~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST-SEPTEMBER 1975

EO 1.4.(c)

P.L. 86-36

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. II, Nos. 8 and 9 AUGUST-SEPTEMBER 1975

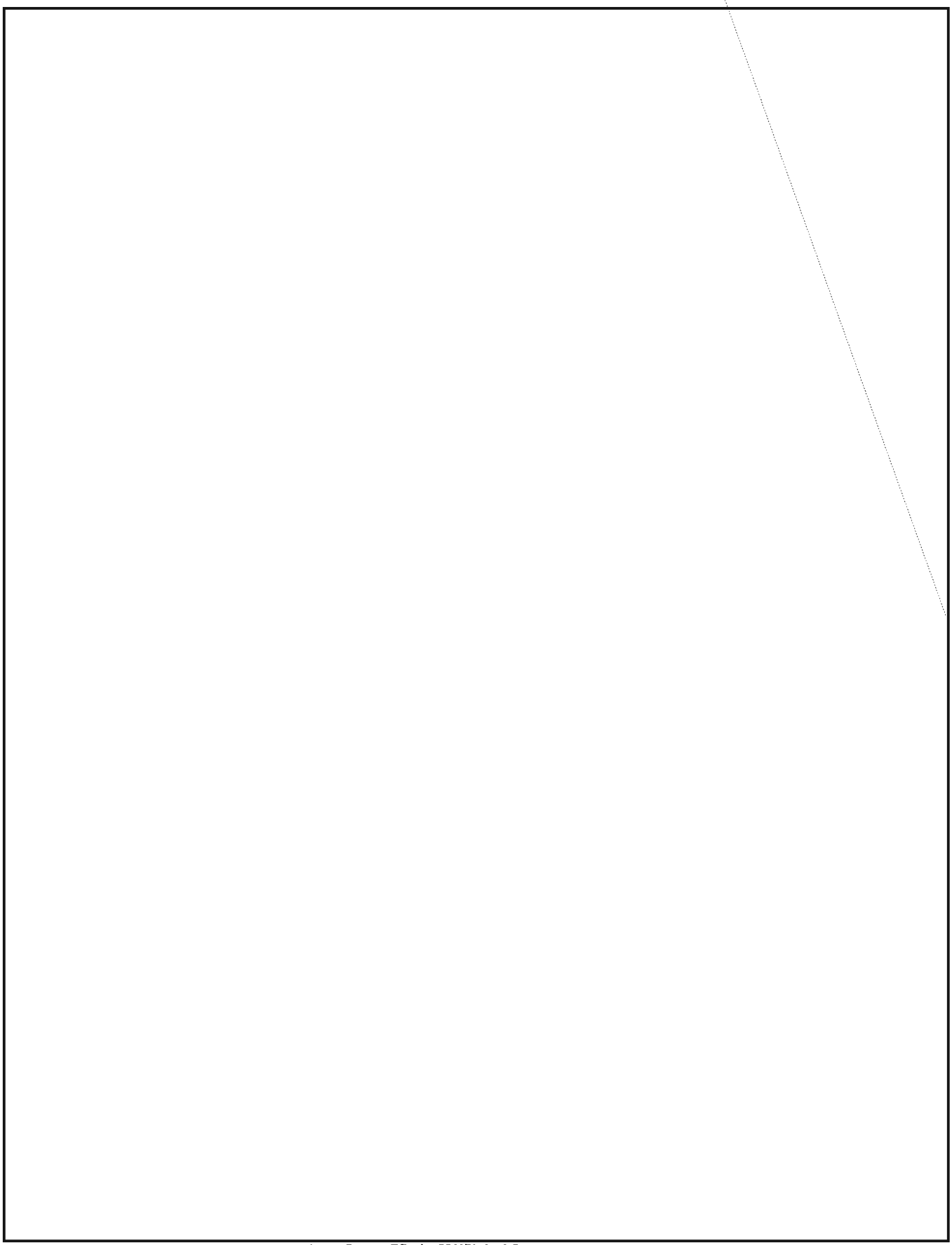
PUBLISHER WILLIAM LUTWINIAK

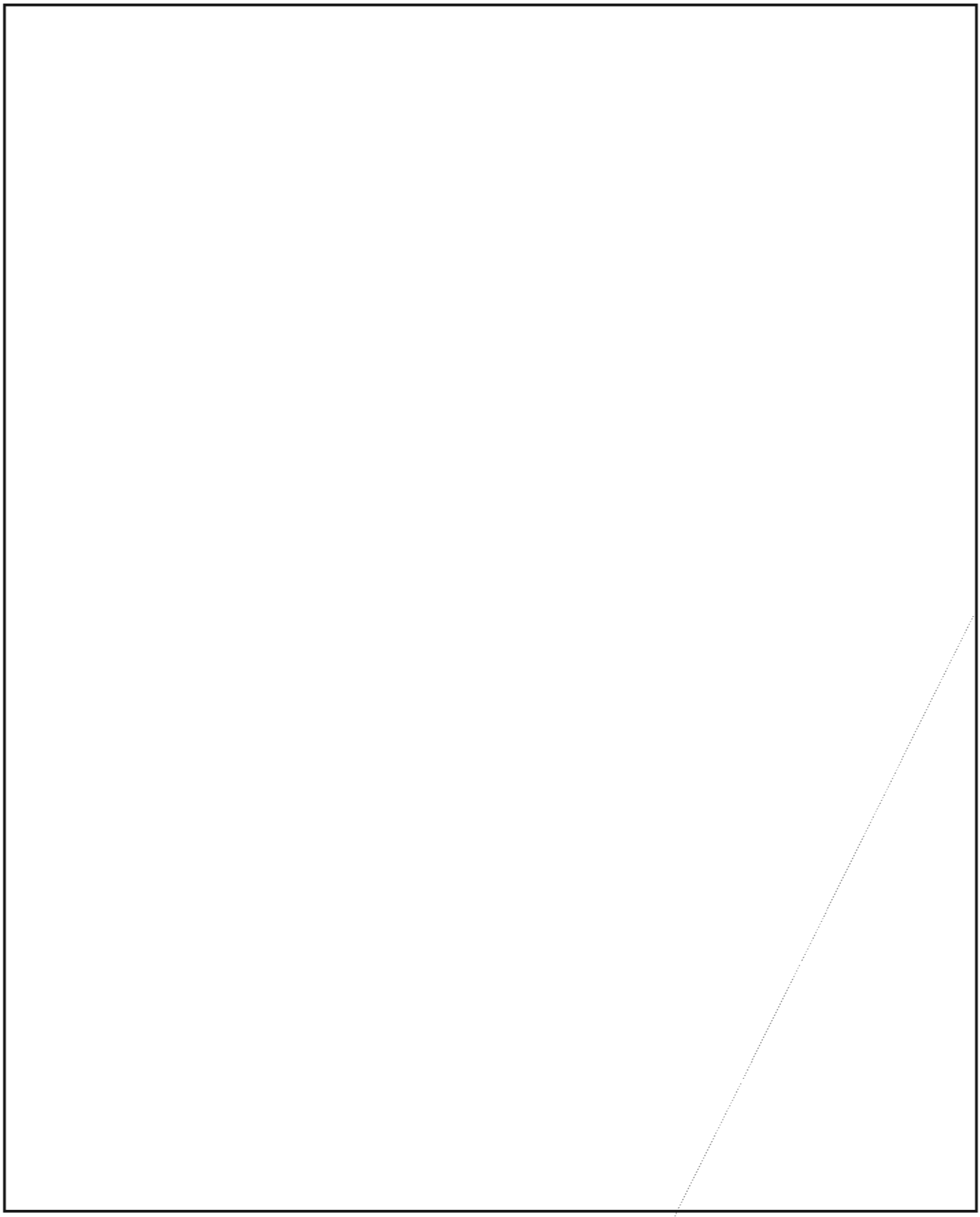
For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

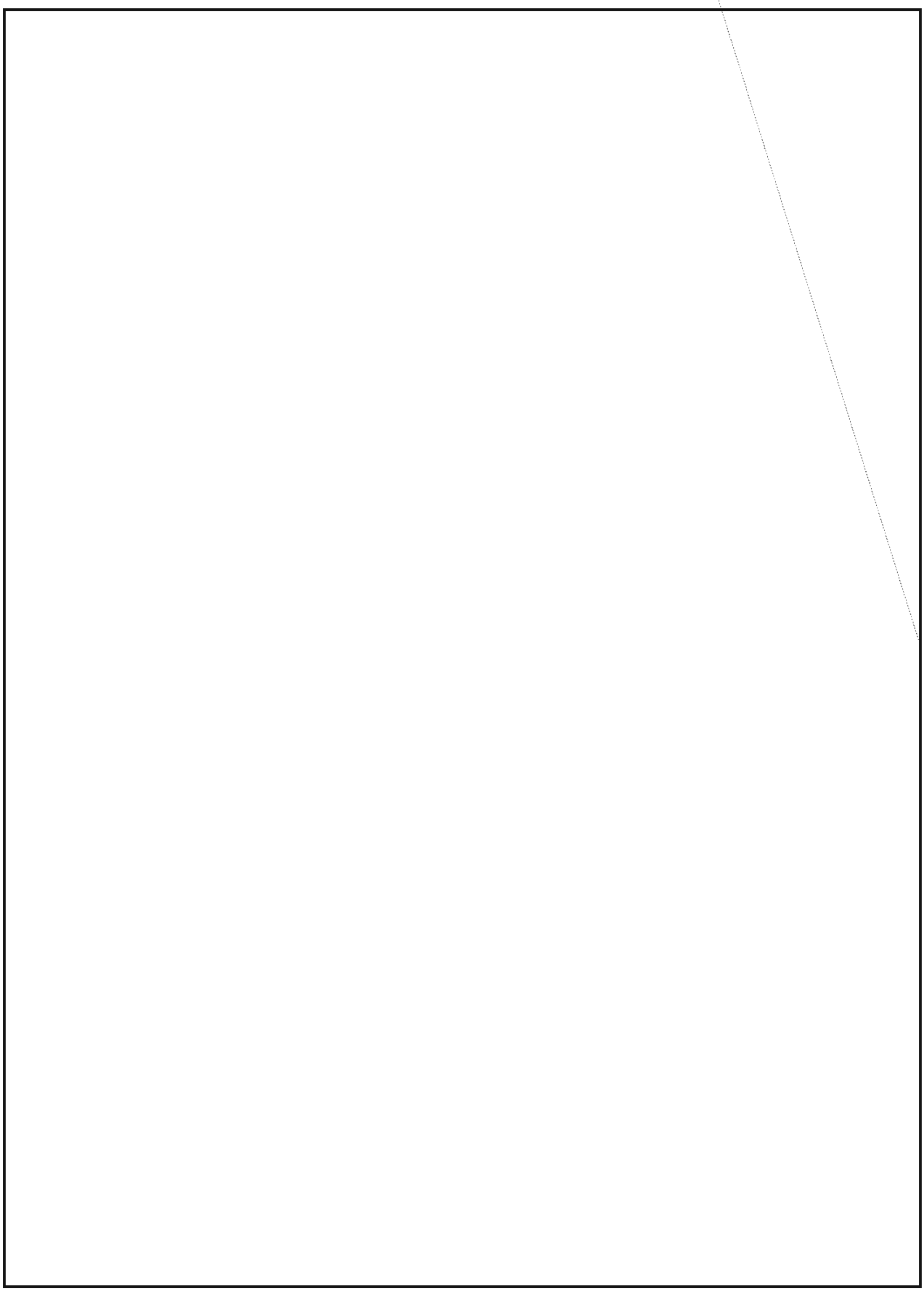
~~TOP SECRET~~

20 YEARS OF TRANSPOSITION

E1 P.L. 86-36







CRY-PTO-LOGROLLING

Have you ever seen puzzles in which the same series of letters "slides" or "glides" through all the words in the solution? As in the following S A M P L E ?

1.	**S**	**A**	M	P	L	E
2.	I	**S**	**A**	I	A	H
3.	E	S	**S**	**A**	Y	S
4.	T	U	S	**S**	**A**	H
5.	C	A	B	A	**S**	**A**

Letters used

√√√	√	√	√√	√√	√√	√	√	√	√√√	√	√	√
AAA	B	C	EE	HH	II	L	M	P	SSS	T	U	Y

Definitions

1. Specimen
2. Hebrew prophet
3. Short literary compositions
4. Fabric made of cultivated silk
5. Percussion instrument made of a hollow gourd enclosed in a net of threaded beads for use in a Cuban band.

This type of puzzle is variously called "slide-o-gram," "glide-o-gram," "step-o-gram," etc. But the CRYPTOLOG editor thinks that the letters do not slide, glide, or step at all. Instead, they *roll* through the words. So, in the puzzle below, roll the letters CRY through. On page 12, roll PTO through. And, finally, on page 20, try your luck at LOG-rolling.

1.	C	R	Y						
2.		C	R	Y					
3.			C	R	Y				
4.				C	R	Y			
5.					C	R	Y		
6.						C	R	Y	
7.							C	R	Y

Letters used

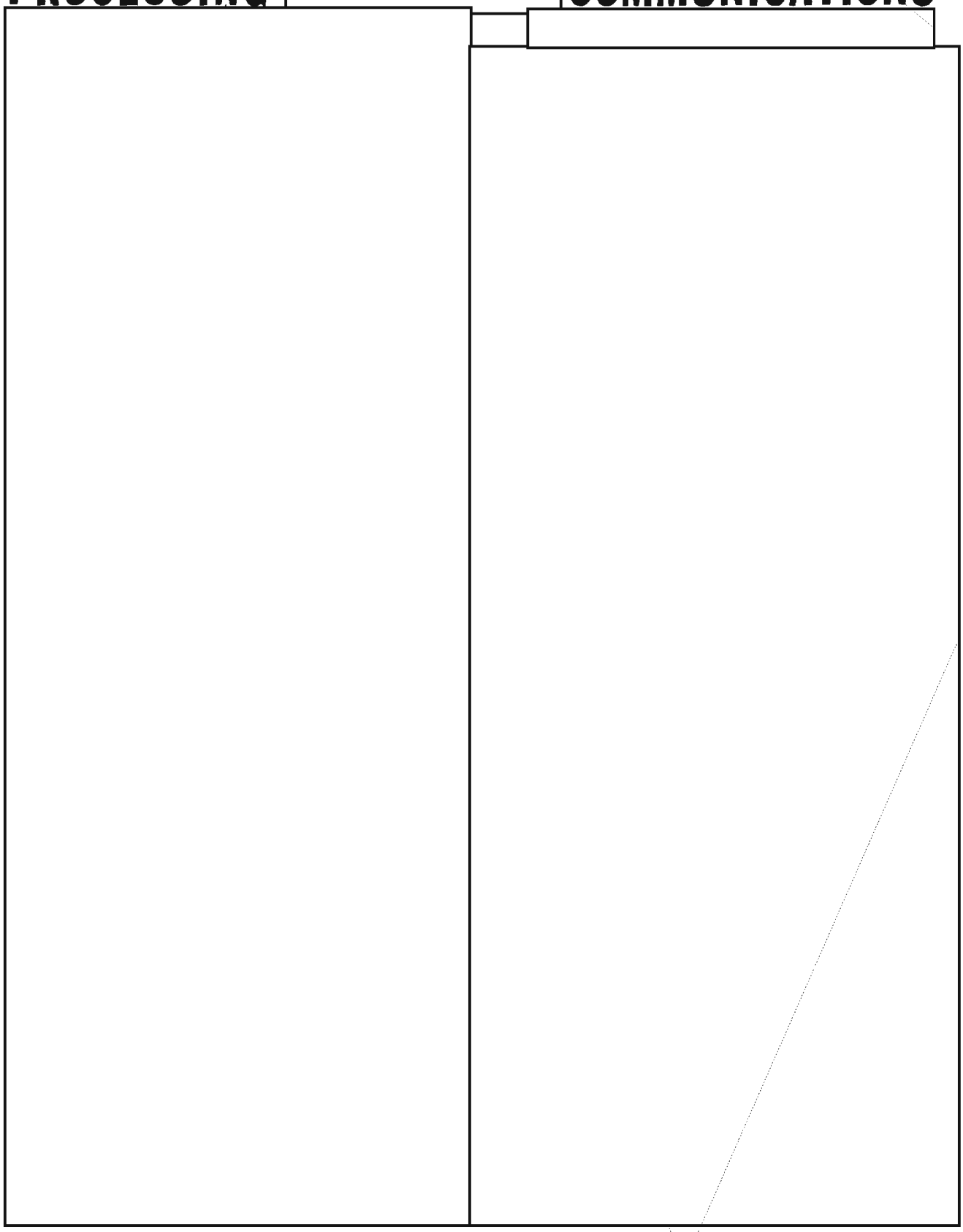
AA DDD EEEEEE F GG III LLLL
NNNNN OOOO PP R SSS TTTT U X

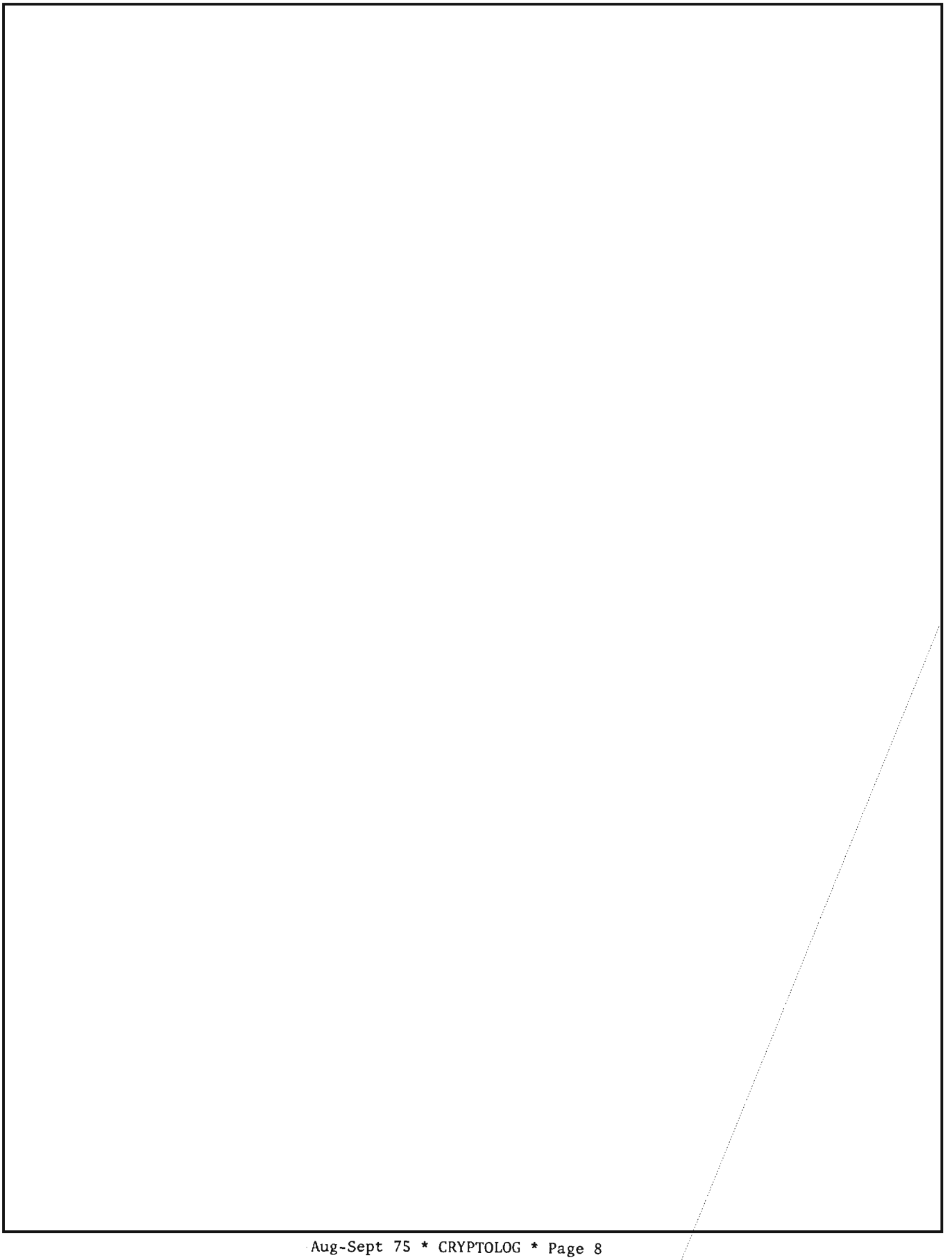
Definitions

1. NSA publication
2. Salts or esters of $CH_2CHCOOH$
3. Encoded or enciphered
4. Discovering
5. A crystal foreign to the rock in which it occurs.
6. Possible trade name for a bread to be served at smorgasbord (2 words)
7. In hot pursuit (3 words)

Puzzles on this page and pages 12 and 20 are UNCLASSIFIED.

PROCESSING [redacted] COMMUNICATIONS





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

The Voynich Manuscript: Third Theory

Boris Miller, p16

When a newspaper editor needs a filler, he can always fall back on the Loch Ness Monster or the Abominable Snowman. For the editor of a cryptologic magazine the obvious device is another blurb on the subject here discussed. So, evidently, thought a former editor, among whose effects the following paragraphs were found.

Is the Voynich manuscript "real"? No. Is it a hoax? No. What is it, then? A make-believe--an elaborate fantasy produced purely for the satisfaction of the maker.

That was my reaction the first time I looked at it closely, but faced with all the profound theories about it I lacked the courage to say so. However, a recent rereading of Elizabeth Friedman's article in the Washington Post (August 5, 1962) and of Brigadier Tiltman's paper in the NSA Technical Journal (Summer 1967), plus some phenomena I have seen in the meantime, have emboldened me to give the world the benefit of my thoughts.

Some of the pertinent facts brought out in the above two sources are:

The exact number of symbols is uncertain, because of what may be variant forms and also because some apparently single symbols may in fact be two. Spacing appears to be random and punctuation completely absent. Paragraphs nearly always begin with one of two favorite symbols, which also occur frequently in the top lines of paragraphs, where there is some extra space. The number of different "words" is quite limited, and the same vocabulary appears in all sections, whether the content (judged by the illustrations) is botanical, biological, or astronomical. The "words" average four and a half symbols each, with very few of only one or two symbols, or of over seven. There are no erasures or corrections. Some of the commonest words occur several times running, but there are no repetitions of whole phrases, such as would be expected in any scientific text.

Brigadier Tiltman concludes that this is no natural language: "Languages simply do not behave in this way." On the other hand, it is equally impossible, for cryptologic reasons, that it can be the result either of simple substitution or of transposition. He draws no conclusions as to the nature of the text, but in this story I will be the truth-telling child who says rashly and cheerfully, "The text is nonsense."

This theory has always been disparaged on the assumption that no one would go to such lengths to produce a book without meaning. Who would have the time and the patience? What would be the point?

Well, first, the book presumably had some meaning for the originator, but this meaning may be in the pictures rather than in the text. As for time-- All through history many people have had more time than they knew what to do with: prisoners...invalids...unmarried aunts in well-to-do families. Empty hours stretched on into empty years, frightening years, and a long, long project would be something to cherish.

Suppose an imaginative woman chose to take up drawing instead of needlework, or suppose that a prisoner of state had a flair for art; and suppose that either of these, being illiterate (not unlikely at that time) but quite capable of imitating writing, decided to pass the time by creating a splendid book. A model book, so to speak. It makes as much sense as dollhouses, or boats in bottles; and you can make it life-size.

Or suppose that a country gentleman of means and learning has suffered an illness that leaves him slightly balmy. He spends his days in the field communing with the flowers or in his study painting impressions of them. (Look at those plants! They are lurid, even menacing, like Van Gogh's sunflowers; they are larger than life, with an animal shagginess and strength about them, and look as if they might well have dictated the whole project themselves.) He spends his evenings communing with the stars and depicting them. Neither his planets nor his plants bear much resemblance to reality, but he is living an intense inner life.

He decides to make a book. The writing skill remains in his fingers, but his brain no longer remembers the connection between the signs and the sounds. So he develops an alphabet of his own, of signs he enjoys making, and fills up the book with what amounts to "psycholcgical random" groups of these. At his death his family quietly lays the book away, and when it discovered years later, no one any longer knows its history.

Creative but frustrated people adopt strange means of self-expression. In Watts, California, stands a group of towers--the tallest a hundred feet high--built by a poor tilesetter out of steel rods, mesh and mortar, and covered with

mosaics made of bits of tiles, dishes, bottles and seashells. It took him 33 years, working without a plan, without assistance, without scaffolding--climbing, as he built, with a window-washer's belt. Then he gave the land to a neighbor and moved away. Why did he work so long on a useless fantasy? "I had in mind to do something big," he said, "and I did."

In the Smithsonian Institution stands the "Throne of the Third Heaven of the Nations' Millenium General Assembly": a room-sized composition of chairs, tables, pedestals, cardboard cutouts, old jelly glasses, used light bulbs, pieces of mirror--all covered with "gold" and "silver" foil and assembled into an astonishing and magnificent structure. It was built, over a period of 14 years, by a Washington laborer, in a garage he rented for the purpose, and was discovered only after his death. Its purpose or meaning is unknown.

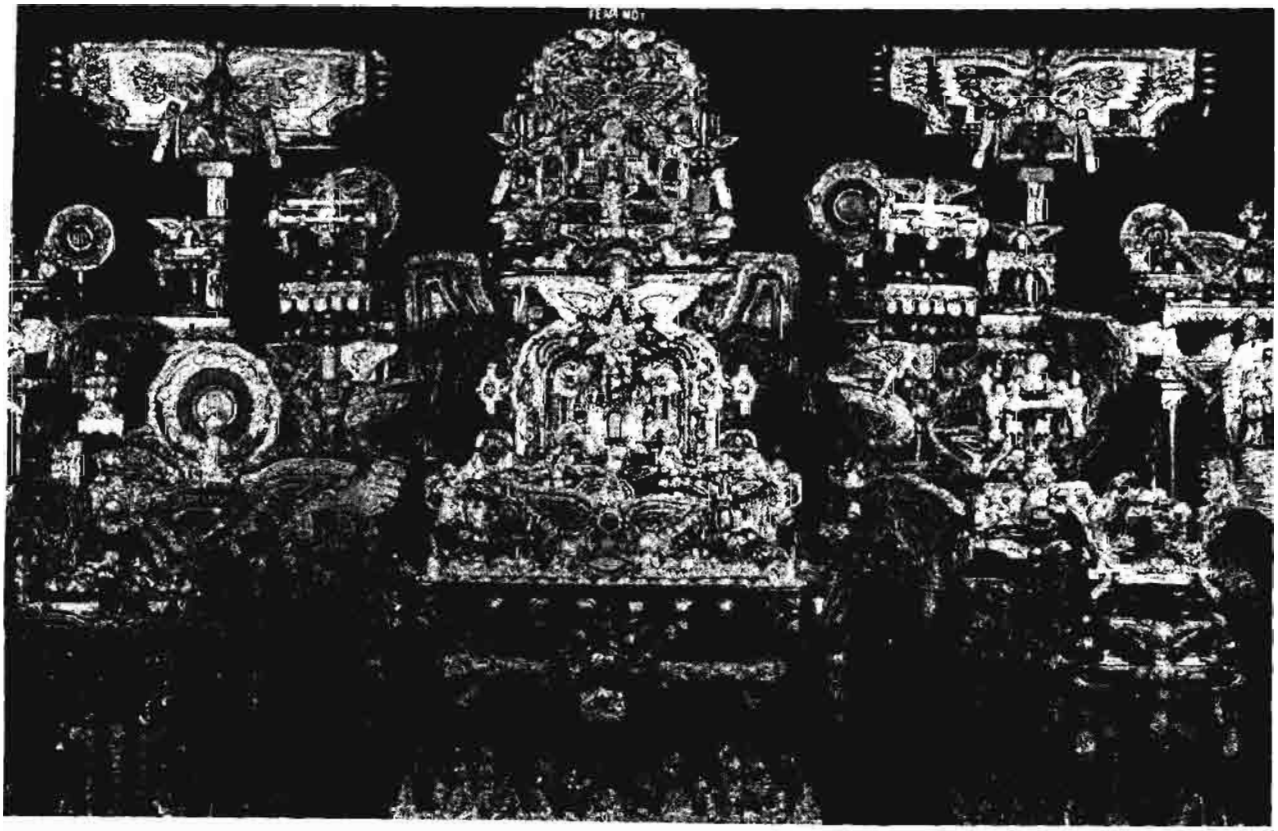
But, you may say, they at least produced something tangible--a work of art. So did the maker of the Voynich manuscript--a fascinating work of art; and the "text" may serve the same purpose as the mosaics on the towers or the foil-covered bulbs on the "Throne"--it is part of the general effect.

It is possible, of course, that the writer also harbored a secret hope. A record called "The Gift of Tongues (Glossolalia)," issued by the Scepter Company, purports to be the voice of a man "speaking in tongues." It takes the hearer only a few minutes to become convinced that the man is inventing: the sounds do not pour out spontaneously, but haltingly and lamely, with an embarrassing amount of repetition. Is the speaker a fraud? Not necessarily: he may naively suppose that this ability to invent is actually the fabled gift of tongues, and that even though he has to search for the sounds, the Power that permits him to find them also knows their meaning...

In any case, why assume a message where there is no evidence of one? Visually, the pages are a joy, and if the "text" turns out to be written glossolalia, or abstract art, why not?

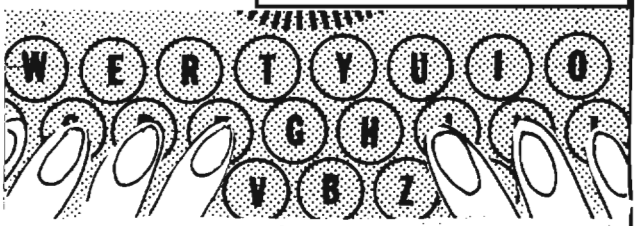
"I had in mind to do something big," says the author, "and I did."

Yes, we do have a copy of this famous manuscript in the Crypt Library (Room 3W076), and you may like to go and see it. But there are a lot of other things in there more worthwhile -- in fact, we've been trying for some time to get an article on the library. Any volunteers?



Photograph by Charles Phillips,
courtesy of Smithsonian Magazine

TYPEWRITER RANDOM -- A NEW LOOK.



The right hand-left hand test for possible 'typewriter random" generation of key is an old standby. We might apply another test involving movement to the right or to the left on the keyboard. Under the two tests, quite different interpretations would arise concerning the following group:

Text	8 6 9 6 0
Right hand-left hand	R R R R R
Directional	L R L R

One theory would be that the right hand only was used in typing the group (since numbers 6 through 0 are normally typed with the right hand). Another possibility is that a "two-fingered" (hunt-and-peck) typist used his two fingers alternately.

The equiprobable measure does not apply when the directional test is used (e.g. there are millions of ways to produce RLRLRLRLR, but only one case gives RRRRRRRRR).

Random probabilities have been computed for trinomes, tetranomes, and pentanomes. The probabilities labeled "*with*" are for text in which groups with doublets (the "hits") category) have been retained. The "*without*" probabilities apply when groups with doublets are not counted.

TRINOMES

	With	*Without*
LL	.12	.148
LR	.285	.352
RL	.285	.352
RR	.12	.148
Hits	.19	

TETRANOMES

	With	*Without*
LLL	.021	.029
LLR	.087	.119
LRL	.1695	.233
LRR	.087	.119
RLL	.087	.119
RLR	.1695	.233
RRL	.087	.119
RRR	.021	.029
Hits	.271	

PENTANOMES

	With	*Without*
LLLL	.00252	.0038
LLLR	.01638	.0250
LLRL	.04938	.0753
LLRR	.02892	.0441
LRLL	.04938	.0753
LRLR	.10317	.1572
LRRL	.06192	.0944
LRRR	.01638	.0250
RLLL	.01638	.0250
RLLR	.06192	.0944
RLRL	.10317	.1572
RLRR	.04938	.0753
RRLL	.02892	.0441
RRLR	.04938	.0753
RRRL	.01638	.0250
RRRR	.00252	.0038
Hits	.3439	

~~(CONFIDENTIAL)~~

KEEP ON ROLLING!

1.	P	T	O						
2.		P	T	O					
3.			P	T	O				
4.				P	T	O			
5.					P	T	O		
6.						P	T	O	
7.							P	T	O

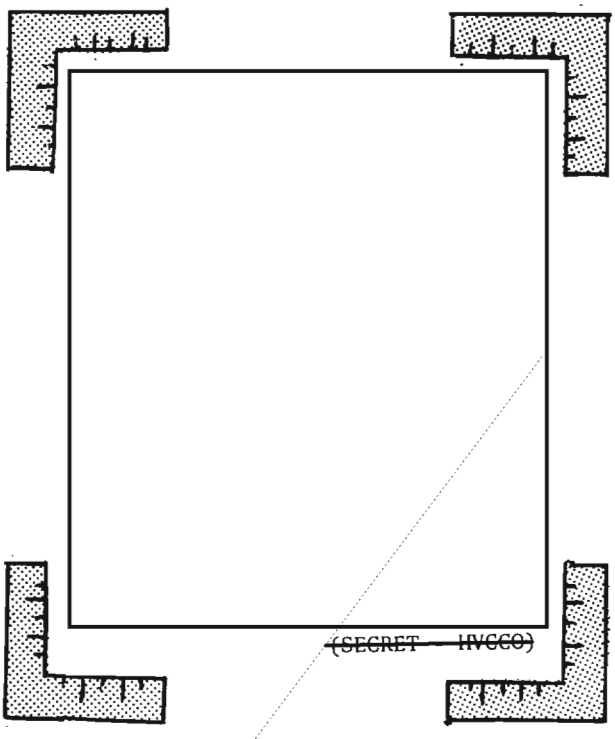
Letters used

A CC EEEEE GGG H IIIIIII LLL M NNN OO P RR S TTTTT UU V W Y

Definitions

1. Of or relating to the Greco-Egyptian rulers of Egypt from 323 B.C. to 30 B.C.
2. Those those live in the residential section of a city
3. Walking or proceeding quietly or cautiously
4. Popular monthly
5. Incapable of performing something (4 words)
6. The highest degree or extent (2 words)
7. Utter (3 words)

(UNCLASSIFIED)



~~(SECRET -- HVCCO)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

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

A FIX FOR THE LANGUAGE PROBLEM?

JOHN B. THOMAS, JR., Special Assistant, Language, A9

An "old hand" proposes a management tool that might be of help to deal with a perennial "bucket of worms."

P.L. 86-36

Doris Miller's article "Language and the COMINT Production Process" (*NSA Technical Journal*, Summer 1974) falls gracefully into [redacted] category of "What oft was thought, but ne'er so well express'd." It is for good reason that that article won the First Prize in the Crypto-Linguistic Association's 1975 Essay Contest.

I would like to expand this subject in the same general vein, by:

- supplying a kind of postscript dealing with some specific points about voice language work and the role of the military;
- examining the paradox: If these ideas were indeed "oft thought," why hasn't more been done about them?
- suggesting a methodology and management posture by which the working linguist's and the working linguist-manager's wisdom and observations can be converted from a still small voice into a real help for higher management.

Looking first to the voice problem, I would caution that we are on shifting ground in this area. Miss Miller discusses things that specialists almost unanimously feel should be done. She considers the problem to be one of enlightening and persuading management to put some force behind the ideas she projects. The voice problem, on the other hand, I think finds even specialists with more uncertainty about standards and procedures. This is no wonder.

The Voice Explosion is terrifying. [redacted] You zip voice tracks back and forth in fancy machines, and then you get more fancy machines to zip printed transcripts back and forth. But no "machine" can *produce* a transcript. Finally, you bite the bullet and admit that the human transcriber remains the heart of the business. [redacted]

[redacted]

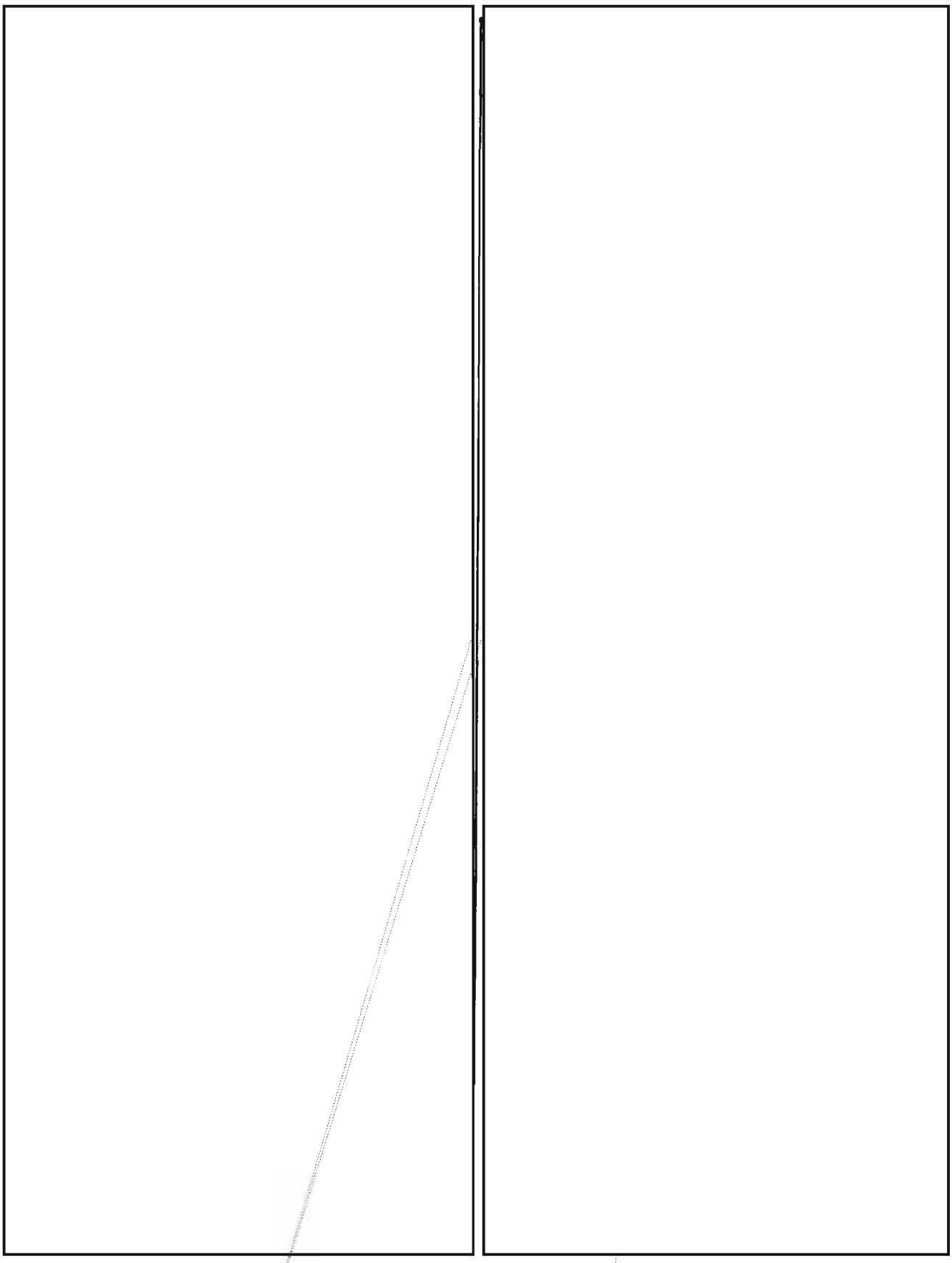
We need all the help we can get. Channel identification, [redacted] and any other possible selection processes need to be exploited to the fullest to put the best possible intercept, the richest of all the ore, before the transcriber.

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

Does everyone fully realize that, until the magical "machine transcriber" appears, the voice language processor is the valve through which the whole production stream must flow? Some realize it and apply the unfair, pejorative term "bottleneck" to him. But the term is passive, whereas the transcriber is active. In fact, only in the degree to which he is active is any intelligence possible. And a person carrying out a key (that is, critical) process deserves to be recognized with at least a positive-sounding term. "Key processor" sounds awkward, but it is certainly accurate.

[redacted]

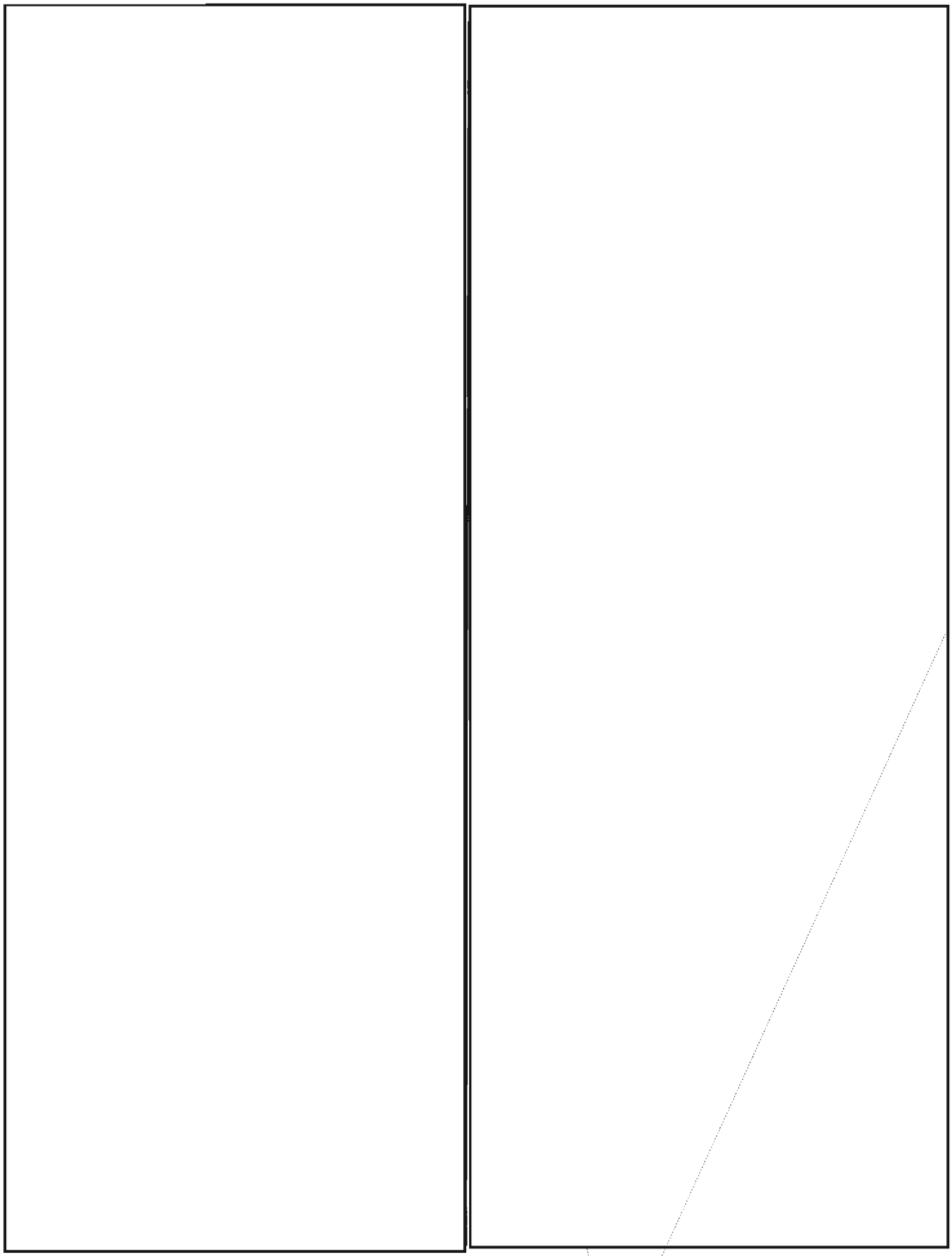
EO 1.4.(c)
P.L. 86-36



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

P.L. 86-36

~~SECRET~~



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

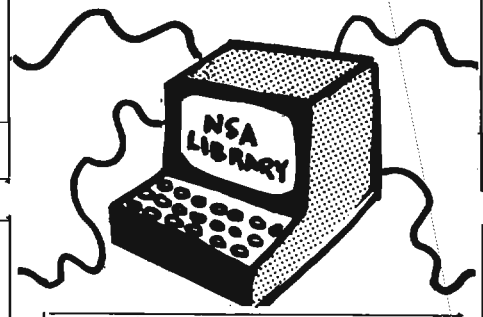
EO 1.4.(c)
P.L. 86-36

~~(SECRET - HVCCO)~~

NSA ON-LINE ACCESS TO OUTSIDE SOURCES OF INFORMATION

FTD
USAF Foreign Technology Division, Dayton, Ohio
Foreign scientific-technical literature
Location of terminal: Room 2N090, 5759s

DDC
Defense Documentation Center, Alexandria, Va.
DoD research and development information
Location of terminal: Room 2N090, 5759s



An article on NSA's computer network resources will appear in a future issue of CRYPTOLOG.

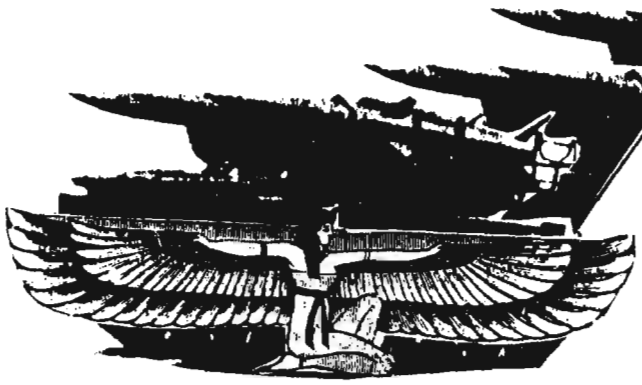
(UNCLASSIFIED)

OCLC
Ohio College Library Center, Columbus, Ohio
Book collections of 400 libraries in network
Location of terminal: Room 2N111, 4084s

NYT
New York Times Data Bank, New York, N. Y.
Index to NYT and certain other publications
Location of terminal: Room 2C051, 3358s

ABDUL & HIS 40 TANKS

Frederic O. Mason, Jr. PJ1



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

LINGUISTS -- WE NEED AN "EXPERTS YELLOW PAGES"!

Time was when a translator had to be extra careful when dealing with the difference between "request" and "demand" or with the exact rendition into English to indicate just how miffed or mad or scared the original drafter of the message had been. Life was simple then, or so it seems now. The *subject matter* in the messages was "general liberal arts," although the language of diplomacy was always much more precise than the language appearing in the daily press. But U. S. interests are a bit more complex and technical now, and so are the subjects that our message texts deal with. Our general-purpose dictionaries, or even our specialized dictionaries, are neither up to date nor up to it.

Simultaneous interpreters advise us to study, in advance, English-language reference aids dealing in general with the subject matter that is likely to be discussed in the foreign language. But we NSA-ers can't always do this. Not when a single translator might have to deal with *specifics* of:

Letter to the Editor

To the Editor, CRYPTOLOG:

Hurrah for CRYPTOLOG!! This little monthly technical publication offers all of us SIGINTers a much-needed informal forum for the exchange of ideas, particularly for highly controversial subjects in need of clarification and resolution. In this process of written debate we all have an opportunity to express an opposing viewpoint, thereby bringing closer a consensus of understanding that we can all subscribe to. The major ingredient required is that the proponent know something about the subject matter involved. Unfortunately, some of the writers state their views with conviction based upon limited background experience. Such views can be dangerous because they are frequently misleading, and sometimes utterly wrong.

The latter type of erroneous view requires an immediate rebuttal before it gains even minimal credence. The anonymous letter in the June issue of CRYPTOLOG (deriding my earlier letter in the May issue) is just such a letter riddled with fallacies -- not just one, but THREE at least. It's fortunate for the author that he did not sign his name to such a gaffe.

1. Nowhere in my letter is there a hint or intent to belittle the contribution or value of the cryptanalysts. I have the highest respect for their specialized expertise, but, really, they are not always needed in the exploitation of codes or charts.

2. Mr. Noname makes his worst error (and most damning self-indictment of his technical knowledge) by assuming that

3. The bookbreaker,

He does it by deductive reasoning, hard, painstaking work, and the maximum use of his language skill and background knowledge of the target.

Time and space do not permit me to comment on Mr. Noname's statement about "true SIGINT production." I'll take a rain check for that one.

~~(SECRET SPOKE)~~

LANGUAGE IN THE NEWS

WASHINGTON POST
Friday, July 4, 1975
By Douglas B. Feaver
Washington Post Staff Writer

The National Transportation Safety Board moved yesterday to repair one of the most potentially dangerous flaws in U.S aviation—the possibility that pilots and air traffic controllers might not understand each other. . . . .

The misunderstanding in the TWA crash was of the terms, "cleared for approach." . . . . the controller at Dulles told the plane, "You're cleared for . . . approach to runway one two."

. . . . those words meant that the plane was authorized to descend only to 3,400 feet until it crossed a navigation point known as Round Hill. Then it could drop to 1,800 feet and continue its approach to the runway.

A recording of the crew's conversations that was recovered from the wreckage showed that crew members briefly debated the meaning of those instructions as they looked at their navigational charts . . . .

Different pilots who testified at the hearing gave different interpretations of what "cleared for approach" meant to them. . . . .

(U)

LAST CHANCE!

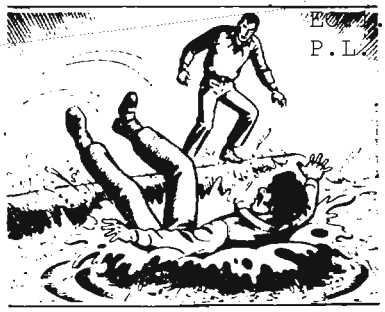
1.	L	O	G					
2.		L	O	G				
3.			L	O	G			
4.				L	O	G		
5.					L	O	G	
6.						L	O	G
7.							L	O	G

Letters used

AA B CCCC DD EEE G HH III MM NN OOOOO PPPP R SSS T UU YYY Z

Definitions

1. A dispute over words
2. Express tersely or as to induce action or instill opinion or belief
3. Inflammation, especially of external parts of the body
4. Freed from obstructions
5. Of or relating to soil science; of or relating to child study
6. Phrenology (usually used disparagingly)
7. Guess!

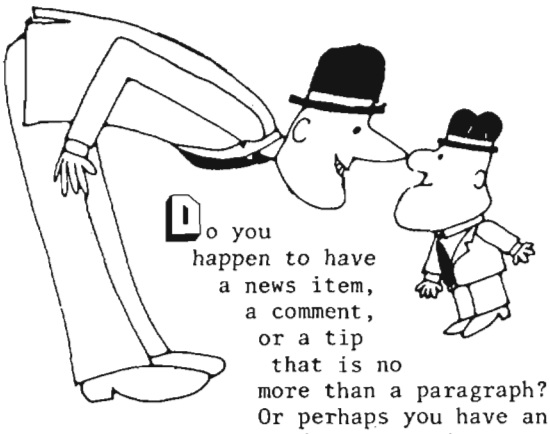


E.O. 14.(c)
P.L. 86-36

In case you fell off somewhere, the answers to all three puzzles will appear in next month's issue.

(UNCLASSIFIED)

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words...? Long or short, if it has something worthwhile to say, we'll print it. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

First-person articles or stories about your own experiences are welcome, so long as they relate to our work. (See "Busman's Holiday" in August 74 issue.)

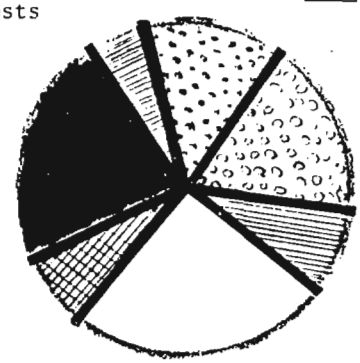
Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

Photographic illustrations can be reproduced, at the same quality as those in the NSA Newsletter.

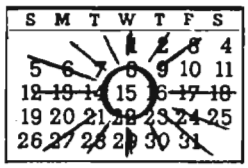
Sensitive materials? No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exclusive sources.

Your contribution does not have to be typed; we'll give preference to content over form, every time. (Though, especially in the case of a long piece, the editorial eye will appreciate any effort you can make in that direction--garbles and strikeovers freely forgiven.)

Something missing? *If you feel that* <u>your</u> work or <u>your</u> interests are not being well represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.

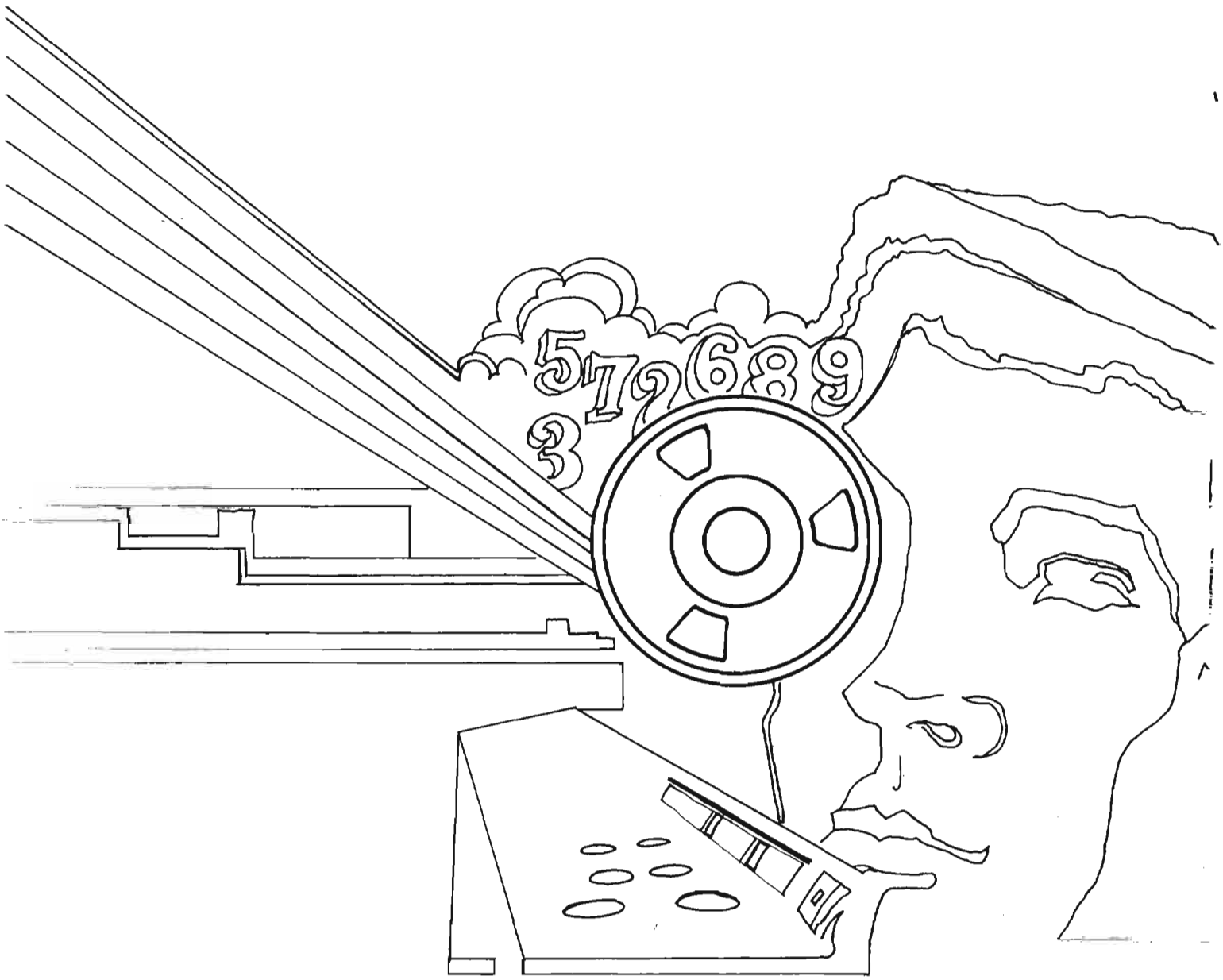


Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't quite know what to do with. A call to the appropriate departmental editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Our deadline is theoretically the middle of the month (the 15th of August, for publication in October, and so on), but don't let that stop you if something good comes along on the 16th. And anyhow, this is a monthly publication; if you miss this month's deadline you'll be just in time for next month's CRYPTOLOG. See you!

P1-Aug 75-S3-24041


5726893