule. The rule constructor requires "qualifiers"

~~TOP SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

and "choices" for the IF and THEN portions of the rule. While you are in the middle of making the rule, you go off to the side and build a qualifier, which is an enumeration data type whose name is the subject and verb of a sentence and whose values are possible objects for the sentence. When you have built a qualifier, you select one or more values for the rule you are building. ExSys automatically builds a rule that reads like English. Once a qualifier is built, it can be used in other rules; everything is integrated nicely. Before you know it, you have built an expert system.



(U) One particularly nice feature of ExSys is the optional ELSE part to a rule. This does not appear in any of the other three expert system shells reviewed.

(U) Some of ExSys's shortcomings:

▶ Qualifiers cannot have certainty factors; if you must deal with uncertainty, this may not be an acceptable system. Choices (the final output for ExSys) must have probabilities associated with them, and these probabilities will be averaged if multiple rules produce the same answer with uncertainty. That is as far as ExSys goes with uncertainty; no uncertainty is allowed in the IF portion of a rule.

▶ The manual is skimpy in some of its explanations. For example, the order of rule selection is according to the numerical order of choices. I found that out, not by reading the manual, but by rearranging the choices in alphabetical order and thereby messing up my system.

▶ The on-line explanation merely displays the current rule. This is not as useful as Personal Consultant's ability to display the entire chain of reasoning on-line.



Texas Instruments Personal Consultant (\$950)

(U) Personal Consultant, a commercial implementation of the EMycin system, has several of its nice features:

▶ enumeration data types, very handy for user interaction. (The user can select from a list of values instead of typing them in, thereby avoiding mistyping);

▶ runs under Lisp; it is extensible in Lisp, and offers Lisp's advantages for processing symbols (e.g., text). This has a dark side, also: every 15-20 minutes, the Lisp system stops to do its garbage collection, a one-minute interruption on my PC;

▶ multiple rule contexts, to help organize the rules;

▶ comprehensive explanation capability, both during a session and after the session is concluded;

▶ an intuitive certainty factor system.

(U) Personal Consultant has some surprising problems: the documentation is badly organized and hard to use; a few features that I had not liked in the mini-Mycin package are unchanged in the TI package; and, worst of all, it requires a key disk in drive A, one of my pet peeves.

(U) Some other complaints about Personal Consultant:

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

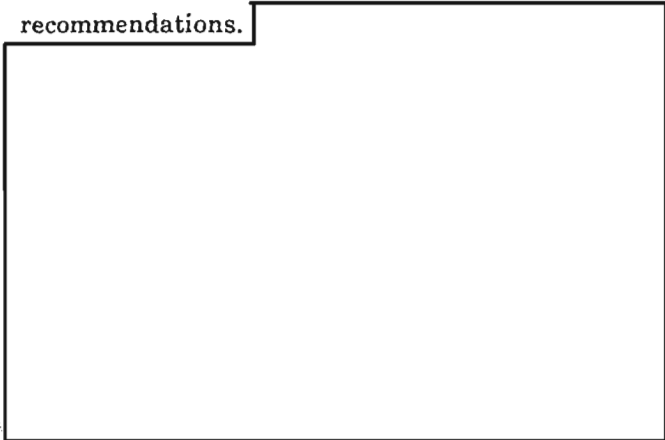
~~TOP SECRET~~

▶ The rules are given names; then, when the rules are listed on the printer, the names are omitted and numbers are used.

▶ A user with no Lisp training will find some of Lisp's ideas confusing (for example, parentheses all over the place, and the ubiquitous garbage collection) Non-Lisp-oriented users would have trouble even with the installation.

(U) Mycin does offer a lot of power for building expert systems, and the Personal Consultant offers that power in a nice package, except for the copy protection.

~~(TS-CCO)~~ Personal Consultant would be better than ExSys in an application with a complex knowledge structure. It also has graphics to display either input data or to explain its recommendations.



(U) A new version, called Personal Consultant Plus (\$3,000), has graphics, metarules, frames, DOS program execution, the capability to insert a procedure to determine the value of a variable, and the capability to insert a procedure to be executed when a variable changes.

GURU (\$3,000)

(U) The documentation of Guru is bulky. The four manuals -- a two-volume reference manual and two user's guides -- are intimidating. I found almost no use for the two user's guides.

(U) After running through the demonstrations, I tried to build a small (five-rule) expert system of my own. This took about ten hours. I had previously built the same five-rule system with ExSys in two hours and with Personal Consultant in 2 hours; and I later built an equivalent system with Expert-Ease in 2 hours.

(U) Some specific problems :

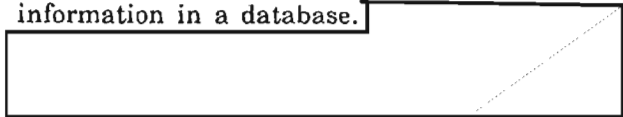
▶ Inadequate error handling: In ignorance I used `display`, a reserved word in Guru, both as a variable and as a rule name. The compiler did not tell me that I had used a reserved word. When I tried to run the erroneous expert system (Guru didn't stop me), the message "misplaced LOGIC" appeared on the screen. I knew something was wrong, but the error message gave me no clue whatever.

▶ Incomprehensible description of certainty factors in the manual. Although the claim is made that there are 16 ways to combine certainty factors, there are actually four very similar probabilistic ways that can be paired to make 16 combinations.

▶ Lack of enumeration type that would allow you to specify a limited set of string values for a variable (e.g., Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday). You should be able to access this through a menu function (missing in the current version of Guru) rather than having to write a subroutine.

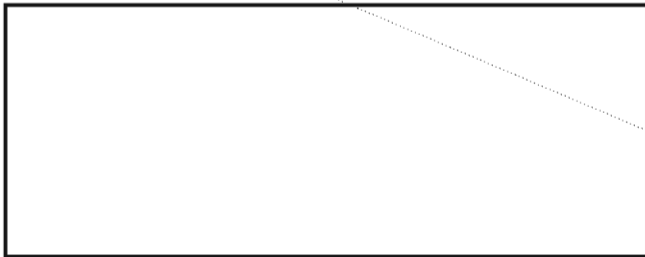
(U) Guru is difficult to use but broad in its applicability. It would probably be good for a rule-based application for which access to a data base or spreadsheet or remote computer file is important.

~~(TS-CCO)~~ When the bugs are worked out, Guru may be useful for complex data base retrievals or for help with decisions based on information in a database.



~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~**EXPERT EASE (\$495)**

(U) Expert-Ease is a different kind of expert system shell. It builds rules using "examples" given by the user, a technique developed by Donald Michie in Scotland. This appears to be a very easy way to do it. It was surprisingly easy to set up the toy system I used to test all the packages.

(U) It was easy learn and to use, and it does allow linkage of multiple rule sets, and does deal with uncertainty in a limited way (three categories); but it has several major defects:

- ▶ it has no high-level language connection and it is not extensible.
- ▶ it provides no explanations of its reasoning chain.
- ▶ it has no reference manual. The manual is a tutorial, without an index.

(U) Expert-Ease runs under UCSD Pascal, and requires a Pascal partition to run it on a hard-disk system, causing problems for someone who wants to run it alongside DOS or Unix programs. The lack of extensibility and the lack of explanations make it inadequate for the kinds of things expert systems are noted for. It might be useful for someone who wants to experiment with building an expert system using examples instead of constructing rules.

SUMMARY

(U) Of the four systems reviewed, ExSys offers the most power for the money. It is superior to the others for ease of use, power, cost, and external program connections. But there are

some applications in which it would fail miserably.

(U) My second choice would be Personal Consultant. For general power without respect to cost, for a Lisp connection, for good certainty factors, and for explanations, it is the best of the four. Personal Consultant Plus offers even more features (metarules, graphics, frames, external DOS programs), although at a higher price.

(U) Guru has a number of problems, but its concept is a good one. It is the only shell I know of that integrates a data base and spreadsheet with the expert system; it also has a natural language interface (not evaluated), graphics, and a communications interface. A new release will be available by the end of 1986.

(U) Expert-Ease is the only product to build an expert system from user-provided examples. Other than that, there is nothing to recommend it. □

REMINDER

If you want to be sure of receiving CRYPTOLOG after you move or are reorganized, send a change of address to Editor, CRYPTOLOG, P1, and include your name and both old and new organizations.

~~TOP SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

P.L. 86-36

To the Editor:

~~(FOUO)~~ [redacted] article on collection management (Aug-Sep 1986) is thought-provoking. I'd like to know if the situation as [redacted] has portrayed it is so. Has the NSA collection manager become a wart on the smooth skin of SIGINT operations? Do other collection managers feel as [redacted] does?

~~(S-CCO)~~ For the younger readers, a little expansion of [redacted] history may be in order. Before he arrived, elements of the Agency within Production (PROD) included General Studies (GENS), Asian Communist Studies (ACOM) [redacted]

[redacted] and All Other (ALLO). There was another element that was specifically concerned with the management of collection resources; Collection (COLL), although it was charged with other responsibilities as well. In fact, shortly after the element had been organized, it changed its name to Collection and Signals Analysis (COSA) to reflect more accurately the element's responsibilities. Even that name fell short. It omitted consideration of Non-Morse General Search (COSA-41), Morse General Search (COSA-42) and others.

~~(S-CCO)~~ That's enough of the gratuitous history lesson. Other readers with better memories than mine will almost certainly find some inaccuracies in the foregoing. The fact is that at that time things started happening to

the way NSA was funded. The "good old days" ended about that time and the program elements and subelements began. Each part of the Agency was funded to perform specified functions; each had to justify its existence and its budget every year. Consequently, each insisted on exercising complete control of assets that were associated with the targets for which the subelement was funded. There suddenly was no longer a pool of intercept positions that belonged to the Agency and that could be assigned as required to perform functions that needed to be done. [redacted]

[redacted] That was when GENS became A, ACOM became B and so forth. And, that was when the collection managers who had managed the Agency's resources found themselves often in conflict with subelement managers who insisted on managing the resources they had to be responsible for. At this time, the role of the collection manager began to be eroded to the state described by [redacted]

~~(FOUO)~~ Please note that I am not disputing the events and facts described by [redacted]. Those dates are true. I am just mentioning additional factors that were involved in the evolution of the role of the collection manager. There are probably other factors as well. The point that I am trying to make is that it is not a simple problem. Solutions, therefore, will not be simple, if they exist at all.

P.L. 86-36

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

Oct-Nov 1986 * CRYPTOLOG * page 27

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~(FOUO)~~ It would be useful to have responses to [redacted] queries from other collection managers

[redacted] P041.



To a Mixed-Up Fireman on a Diesel Locomotive:

(U) Just thought I'd let you know that I spent part of my time here on this holiday [11 November] reading your article in CRYPTOLOG.

(U) I enjoyed it. I hope it brings the results you want.

P.L. 86-36 [redacted], G05



To the Editor:

~~(S-CCO)~~ I read with interest the article on collection management. Although the historical portion was somewhat informative the remainder was rather insensitive, misleading and a bit upsetting, at least to me. I would

[redacted]

Likewise, I can't imagine a great deal of support for your recommendations coming from the Signals Collection Career Panel, collection professionals and aspirants, or the Collection Association. Some criticism, perhaps.

~~(S-CCO)~~ As collection managers we are continually involved in a multitude of sins to include:

[redacted]

A good collection

manager is in some way always associated directly or indirectly with many of those functions. This was not very well reflected in the article, if at all.

~~(S-CCO)~~ In fact, if it wasn't for the highly dedicated efforts of our relatively small work force of collection managers the current ability of this agency to satisfy its SIGINT requirements [redacted]

[redacted] would be greatly diminished and/or in a messy state of disarray. And as NSA's mission continues to grow, the functions and roles of our collection managers will most likely continue to expand, not diminish.

~~(S-CCO)~~ I believe that the role of the collection manager and collection management as a profession is absolutely essential if NSA is to continue to satisfy its SIGINT requirements. I further believe that the collection manager in the performance of the multiplicity of his or her duties and functions in the process of getting the product to the consumers is absolutely vital and should be so acknowledged. Today's collection manager can be and should be very proud of his or her chosen profession.

~~(S-CCO)~~ This is not to say that collection managers cannot or need not improve upon their past performance and accomplishments -- they can and they are very willing to. In fact, today's collection manager is in a better position than ever before to do a more effective job more efficiently due to the modern tools of the computer age coupled with recent telecommunications upgrades. The most significant shortcoming of today's collection manager is due to the lack of a meaningful training program. All of the efforts and all of the tools and communications enhancements will not optimize the collection manager's skills or maximize his or her productivity unless they are fully and formally trained to handle the many and various collection-related matters in which they become involved. A good, complete, well-structured formal collection manager's training program is sorely needed to remedy the initial lack of technical, subject-matter related and literary expertise of our new collection

~~SECRET~~

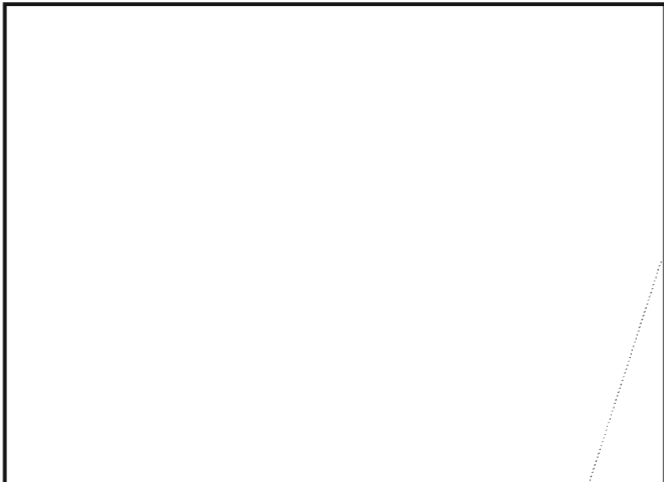
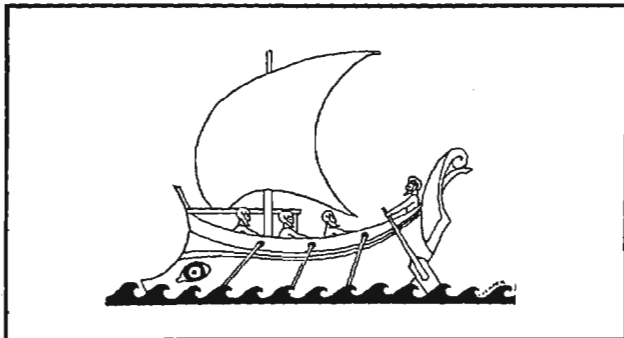
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

manager trainees. This approach, I believe, would be a positive step in the right direction.

is the capability to feed back decrypts to field sites seven days a week without having an analyst on hand to monitor the process.

[redacted] G841.



To the Editor:

~~(FOUO)~~ We read with great interest two letters to the editor concerning the ODYSSEY/CAMS article in the CRYPTOLOG. We in the organization where the process was begun would like to address the various points that were made in these two unsigned letters. So, to 'A Retiring Cryptanalyst,' 'An Old Timer,' and anyone else who may be interested, please read on.

~~(C-CCO)~~ Both letters showed concern over lost messages and perhaps never seeing key messages. These fears are unfounded since all messages that pass the various thresholds and process through the system are accounted for;

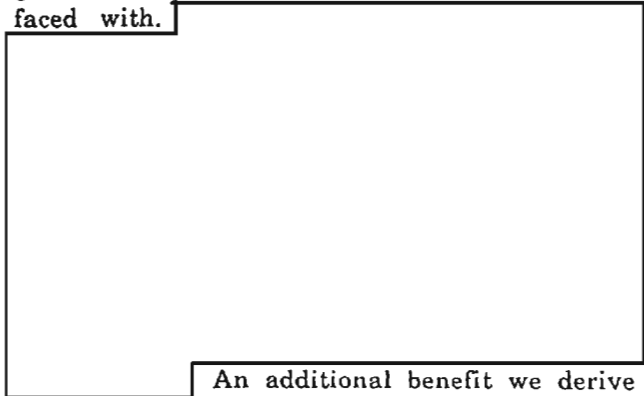
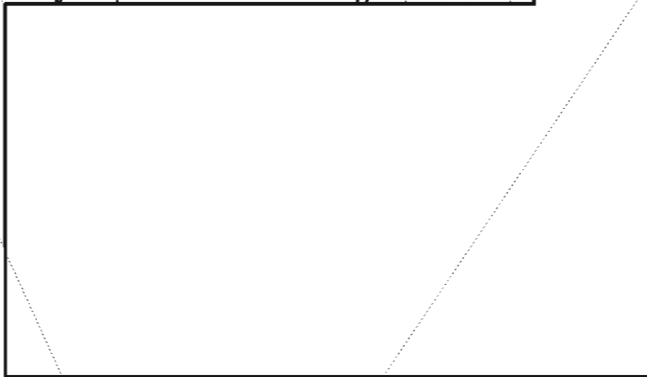


~~(S-CCO)~~ Let us address the points common to both letters. Each advocates interactive editing either "very early . . ." or "before . . ." . Interactive editing would defeat the purpose of this process.

~~(C-CCO)~~ The final point in common is a concern over the quality of AG22 data. We see no point in debating this issue. Given our successes as demonstrated by the above statistics, the quality must not be too bad. There is an additional capability which was not fully explained in the original article.



the shortest possible time with an absolute minimum of human intervention. In order to understand why, for us, the issue of 'minimum human intervention' was and is critical, let us give a few statistics about the volumes we are faced with.



~~(FOUO)~~ After we first started using the CAMS process, B53 gave demonstrations and talks about ODYSSEY/CAMS to interested people and organizations; the most notable being for the 1982 CA-305 course and for the 1982 CISI Spring Conference. We will be happy to discuss

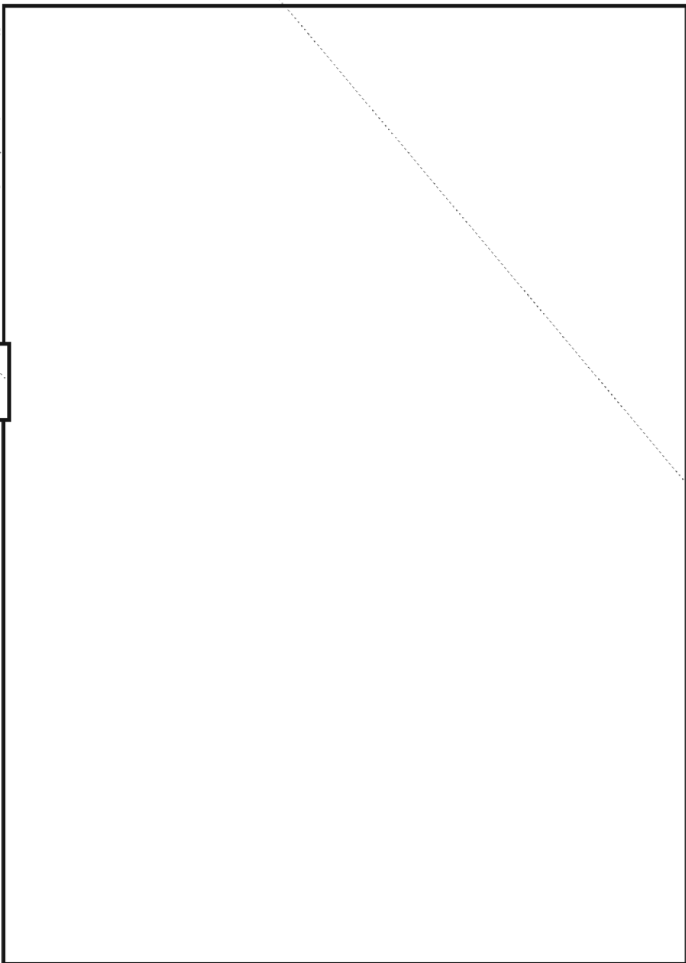
An additional benefit we derive

~~SECRET~~

~~SECRET~~

any of these points further or to give demonstrations to anyone interested.

~~(C)~~ This organization does not view ODYSSEY/CAMS as a universal processing method. It is not the "be all and end all" for Agency cryptanalysts. For the original purpose for which it was created, ODYSSEY/CAMS is a very successful process and we highly recommend it to any organization that is tasked



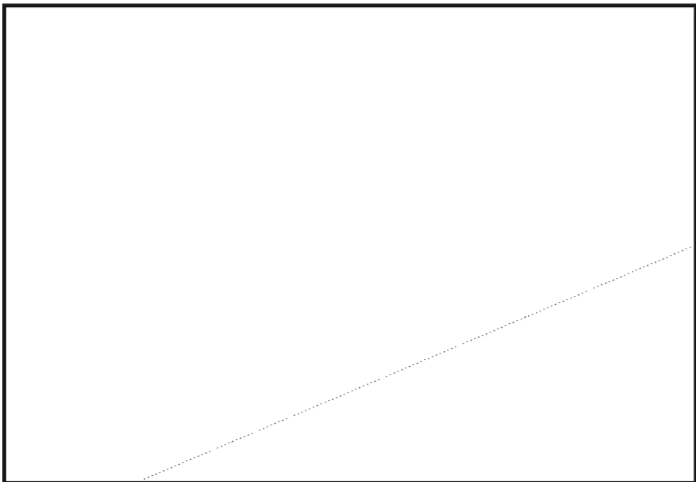
B53 Management and Cryptanalysts



P.L. 86-36

~~The following letter is classified
G CGO NO CONTRACT in its entirety.~~

To the Editor:



CRYPTOLOG

is a classified publication.

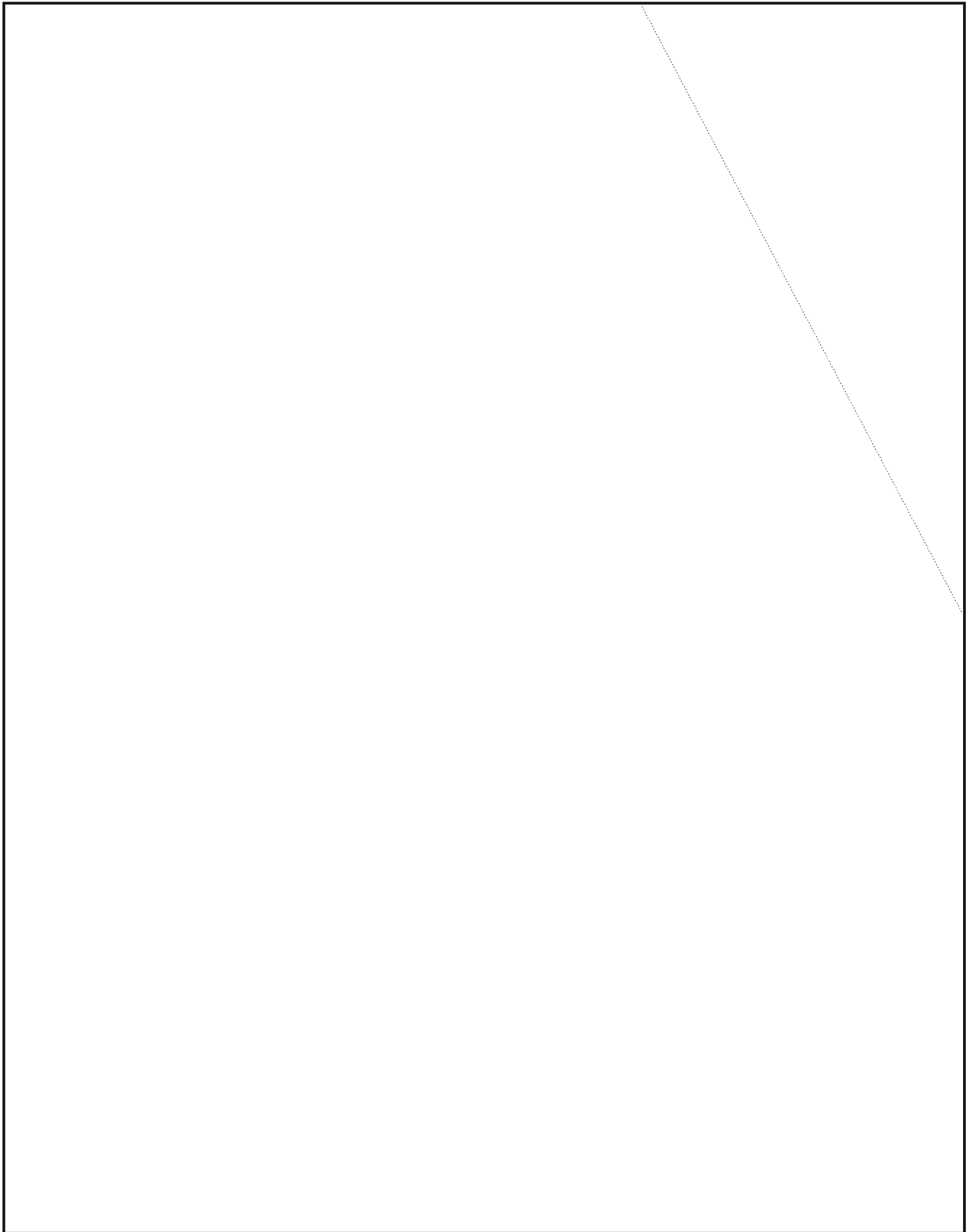
It may not be read in the cafeteria

or in other insecure areas.

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

FROM THE PAST (U)



RESULTS OF THE READERS' SURVEY (U)

In the May-Jul 1986 issue we used a variety of type faces, word spacings and leadings. Also, for some articles we right-justified the text, for other articles we didn't. An additional variation, a more subtle one, consisted of using for some articles 12-point type at 80% and for others, 10-point type at 100%; these two are theoretically equivalent. The purpose of this experiment was to determine what combination of variables would provide the most readable text, given the limitations (and bugs) of the current word processing software. And so we asked readers for their opinions. Meanwhile, we were moved to another press and a new page size.

Of the 38 responses received, one-third (idiosyncratically, as might be expected of the NSA population) gave only a few top and bottom choices, so the totals are not the same for all entries. Overall, people were more in agreement about what they *didn't* like than about what they did like. The scores show an aversion to fonts designed for optical character readers and to closely-spaced words and lines. The few comments indicated preference for serif type faces. And some respondents hadn't noticed any difference at all!

This text is set in 12-pt Classic, double space between words, with 15-pt leading, reproduced at 90% now that we are using the new standard page size of 8½x11. The result approximates 11-pt type, considered ideal for narrative text. We believe that this combination will be very readable. About right justification: we try it out for each article. When it causes grotesque spacing -- usually because of a sequence of long words -- we revert to ragged rights. We expect to right-justify routinely beginning in mid-1987, when upgraded software with automatic hyphenation is to be installed.

In the summary below, the NET column shows TOP 3 minus BOTTOM 3, for a net score.

ARTICLE	TOP 3	MIDDLE 9	BOTTOM 3	NET	TYPE FACE	SIZE	LEAD- ING	WORD SPACE	JUSTI- FIED?
Odyssey	14	15	2	12	Classic	12/80	13 pts	Double	No
C3	2	18	9	-7	Classic	12/80	12 pts	Single	No
Linguist	18	12	1	17	Classic	12/80	15 pts	Single	No
AI	3	16	14	-11	Classic	12/80	12 pts	Single	Yes
Documents	11	17	1	10	Modern	12/80	13 pts	Single	Yes
Team	8	21		8	Classic	10/100	11 pts	Single	No
Passwords	12	15	4	8	Modern	10/100	11 pts	Single	Yes
	5	21		5	Modern	10/100	12 pts	Single	No
Editor	6	14	6		<i>Mod Ital</i>	12/100	12 pts	Single	No
	6	19	2	4	Modern	12/80	14 pts	Single	Yes
	8	8		8	Classic	12/80	14 pts	Single	Yes
	1	15	9	-8	<i>Class Ita</i>	12/80	14 pts	Single	Yes
		7	21	-21	ocrA	12/80	13 pts	Single	No
		10	17	-17	ocrB	12/80	13 pts	Single	No
	3	21	2	1	Titan	12/80	14 pts	Single	No

PUZZLE

by

"Wheel of Fortune" has become one of the most popular TV game shows in history. The object is to solve a word or phrase by guessing the letters that appear in it. For a bonus prize each contestant is invited to supply five consonants and one vowel, then given 15 seconds to solve a phrase with only those six letters revealed. Most contestants choose the letters L N R S T E, which are the ones revealed in the phrases below. A brief clue is provided for each. An additional clue is that all the solutions relate to cryptology. Note that 'Person' need not indicate a proper name.

EXAMPLE:

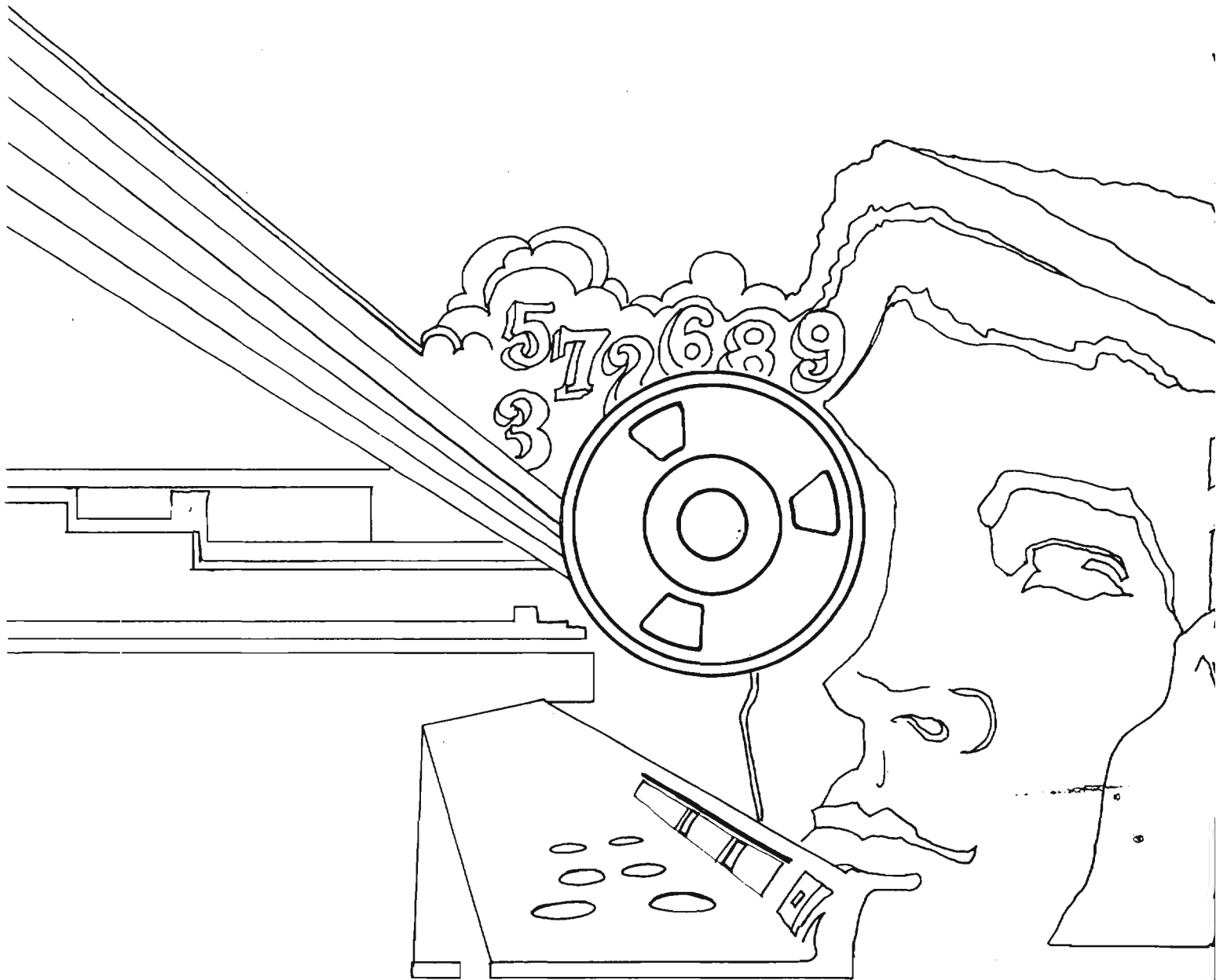
Place: N _ T _ _ N _ L S E _ _ R _ T _ _ _ E N _ _
Thing: _ _ N _ _ L _ _ _ _ _ ET _ _ _ S _ _ S T _ T _ T _ _ N

SOLUTION:

NATIONAL SECURITY AGENCY
MONOALPHABETIC SUBSTITUTION

.....

1. Person: _ _ L L _ _ _ _ R _ E _ _ _ N
2. Place: _ R L _ N _ T _ N _ _ L L
3. Person: _ _ _ _ E R _ _ L E R _
4. Thing: _ _ _ _ L E T R _ N S _ _ S _ T _ _ N
5. Organization: _ _ _ _ _ R E _ _ E R S _ _ R _ _
6. Thing: _ _ R N _ _ _ _
7. Thing: _ _ L L S _ _ N R _ T _
8. Place: R _ T _ _ S _ _ _ N
9. Thing: _ E _ T _ R E _ _ _ N _
10. Place: _ _ E L T E N _ _ _
11. Thing: _ N E - T _ _ E _ _ _
12. Place: _ L E T _ _ L E _ _ _ R _
13. Thing: S _ R E _ _ S _ E _ T R _ _
14. Place: _ _ R _ _ R T S _ _ _ R E
15. Thing: _ L _ _ _ _ _ R S _ _ _ R E
16. Thing: N _ R _ _ L _ _ S T R _ _ T _ _ N
17. Phrase: _ _ R _ _ _ _ _ _ L _ S E _ N L _
18. Thing: _ _ _ _ _ N _ _ _ T _ _ N S S E _ _ R _ T _
19. Historic thing: _ _ _ _ _ E R _ _ N N T E L E _ R _ _
20. Thing: _ _ _ E L _ N _ _ _ _ _ N E



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~