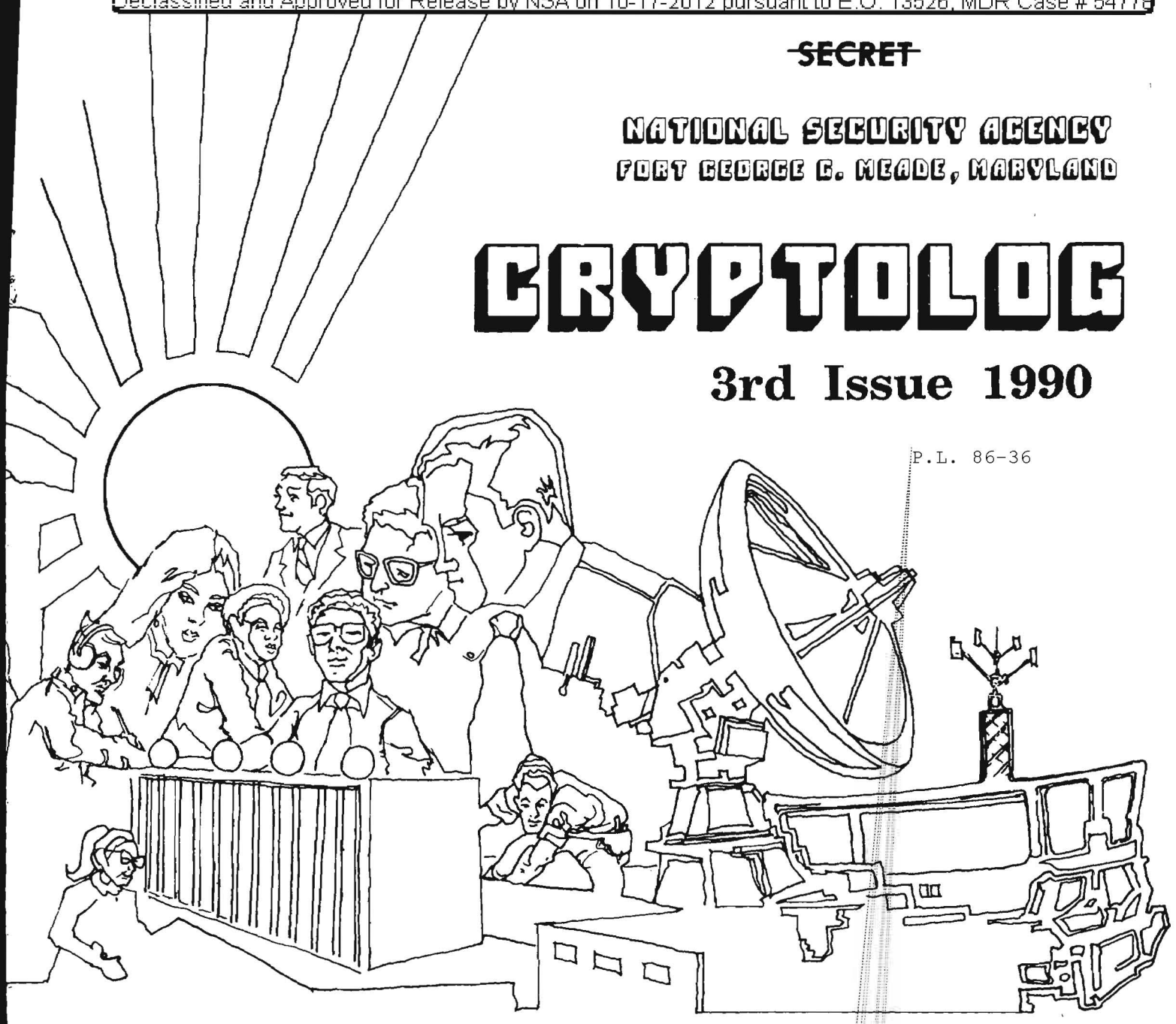
DOCID: 4012034
Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1990



P.L. 86-36

HAIRCLOTH . . . . . [redacted] . . . 1
UNCLASSIFIED FACTS. . . . . [redacted] . . . 7
QUOTE WITHOUT COMMENT . . . . . [redacted] . . . 8
AURAL LANGUAGE IDENTIFICATION . . . . . [redacted] . . . 9
SIFTING WHEAT FROM CHAFF. . . . . [redacted] . . .14
LETTERS 18, 33
THE MAYAGUEZ INCIDENT . . . . . [redacted] . . .19
THE THREE FACES OF COLLECTION . . . . . [redacted] . . .21
HOW IT STARTED. . . . . .David Gaddy. 22
HOW THE FRIEDMAN AUDITORIUM DID NOT GET ITS NAME! . . . . . [redacted] . . .23
TECHNICAL LITERATURE REPORT . . . . . .David Harris 25
EDITORIAL 30
BOOK REPORTS: DOUBLESPEAK . . . . . [redacted] . . .31
. . .HOW TO EDIT A SCIENTIFIC JOURNAL . . . [redacted] . . .32
GOLDEN OLDIE. 36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

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

~~NOT RELEASABLE TO CONTRACTORS~~

DOCID: 4012034

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVII, No. 3 . . . . . .3rd Issue 1990

PUBLISHER. . . . . [redacted]

BOARD OF EDITORS

EDITOR . . . . . [redacted] (963-1103)

Computer Systems . . . . . [redacted] (963-1103)
Cryptanalysis. . . . . [redacted] (963-5238)
Cryptolinguistics. . . . . [redacted] (963-4382)
Information Resources. . . . . [redacted] (963-3258)
Information Science. . . . . [redacted] (963-3456)
Information Security . . . . . [redacted] (972-2491)
Intelligence Reporting . . . . . [redacted] (963-5068)
Language . . . . . [redacted] (963-3057)
Linguistics . . . . . [redacted] (963-4814)
Mathematics. . . . . [redacted] (963-5566)
Puzzles. . . . . [redacted] (963-6430)
Science and Technology . . . . . [redacted] (963-4958)
Special Research . . . . . .Vera R. Filby (968-5043)

Classification Officer . . . . . [redacted] (963-5463)
Bardolph Support . . . . . [redacted] (963-3369)
Macintosh Support. . . . . [redacted] (968-7315)
Illustrator. . . . . [redacted] (963-3360)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH

If you used a word processor, please include the floppy or cartridge with your hard copy, with a notation as to what computer, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five: note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

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

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

Contents of CRYPTOLOG may 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.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

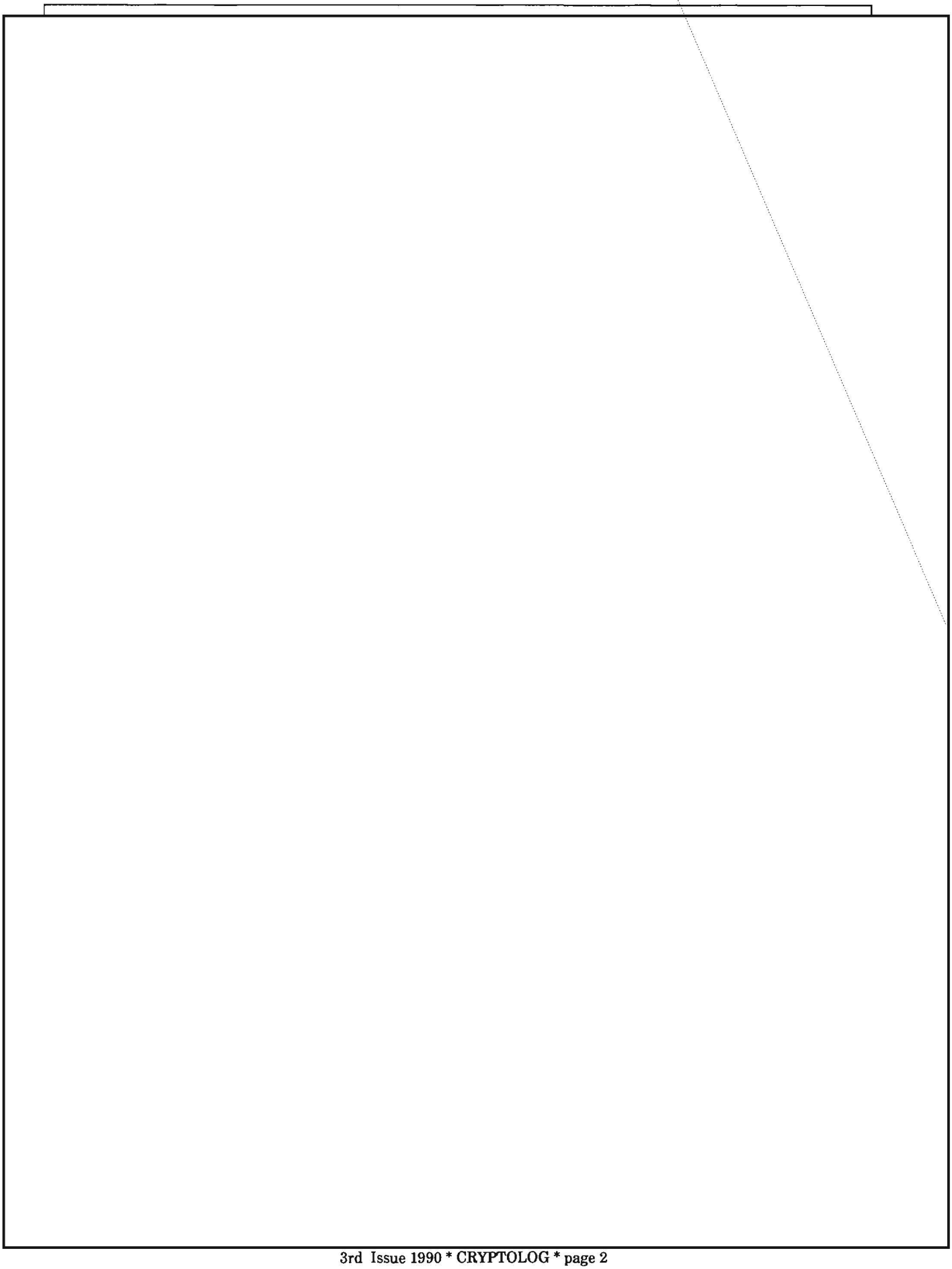
HAIRCLOTH

P.L. 86-36

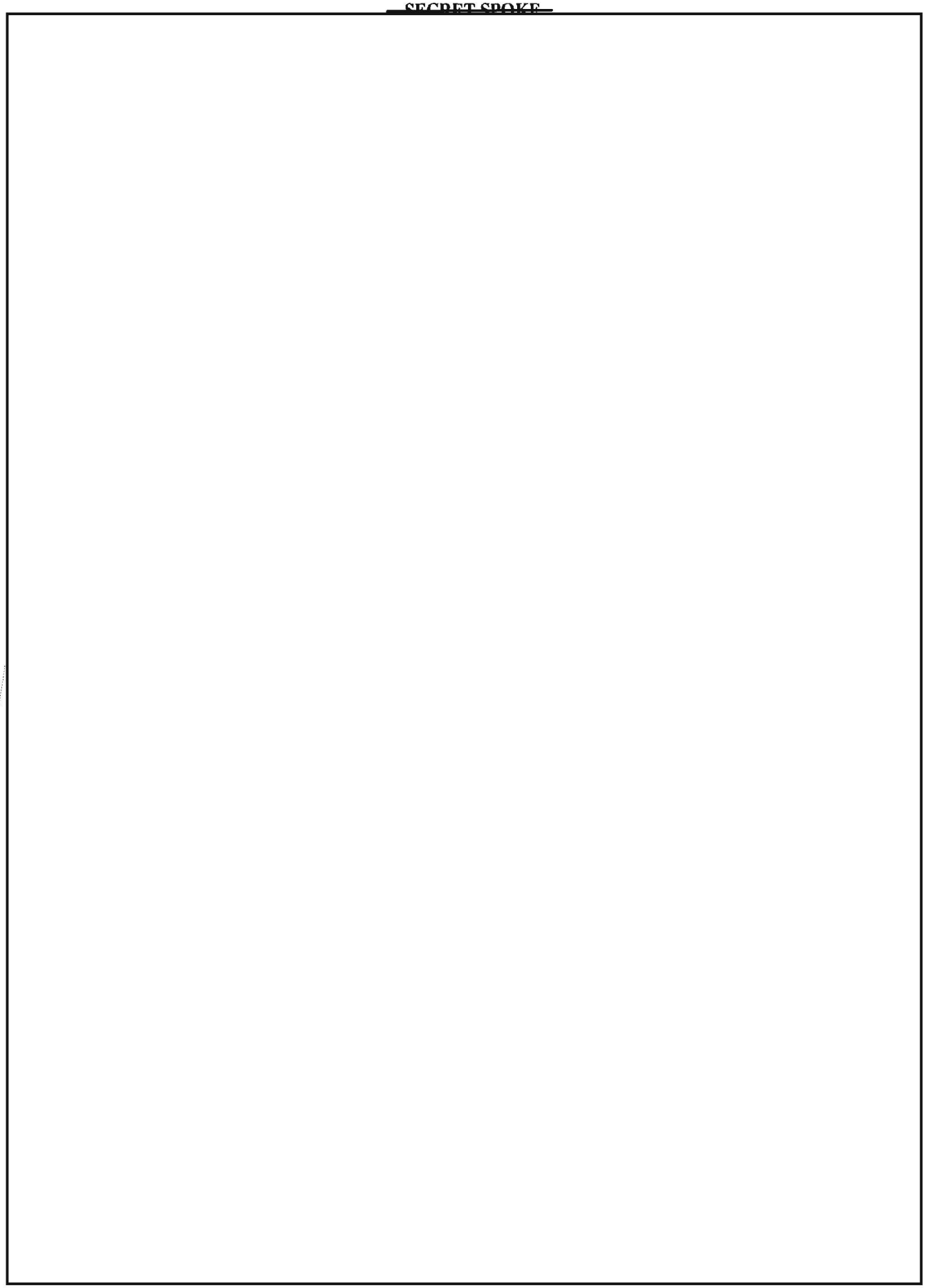
EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

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



DOCID: 4012034

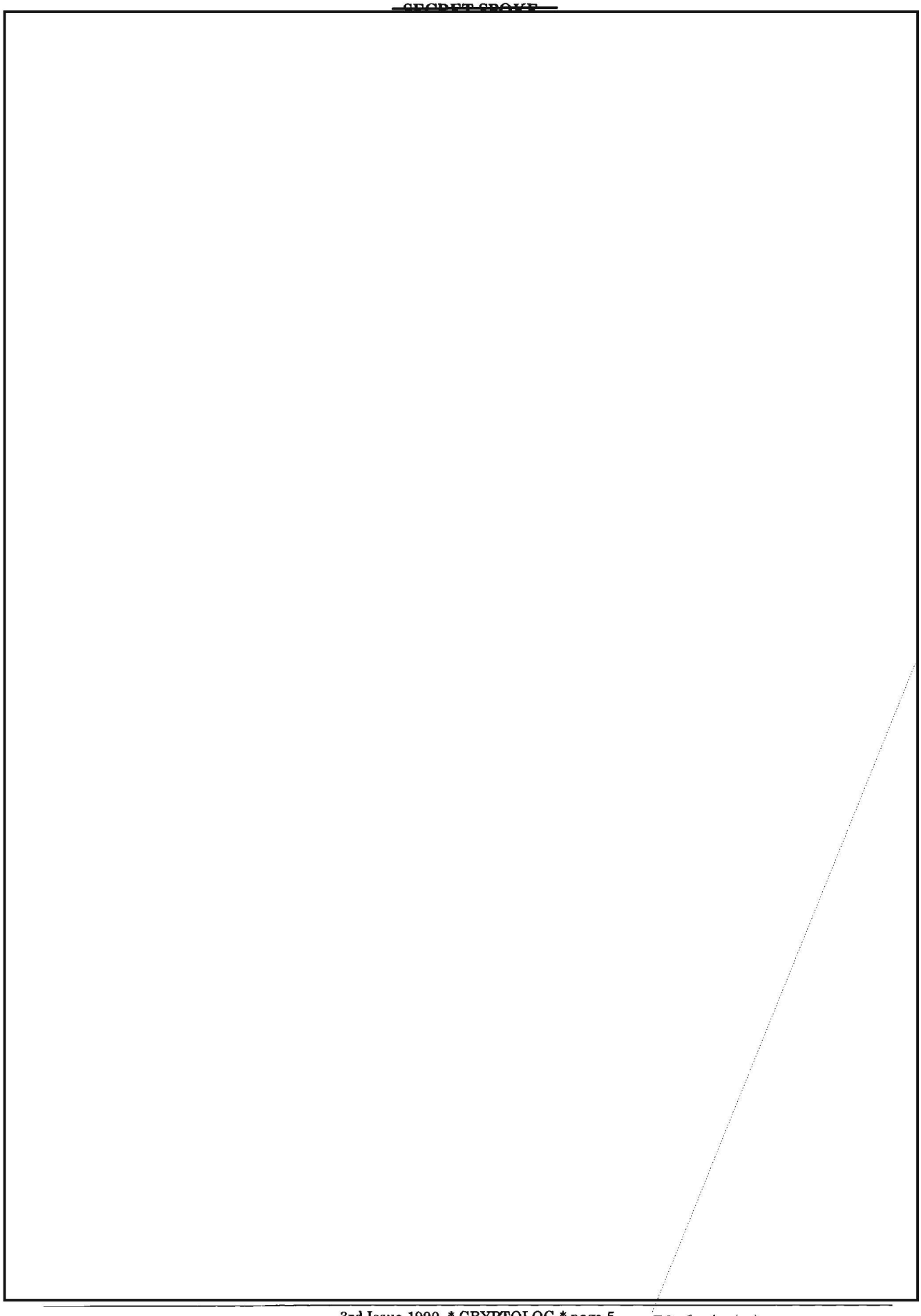


EO 1.4.(c)
P.L. 86-36

DOCID: 4012034

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

DOCID: 4012034



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

DOCID: 4012034

SUBSCRIPTION TO CRYPTOLOG

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

- ❒ Please enroll me as a new subscriber
- ❒ Please check my current mailing address
- ❒ Please change my mailing address
- ❒ Please change my name
- ❒ Please remove my name from the mailing list because I am
  - ❒ retiring or resigning
  - ❒ going to a field site
  - ❒ taking long-term training
  - ❒ too busy to read CRYPTOLOG (though I know I'm missing a lot)

OLD NAME AND ADDRESS

_____
Name (Last, first, mi)

_____ _____
Org *Bldg*

CURRENT OR NEW NAME OR ADDRESS

_____
Name (Last, first, mi)

_____ _____
Org *Bldg*

Mail to: **Editor CRYPTOLOG**
P1 NORTH

Asphalt and related bitumens (native):					
Bituminous limestone & sandstone & gilsonite	short tons	1,980,562	$8,879	1,918,748	$8,561
Carbon dioxide, natural (est.)	1,000 cu. ft.	1,109,530	191	1,194,836	144
Coal: Bituminous and lignite[2]	thous. short tons	602,932	3,772,662	560,505	2,795,509
Pennsylvania anthracite	thous. short tons	9,729	105,341	10,473	100,769
Helium: Crude	thousand cubic feet	4,030,000	47,992	3,992,600	46,843
Grade A	thousand cubic feet	647,000	17,405	759,800	21,599
Natural Gas	million cubic feet	21,920,642	3,745,680	20,698,240	3,455,615
Natural gas liquids:					
Natural gasoline and cycle products	thousand 42-gal bbls.	206,305	603,024	201,784	603,084
LP gases	thousand 42-gal bbls.	399,611	672,088	378,457	498,927
Peat	short tons	526,000	5,986	565,760	7,055
Petroleum (crude)	thousand 42-gal bbls.	[illegible]	[illegible]	[illegible]	10,426,680
Total mineral fuels		...	$20,152,974	...	17,965,000
N[illegible] (except fuels)					
Abrasiv[illegible]	short [illegible]	[illegible],134	[illegible]	[illegible]1	$600
Asbestos	short tons	125,314	10,696	125,936	10,648
Barite	Thousand short tons	854	12,800	1,077	15,753
Boron minerals	thousand short tons	1,041	86,827	1,020	81,261
Bromine	thousand pounds	349,748	60,560	391,883	87,990
Calcium-magnesium chloride	short tons	4	4	4	4
Cement: Portland	thousand 376-lb. bbls.	381,001	1,268,718	400,883	1,284,600
Masonry	thousand 280-lb. bbls.	21,275	67,537	23,253	69,106
Natural and slag	thousand 376-lb. bbls.	4	4	4	4
Clays	thousand short tons	53,932	258,332	58,694	264,415
Emery	short tons	4	4	4	4
Feldspar	long tons	4	4	673,985	8,869
Fluorspar	short tons	269,221	13,923	182,567	8,411
Garnet (abrasive)	short tons	18,837	1,936	20,458	1,874
Gem stones (estimate)		NA	2,396	NA	2,390
Gypsum	thousand short tons	9,436	35,132	9,905	38,354
Lime	thousand short tons	19,747	286,155	20,209	280,736

UNCLASSIFIED FACTS

[redacted] *P05/SAO* P.L. 86-36

We make continual efforts to protect our classified facts to the degree that we sometimes forget to acknowledge the unclassified ones that should not be revealed outside of official channels. Of course, there is no way every unclassified fact with which NSA is associated could actually be compiled. Below is a list of unclassified facts that are most frequently asked about in the Operations Organizations and that fall in that category:

❒ The terms "signals intelligence" (SIGINT), "communications intelligence" (COMINT), "electronic intelligence" (ELINT), and "foreign instrumentation signals intelligence" (FISINT) when used out of context.

❒ Elementary principles of traffic analysis, military cryptanalysis and cryptography.

❒ Individual job titles and descriptions that do not contain information otherwise listed above as requiring classification. (NSA regulation 10-11 provides unclassified job titles and job descriptions.)

❒ The "fact of" overhead reconnaissance.

❒ The mere "fact of" SIGINT liaison or collaboration between NSA and GCHQ, CSE, DSD, GCSB, UKLO, CANSLO, AUSLO, or NZLO.

❒ The terms "NSA/CSS Representative Alaska," "NSA/CSS Representative Europe," "NSA/CSS Representative Pacific," [redacted] and their abbreviations.

❒ Statements forwarded to contractor facilities or other government organizations which disclose the indoctrination status of individuals. This statement is to read: "The individual concerned is certified cleared and indoctrinated for access to TOP SECRET, Special Intelligence," and any other accesses should be abbreviated, such as TK, B, MC, LM, GG, etc.

❒ The caveat "HANDLE VIA COMINT CHANNELS ONLY" and combinations of, or other individual channel caveats, including those identifying the BYEMAN, TALENT KEYHOLE, or LOMA control systems. ❒

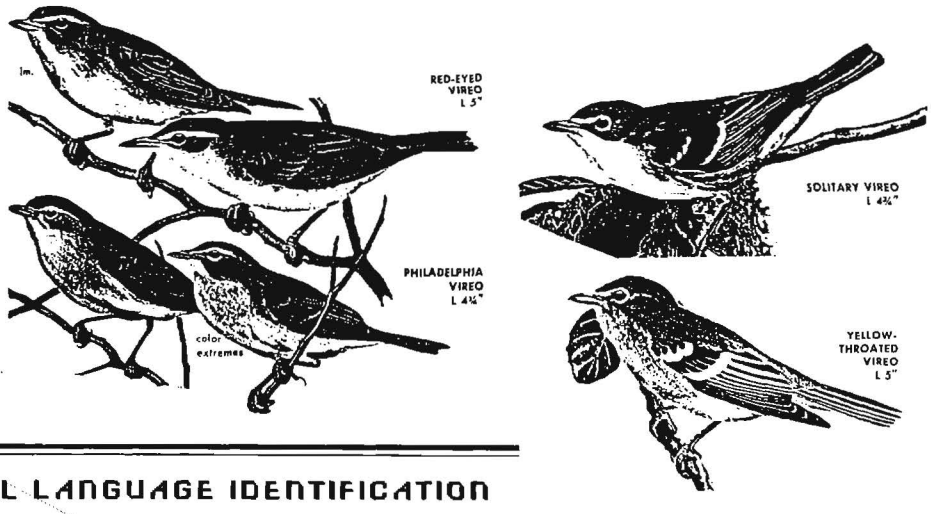
~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

Extract from

"National Cryptographic Habits"
by Preston Currier
Collected Papers on Cryptanalystic Diagnosis.
April, 1969. (S-194-074)

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



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

AURAL LANGUAGE IDENTIFICATION

~~(C-CCO)~~ The problem of identifying spoken languages at the Agency is an old one, as evidenced by the existence of the second edition (1958) of *A GUIDE TO SPOKEN LANGUAGE IDENTIFICATION*, Prod-03 Informal No. 10/2. More recently it was the subject of an article by [redacted] in *CRYPTOLOG*, December 1986, pp. 11-17, "The Language Identification Problem."

P.L. 86-36

~~(C-CCO)~~ When I returned to NSA in 1987 after an absence of 18 years, I was surprised to find it was more of a problem than ever, when [redacted] asked me if I had any ideas on how to solve it. After I had been thinking about it for a couple of months, she sent me a copy of a suggestion by [redacted] that had been adopted by DDO [C-547-85], stating that

[redacted]

[redacted]

(U) [redacted] had been exploring formal features in the same way that distinctive features are used in professional linguistic descriptions, and had even been working by computer to systematize them. But that approach would not work in the situation Barbara had described.

(U) My initial approach was also based on an analysis of distinctive features, but relying on features that are more subjective than scientific. There was one overriding reason for this approach: I had noticed years before that Polish and Spanish sound the same to me when I am far enough away not to distinguish words; this is because both languages are accented predominantly on the penult, the second syllable from the end of the word. I'm told that English and Norwegian have a similar relationship and sound alike if not heard distinctly.

(U) Thus I started on the premise that languages might be classified by their aural impression on a listener, so I compiled a list of seven

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

P.L. 86-36

DOCID: 4012034

classes of language based on predominant accentuation, tone, and vowel, and consonant characteristics. Though some of the principles were useful, this scheme eventually proved to be too cumbersome to be practical. My original analysis is shown in the chart on the next page.

(U) At about this point it became obvious that this process might produce a scheme valid for some uses but not for this purpose. Additional criteria could have been added to form more groups, and more distinctive ones, such as the exact type of stable accentuation, nasality, clicks, retroflex consonants, the presence of "th" sounds, etc., but they would have made the scheme even more complex and unwieldy to be handy.

(U) My next approach was based on field bird study. I used to be able (before losing a lot of my hearing) to identify more than 100 Maryland birds by their songs and calls, sometimes only by one feature which occurs in a stream of notes. At times a family of birds, rather than a single species, can be identified before it is clear what the species is: Vireos are a good example. At other times different species have seemingly identical sounds, so the observer has to listen until a distinctive sound is uttered. In many ways this parallels human language: we do not understand any particular "words" used in bird communication, and perhaps we do not need to know any words in any particular language to identify the language; perhaps we can identify languages by subjective means.

(U) This has a parallel in field ornithology as well. American ornithologists insist that diagnostic markings be carefully observed for positive identification; this would be equivalent to identifying a language by words which are understood. British ornithologists accept the principle of GIS, meaning General Impression and Size; this corresponds to the subjective impression made by the sounds and mannerisms of the call.

(U) Take the bird family Vireonidae, for example. Vireos are small birds, olivaceous and grayish in color, often hard to find and to see clearly, and best identified by their songs. Six vireos can be found in Maryland. Four have predominantly robin-like phrases (comparable to a language family) and can be identified by song as follows:

> *Red-eyed vireo:* short, frequently repeated phrases [This can be compared to Chinese].
>
> *Solitary vireo:* short phrases, slower than red-eyed [This can be compared to staccato Hungarian phrases].
>
> *Yellow-throated vireo*: diagnostic "three-eights" note [This "distinctive" feature can be likened to clicks in Hottentot].
>
> *Philadelphia vireo*: very close to red-eyed vireo, but more mellifluous and slower. [Comparable to Estonian "overlong" vowels].

(U) The ability of the listener to identify the language is what is important, even if the guidelines are unscholarly. If linguists find (as some have) that Japanese sounds like Turkish, but is more "singsongy", the only question is: Does it work? Subjectively we find that for some people Greek is thin and Armenian is thick, Romanian is like Italian with more sh sounds, Portuguese is like Spanish spoken with a cold, and even that "Zulu reminds me of Italian." Whatever works is correct.

~~(FOUO)~~ Eventually I reorganized my findings and in the fall of 1987 presented them in a course at NCS listed as LG-220, Aural Identification of Languages, to ten students. The final course was organized with a combination of three potential approaches: distinctive features, subjective impressions, parallels with bird calls.

~~(C-CCO)~~ The results of the session were mixed. Everyone seemed able for a time to distinguish some of languages we started with. Some, who had to deal directly with collection in the field during the period spanned by the course, found that they could isolate their priority languages and eliminate others quite well. Other students could not identify certain languages at all.

DOCID: 4012034

Initial Distinctive Feature Analysis

Class 1/2 vowels

	glottal	dominant accent	long vowels	tone	example
1	+	-	-	-	Tagalog
2	+	-	+	-	Spanish
3	+	-	+	+	Hungarian
4	+	-	-	-	+ Lingala
5	-	+	-	+	- Ilocano
6	-	+	-	-	- Kurdish
7	-	-	+	-	- French
8	-	-	-	-	- English
9	+	-	-	+	- Serbian

These criteria were based on my observation of how I hear the languages.

1/2 vowels means broadly that there are many open syllables (i.e., ending in a vowel rather than in a consonant), which can make a language sound either very deliberate or fast.

Glottal refers to any sound deeper in the throat than normal American English sounds and therefore includes glottal stops and pharyngeal sounds.

Dominant accent means a predominant emphasis on the first, last or penultimate syllable.

Long vowels refer to languages where long and short vowels are phonemically different, sometimes difficult to determine without knowing the language because vowels are often lengthened for the sake of emphasis.

Tones refer to higher and lower pitches used in a consistent manner. ~~(S-CCO)~~

(U) Some members of the class never did accept the fact that the purpose of the course was immediate recognition of the language being heard. They wanted to follow their own instincts to identify languages by words which they understood. The great drawback here, as [redacted] has already pointed out in the paper mentioned above, is that there are recognizable cognates in many languages, so language identification based on words alone is flawed from the start.

P.L. 86-36

(U) Despite the early mixed results and mixed student evaluations the course has continued, and several sections are taught every year, mainly to students going on TDY and PCS. Happily, the two sessions given in FY90 received uniformly favorable student evaluations.

METHODOLOGY

(U) As is common in teaching practice, we try to go from the familiar to the unknown. Everyone seems to recognize French—why or how that is, I'm not even sure of the correct question to ask here—and almost everyone is quite sure of German, Spanish and Chinese. From there on we are on less secure ground.

(U) I begin by classifying the main accentuation pattern of non-tonal languages with practice for each type. We use four patterns:

first syllable (as in Hungarian, Czech, Estonian),
penult (Polish, Spanish, Italian),
last syllable (French, Turkish, Hebrew) and
mixed (Russian, Tagalog and Albanian).

(U) From here we move on to other features which are not quite so distinct:

nasality (French, Portuguese),
long vowels (Hungarian, Finnish),
palatalization (Russian, Chinese),
retroflex consonants (Hindi, Tamil),
tone (Asiatic: Chinese, Vietnamese; and African: Bantu languages, Malagasy), etc.

(U) The major Romance languages are presented as follows:

French nasal and final accentuation
Spanish penult accentuation
Portuguese nasal and penult accentuation
Italian penult accentuation and long consonants
Romanian like Italian but mixed accentuation and many sh and sht sounds.

(U) Some languages are hard to characterize, i.e., all Slavic languages have many palatal consonants, but Russian adds a great deal of vowel palatalization. Unfortunately the only way to classify Ukrainian is by the lack of this vowel palatalization, and ultimately perhaps it can only be recognized by those who already have a knowledge of Russian.

(U) The major Slavic languages are presented as follows:

Czech, Slovak accented on first syllable
Polish accented on penult
Serbo-Croatian mixed accent but lilting quality suggesting a tone language
Russian a great deal of palatalization, ya, ye, yo and yu syllables
Bulgarian t sounds in many final syllables, t, ta, te, to
Ukrainian like broken Russian, less palatalization

~~(S-CCO)~~ It may seem at first glance that this is not enough information on which to base the identification of a language, particularly in view of the occasional problems which arise:

[redacted]

[redacted] But-more often, I am amazed at the ability of many students to identify a score or more of languages with facility after just a few hours of training.

(U) Arabic is identified mainly by the wa sound which precedes most clauses; while this is a word meaning "and", it is not presented as a word and knowing the meaning has no real effect on the ability to perceive it and interpret it as an Arabic feature.

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

[redacted]

~~(S-CCO)~~ Recognizing language family is particularly important with creoles and pidgins.

[redacted]

~~(S-CCO)~~ At present we deal with about 50 languages per class, in two different, complementary ways: language families and geographic areas. [redacted] as a major member of the Romance family, but is also reviewed in terms of Central Africa, North Africa and the eastern Mediterranean where Lebanon is located.

~~(S-CCO)~~ The problems involved in the range of languages also include several concomitant

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

situations. One of these is the use of the same language in distinctive dialects in neighboring countries, i.e., Farsi in Iran and Dari in Afghanistan; at present only a person who knows the vocabulary and/or syntactic differences between these two dialects can differentiate them. This

[redacted]

~~(FOUO)~~ We work principally with language tapes provided by the Voice of America because they are clear enough to teach the principles we operate with. We add other languages as required. Even so, the range of languages available does not meet all of NSA's possible needs, and we are constantly looking for new language specimens.

~~(FOUO)~~ Originally, we began by using Jack Gurin's Language Library of recordings (found in the NSA library in the past and now under P16), but many of them were poor because they were recordings of classes; the teacher often used "caretaker" language because of the weaknesses of the student, and the student often had a poor pronunciation. Others were ad hoc conversations between two speakers of a language who had never met before, and the sense of contrivance and artificiality comes through the recordings, making them seem unreliable as real native specimens of the languages.

[redacted]

be sent to collecting stations at home and overseas, as requests keep trickling in for more help in language identification.

(U) Retention is one problem which we face along with all other areas of language training. To enable students to practice and review at home, we have found it possible with our more recent equipment to make special unclassified cassette tapes with many language specimens.

~~(C-CCO)~~ I have speculated about other approaches that might be tried for certain languages. One would be for students to learn the first one or two lessons of some language courses which are on tape or records; in this way they could combine both the word recognition method and the subjective impression method. Two obvious drawbacks are an increase in study time, several hours per language, and the lack of such material in a great many possible target languages.

(U) Another possible method is the time-based versus syllable-based feature, the first of which accounts for the amount of slurring and the second for the degree of clarity and/or staccato in a language. This characteristic requires further investigation.

~~(S-CCO)~~ [redacted] has developed a remarkable computer program for recognizing graphic specimens of languages (I say remarkable because I tested it very successfully with

[redacted]

He believes it can be applied to spoken language after some refinements have been made; if so, and if a small enough device can be developed, the identification problem could be almost completely solved, and LG-220 would have little reason for continued existence.

~~(FOUO)~~ Until then, however, LG-220 is one of the Agency's solutions to the formidable problem of aural language identification. ❐

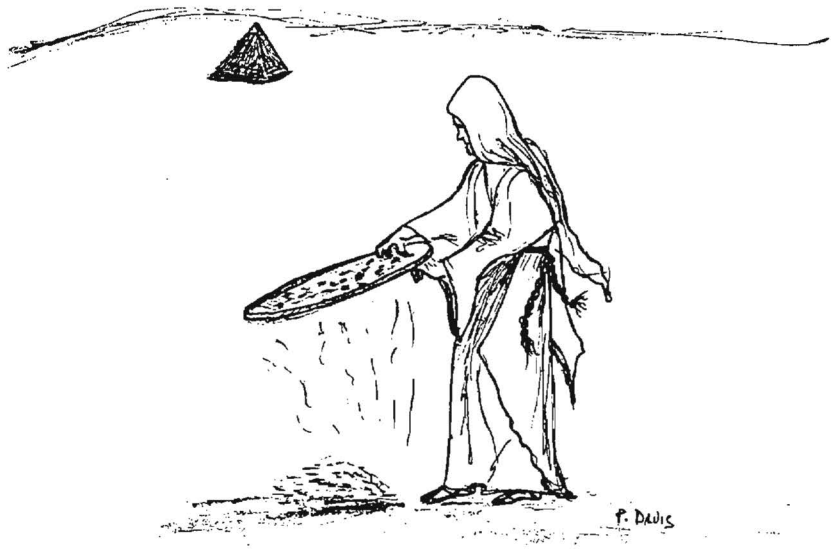
P.L. 86-36

DOCID: 4012034

Sifting Wheat from Chaff

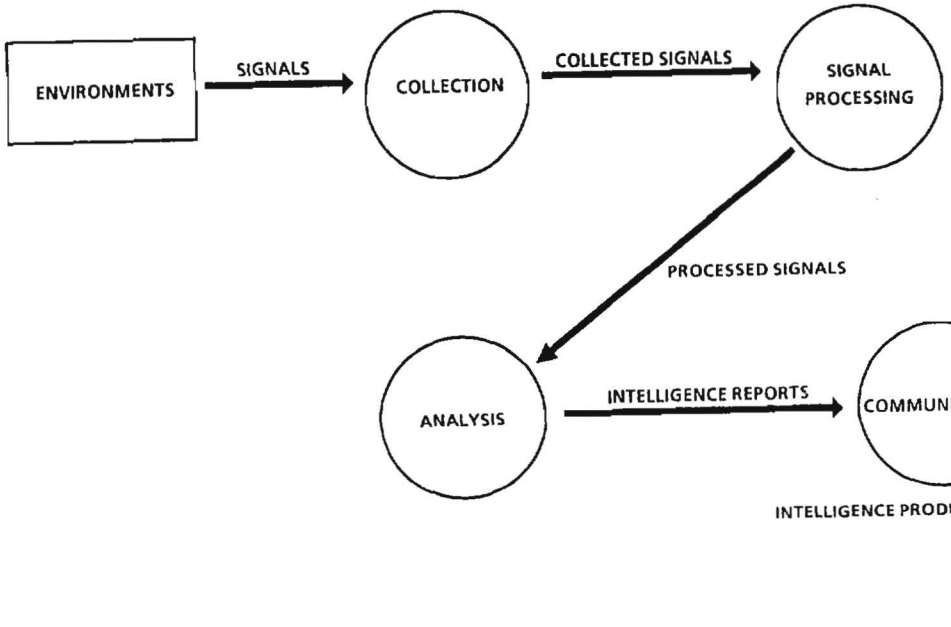
P.L. 86-36

R5



P.L. 86-36

Fig. 1. DATA FLOW



~~FOR OFFICIAL USE ONLY~~

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

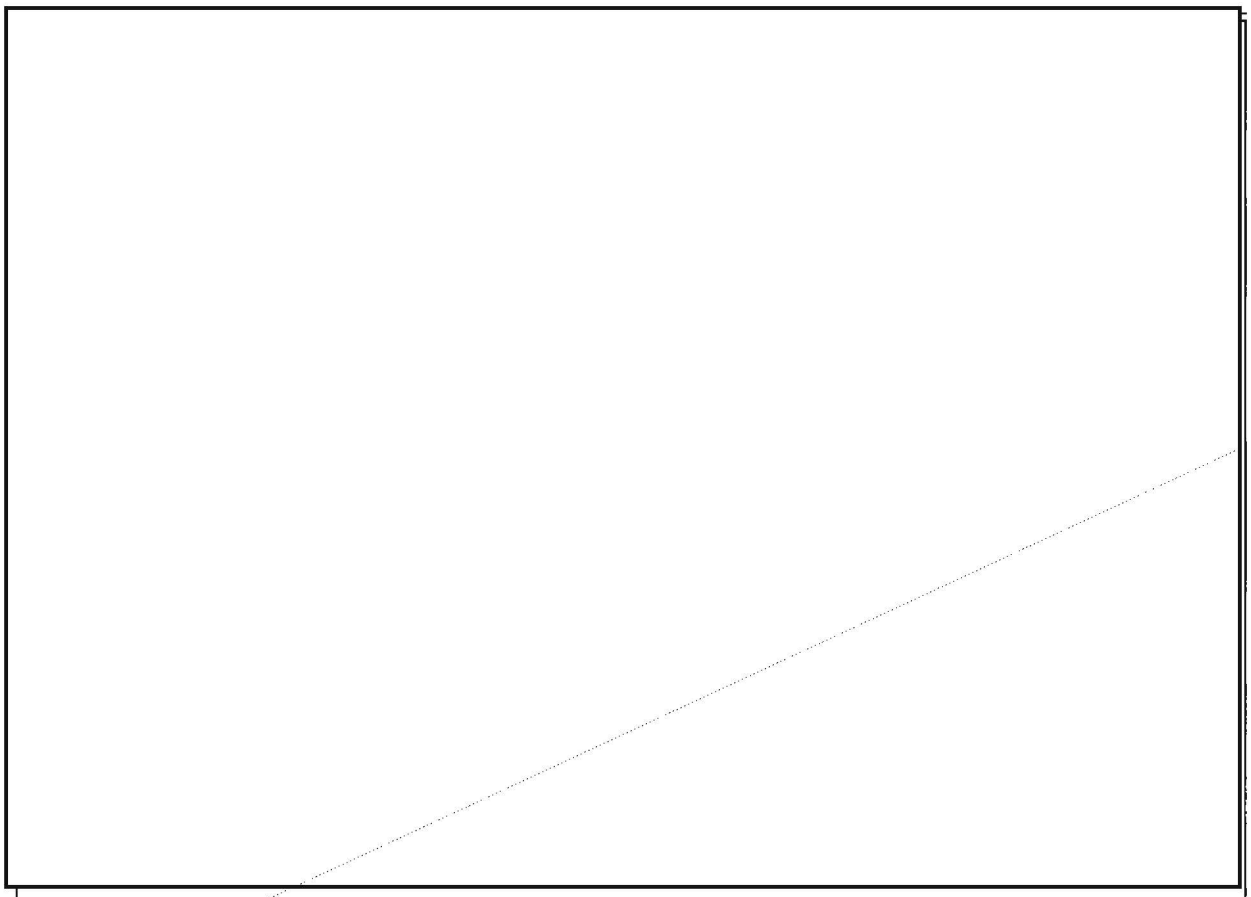
(U) Developing a good characterization of filtering tools will lead to identifying holes and gaps in technological capabilities and to identifying unfulfilled requirements that can be satisfied without new technology. This should not be construed as an exercise in system engineering, system or device design, or building and assembling equipment to do SIGINT.

(U) The key to characterization is clear descriptions of data structures that are passed in the SIGINT system and how they are operated on to produce an intelligence product. Once a function is well understood and described, then science and engineering can proceed with specifics as to what can be done now, and what needs more R&D.

(U) In Figure 1 there is description of the SIGINT system at a top level with a data flow diagram. The problem with this "diode" concept of unidirectional flow is that it displays only the reaction to a signal situation. It does not display a system that must produce product, first based upon who needs data, then the source of the data, and finally, how the data are to be prepared and delivered.

(U) A more accurate snapshot of the SIGINT system is presented by the data flow diagram in Figure 2. The point here is not that Figure 2 is the only way to characterize the SIGINT process, but that the SIGINT System should be shown as a process where the activities interact, share data, and filter (make decisions about) all kinds of data. It is a data flow diagram that stresses the "goes intos" and "goes out ofs" without dwelling on the devices that transform the data. The symbols as shown on the key are defined as follows:

An OUTSIDE INTERFACE is a process or organization lying outside the context of a system that is an originator or receiver of system data;



~~FOR OFFICIAL USE ONLY~~

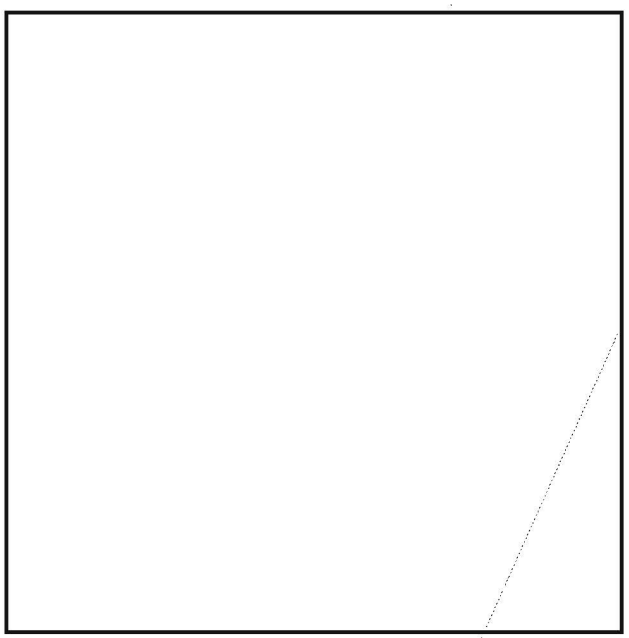
P.L. 86-36

An ACTIVITY is a transformation of input data flow(s) into output data flow(s);

STORAGE is a data store; and

DATA FLOW is a pipeline along which information of known composition is passed.

(U) Data flow diagrams can help characterize what filtering must be done because SIGINT product is produced from data that has been transformed. We must consider data structures in motion, data structures at rest, and the necessary ways to act on them. The diagram shown is only an approximation. The most effective diagram shows how the activity is carried out and has a good data dictionary that correctly describes what the data should be and its form. Filtering may have to include other data to be fused to the flow for good product output.



~~(C CCO)~~ As there are standing requirements for documenting NSA-acquired systems, there is a chance that current filtering techniques are fairly

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

DOCID: 4012094
P.L. 86 36

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

well documented, understood, and therefore characterized.

[redacted]

[redacted]

[redacted]

(U) It should be no surprise that a complete solution to the entire SIGINT problem may be too big to accomplish initially. But we can at least try to see how much of the problem we can grasp, what problems we can identify, and how we can attack these problems.

~~(C-CCO)~~ Currently, we are looking at the following:

LOOKING AHEAD

~~(C-CCO)~~ Is there a stimulus to invent new filtering techniques? Do we have to get serious about characterizing the filters we have, or are they already characterized? The author is hearing all kind of pleas for help [redacted] Yes there is a need, but it is hard to believe enough people have a good grasp of what the

~~SECRET~~ EO 1.4.(c)
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012034

whole SIGINT System really does to glean out the needed intelligence product (the author knows he doesn't have such a grasp).

~~(FOUO)~~ NSA folks must help each other to better understand the problem of SIGINT filtering from an operational as well as a technological point of view. Some of us have problems right here and now with which we are trying to cope (sometimes all by ourselves). Others of us want to talk about what we can do in the future. At times neither group talks to the other, because they are too busy, and some are blinded by their own view of what time tag is most important. Obviously, both aspects have to be considered together to foster a better mutual understanding, a foundation of experience, and some assurance that the current problem of each new day is not a bigger and bigger compounded predicament of the past and present.

~~(FOUO)~~ Is it clear that we'd better get a lot smarter about sifting wheat from chaff if SIGINT is to fulfill its potential? That is an easy question to answer. The harder one is, will the right folks stand up and be counted when the call goes out for input to strategic planning for aspects of the filtering problem, or will there continue to be fragmented efforts to solve such problems without the benefit of both an operational and technological point of view?

To the Editor,

CRYPTOLOG is still very much a winner, providing a very enjoyable break in work when it arrives.

At this time I'm writing to ask for a copy of the do-it-yourself packet on viewgraph preparation described in the 1990 2nd Issue. (With all the high-tech stuff in the National Cryptologic School, where I have been since December, I still find occasions when viewgraphs are the best things to use in my endeavors!)

Please send me a copy of that packet, addressed:

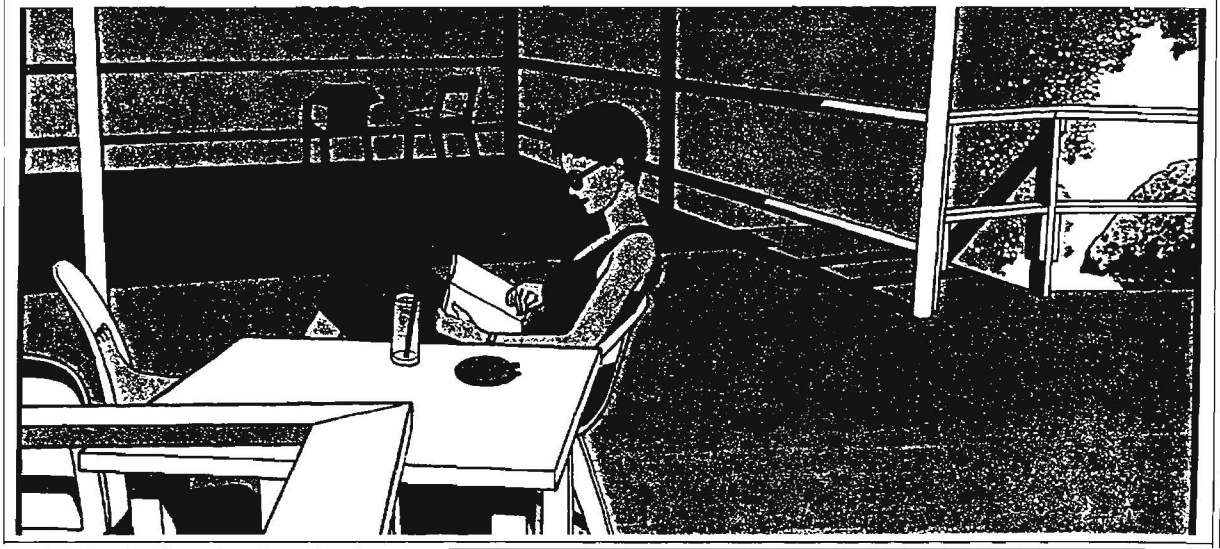
[redacted]
E9
ITB

P.L. 86-36

Thanks, and warm regards.

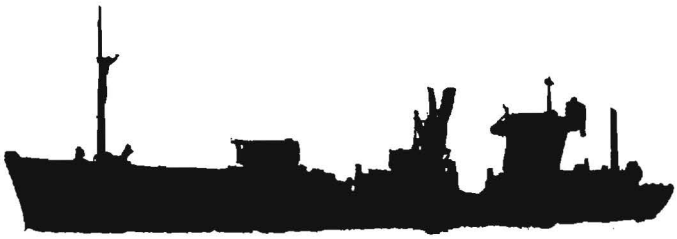
unclassified

CRYPTOLOG is a classified publication. It may not be read in the cafeteria or in other insecure areas.



DOCID: 4012034

THE MAYAGUEZ INCIDENT



[redacted] P.L. 86-36

(U) On 12 May 1975, the SS *Mayaguez*, a US merchant vessel, was seized by Cambodian Communist forces in the Gulf of Thailand. Within two days US Air, Naval and Marine forces launched a rescue operation against Koh Tang Island where the ship and its crew were believed to be held. During this operation, the *Mayaguez* was recaptured and its crew returned. This article described the actions taken by USM-7, Ramasun Station, Thailand, and its personnel in support of the operation.

~~(C)~~ In support of the operation, on 13 May 1975 NSA declared SIGINT Alert One "Vacater" to be used on all SIGINT product relevant to Gulf of Thailand operations. USM-7 was tasked with providing Tactical Reports (Tacreps) and Spot Reports on Cambodian communications relating to the disposition of the SS *Mayaguez* and its crew and to US rescue attempts. In addition, detachments of USM-7 personnel were deployed to several other locations to support these operations.

~~(SC)~~ At USM-7 itself, cast iron (24-hour continuous) cover was provided on eight Cambodian Southwest Region and mainline Morse links. As a result, it issued a total of five Tacreps and four spot reports by the end of the operations. The reports discussed Cambodian defensive activities as well as the results of US actions. Meanwhile USM-7 maintained contact with US Army Security Service, providing informal progress reports to its commander.

~~(SC)~~ The same day the alert was declared, the station commander summoned the NSA Cambodian Technical Representative to USM-7, whom he requested to identify four Army Cambodian linguists for immediate deployment [redacted] (It is interesting to note that the summons came via a two-way radio link, the same one employed at other critical times such as the evacuation of US personnel from Phnom Penh prior to the fall of Cambodia.) Their mission was to search for, intercept, record, translate, and report all Cambodian VHF voice communications reflecting reaction to the recovery efforts.

~~(SC)~~ Within one hour of that initial contact, the five linguists (four Army and the NSA tech rep) and their working aids were flown directly from the nearby Thai air force base at Udorn [redacted] by a US Air Force C-130. Shortly thereafter, the linguists began search efforts and succeeded in isolating several unidentified Cambodian voice links. This search and development effort involved the [redacted] mission, a Strategic Air Command U-2R reconnaissance aircraft.

~~(S-CCO)~~ During the three-day operation, two intercept positions were manned on a 24-hour basis, one for search and development of additional Cambodian voice links, and the other for monitoring the most active frequencies. Immediate one-liner Tacreps were issued through a joint Army-Air Force effort.

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

DOCID: 4012034

~~SECRET SPOKE~~

AREA OF OPERATIONS DEPICTING RELEVANT LOCATIONS

~~SECRET SPOKE~~

~~(S-CCO)~~ The text on which each Tacrep was based was recorded by one linguist, and immediately transcribed and translated by another linguist to provide the follow-up Spot Reports. After the US recovery operation began, [redacted] issued ten Tacreps and nine Spot Reports on the basis of Cambodian voice intercepts. The reports included reflections of Cambodian actions, intentions, and responses to US operation. During the entire Mayaguez operation, all reflections of Cambodian intent were relayed to USM-7 for possible follow-up traffic in HF Morse or voice.

~~(S)~~ In the early morning hours of 14 May, three additional Army Cambodian linguists at USM-7 were briefed, equipped, and sent to [redacted] as interpreters, to assist in US Navy and Marine tactical operations at Koh Tang Island. Their mission was to use bullhorns to advise the Cambodians that the only purpose of the operation was to recover the *Mayaguez* and its crew.

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

~~(S)~~ Of the three linguist sent, only one was successfully deployed to the island, but he was unable to establish contact with the Cambodians. This linguist was later rescued from the island along with the remaining Marine forces approximately eight hours after their deployment. The two other linguists were aboard helicopters that had been damaged by small arms fire and were forced to return to the Thai mainland.

~~(S)~~ On 15 May, another team of three Cambodian linguists was also sent [redacted] After the *Mayaguez* was rescued, when the US prepared to launch a search-and-recovery mission for the US personnel missing in action, the linguists [redacted] prepared a Cambodian text for broadcast and a possible leaflet drop to inform the Cambodians of the mission. But the Joint Chiefs did not concur, so it was not done. The linguists remained on alert aboard ship until their return to USM-7.

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

~~(C)~~ All the linguists deployed returned safely to USM-7 soon after the successful recovery of the SS Mayaguez and its crew on 14 May.

(U) Though the recapture of the vessel and its crew was successful, we were greatly saddened by the loss of our Army, Navy, Air Force, and Marine fighting comrades who gave their lives.

Originally published in the Field Information Letter, *March 1978*

DOCID: 4012034

P.L. 86-36

The Three Faces of Collection

The ongoing DDO restructuring is prompting discussion about what "collection management" is. I am offering my view of it in the hope that it can serve others as well as it has served me.

I believe that Collection management has three components:

◆ *the definition of collection requirements*; This is the process of deciding what we must have in order to produce the information required to satisfy our users' intelligence demands. THIS CAN AND SHOULD BE DONEONLY BY THE TARGET ANALYST.

◆ *brokering Collection*; This encompasses all actions between the statement of collection requirement and performing the collection task. It includes all organizations that traditionally identify themselves as "collection managers," e.g. 04 staffs, P5, A1, G8, B642, etc. Personnel of these organizations have the know-how to convert the collection requirement stated by the analyst into the arcane lingo of our various specialized collection systems.

The "broker" model, drawn from the commercial world, accurately parallels the functions of our "collection brokers:" rather than buying stock ourselves directly from a company, we call on a broker, a specialist who understands the mechanics of the stock market and makes our purchase for us.

As in the commercial world, NSA brokers should also be advisors to their "clients" on the best way to satisfy a requirement. The decision on the requirement; however, always rests with the target analyst. For example, I may call my stockbroker and say I want a long-term investment with a reasonable return and steady growth, "Please buy 100 shares of Amalgamated Circuit Inc." The broker may respond that this has good short term prospects, but for my long term requirements he recommends Integrated Widgets instead. But thenthe choice is mine.

Collection brokers are more than a bureaucratic cog in the cryptologic wheel; they are the human link between the target analysts and the collection system that assures we get the collection needed. This demands an understanding of how the collection systems function and an insight into the true nature of the needs of the target analysts. Regular dialog between analysts and brokers is essential for this process.

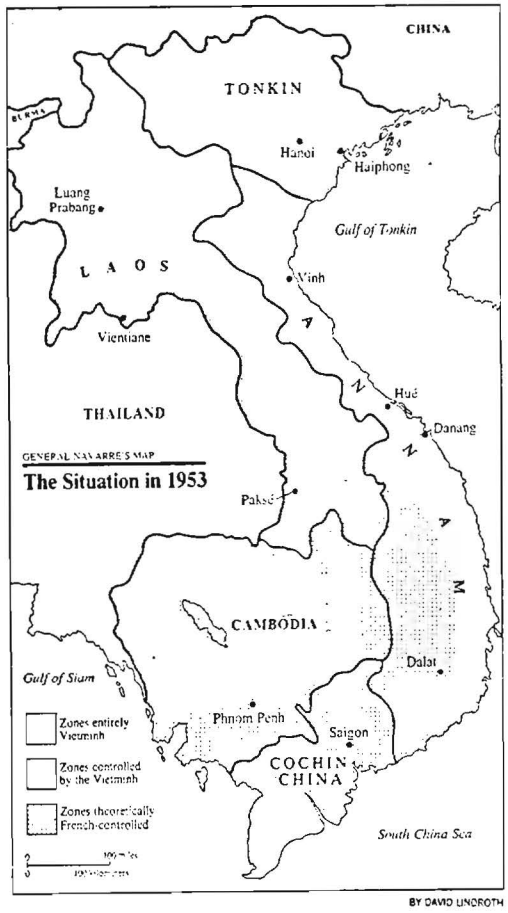
◆ *Collection Evaluation: This is* an assessment as to whether the collection provided actually satisfied the needs of the analytic organization. Perhaps the literal task was completely satisfied, in which case the broker would count it as a job completed, but only the target analysts can say if the intercept provided by the task actually produced the results they were seeking.

In summary, the three components of collection management are collection requirements definition, performed by the target analyst; collection brokering, performed by traditional collection management organizations and; third, collection evaluation, performed by both collection brokers (quantitatively) and target analysts (qualitatively). □

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

HOW IT STARTED



David Gaddy, D9

~~(S-CCO)~~ Last year marked the fortieth anniversary of the problem known for a long time as the "Viet Minh" problem. Forty years. That means 1949 and the days of the Armed Forces Security Agency, AFSA, forerunner of NSA. US involvement in Viet Nam has left a scar on the public conscience that has not yet healed. But it might be time for a little-known account of the SIGINT side.

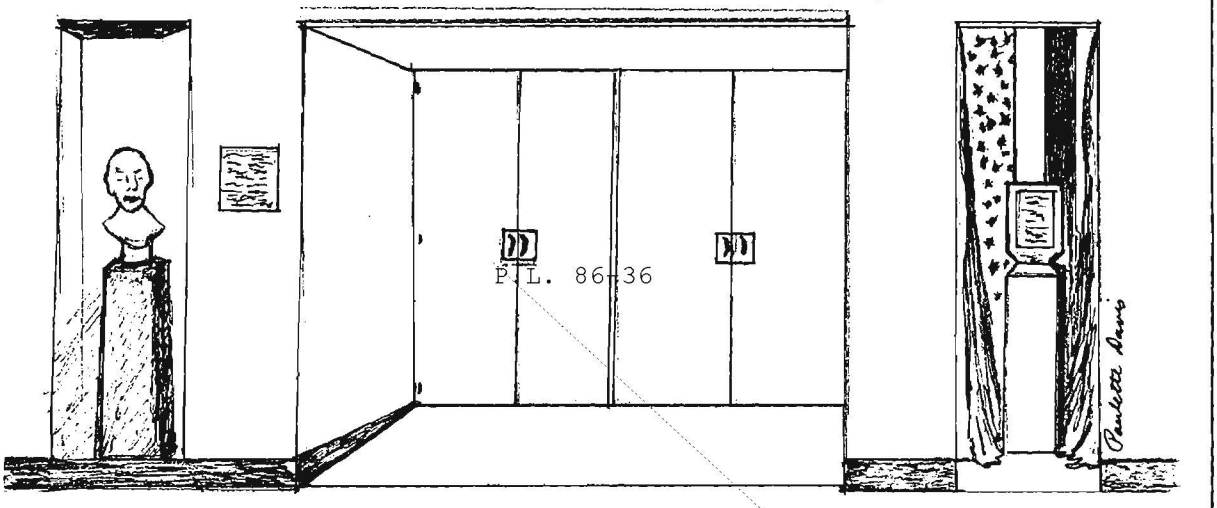
~~(SC)~~ All problems need some lore about their founding, and the Viet Minh problem, as it was called then, has an amusing (and instructive) story. The ingredients are an inquisitive young naval officer and some puzzling new intercept. It seems that USM-9 at Clark Air Force Base in the Philippines had intercepted some strange-looking material. The people at Arlington Hall who puzzled over such things concluded that it was plain text, but what language?

~~(SC)~~ Up pops the Lt (jg.), as I recall the story. He was the sort never to let time slip through his hands, and he often spent his time in the modest language library thumbing through the texts and becoming familiar with exotic languages. "Let me take a look at that," he evidently said. "You know," (combining his awareness of current events with his recollection of a text he had scanned) "I think this must be Annamese. That's the language of the Viet Minh—the people the French are fighting over in Indochina." "Oh?" was the reaction. "Well, since you seem to know so much about it, do you think you could translate these messages?" His hand called, what could the young officer do but agree, run get the glossary (or whatever it was he'd seen), and retreat into the sanctuary of a private spot. He emerged a while later with passable renderings.

~~(SC)~~ Yes, the language was Annamese (as some called Vietnamese at that early date) and the activity was "Viet Minh" (the already outdated name of Ho Chi Minh's anti-French movement). And, according to the story, the naval officer became the first American COMINT "unit" to work the problem.

~~(SC)~~ ~~It's~~ of passing interest, perhaps, that the original notation for such intercept was "VNG" to denote guerrillas in opposition to the government of Viet-Nam. Later it was changed to VH (for Viet Minh), and, as such, it flourished. The war ended in 1954-'55, with the "VH" withdrawing north of the Seventeenth Parallel, leaving a few well-chosen remnants behind. In the "second Indochina war"—the one we got involved in—we again dredged up "VNG" for the so-called "Viet Cong", Hanoi's campaign against Saigon, then later rolled them together as "VC," for Vietnamese Communist. ❐

DOCID: 4012034



How the Friedman Auditorium did *NOT* get its Name!

by [redacted] E9

I suggest that the NSA Auditorium be named the "William F. Friedman Auditorium" and that there be placed at the entrance of that auditorium a painting of Mr. Friedman and a case displaying a sampling of his published works, replicas of his awards, and photos of him with other cryptologic leaders and national figures.

Those words began Suggestion No. C–206–70, sent by me via NSA incentive awards channels on November 3, 1969, *the day after William F. Friedman died.* The idea came so naturally because I had grown up revering Mr. Friedman: I teethed on his *Military Cryptanalysis* works in the late 40's, as a GI studying with Lambros Callimahos, and helped on Callimahos's revision of those works in the early 50's, starting as a civilian in AFSA's Technical Division under Mr. Friedman.

The suggestion was acknowledged promptly by the M Awards Committee, in mid-December, but then nearly two years of **SILENCE** followed, to my great surprise. How naive I was then!

In late 1971, to learn the suggestion's status, I began an exchange of memos and phone calls with M awards people (and eventually the Deputy Director, Dr. Tordella) that continued until mid–1972. The awards people sought my patience, saying the original suggestion and a later duplicate had gone to the Deputy Director's office where each was "apparently lost." A note from me to Dr. Tordella was met with more **SILENCE**.

Finally, in early June, 1972, a memo came from the Incentive Awards Branch saying the suggestion (along with several others for honoring deceased NSA personnel) would not be adopted. It explained: "This decision apparently [sic] is based on the fact that the number of recent losses are regrettably high and that these, together with those that can be expected within the next few years, greatly exceed the number of potential memorials."

I thought "What an incredible excuse!" Mr. Friedman was, in effect, being viewed as some sort of a willy-nilly choice for memorialization from among an immense set of equally deserving people—not as the pioneer he had actually been.

Down but not out, I immediately sent the essence of the original idea to the Commandant of the National Cryptologic School (Frank Austin), suggesting that the National Cryptologic Course Center be named for Mr. Friedman. I justified it as recognizing his early development of comprehensive cryptanalytic training and his numerous contributions to the literature of cryptology. That was on the fifth of June, 1972; and was followed by **SILENCE** . . . .

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

Some guys never learn: In June, 1974—as the fifth anniversary of Mr. Friedman's death approached—I re-sent the original suggestion through Incentive Awards channels, asking again that the NSA Auditorium be made a memorial to Mr. Friedman. This version was duly assigned Suggestion No. C–313–74 and, very promptly, "returned without action."

This time, the suggestion was characterized as failing to meet CSC and DoD criteria for Suggestion System processing. (Surprisingly, those criteria were said to have become effective about the time of the original suggestion in 1969, although that suggestion continued to be processed for another 2 1/2 years!)

I decided on one last shot. Since there was a new Deputy Director, namely, Mr. Buffham, I decided to get the 1969 suggestion directly to him. I did that in a personal memo sent on August 15, 1974. And, guess what? **SILENCE** again!

I was crushed. Five years of trying one method after another following Mr. Friedman's death, and still no memorial.

Imagine, then, my surprise and sense of achievement when, one April morning in 1975, I rode the escalator to the third floor in the Operations Building and found "WILLIAM F. FRIEDMAN MEMORIAL AUDITORIUM" over the auditorium doors. Though stunned, I composed myself enough to send another note to Mr. Buffham, this time thanking him for giving the project the support it needed, and expressing hope I might have the privilege of attending the dedication ceremony I presumed would follow.

By that time I should have been prepared for what followed, but I wasn't. Again, **SILENCE**! I heard nothing, a dedication was held, and I was not invited. And, when I recounted my five years of effort and ensuing disappointment to Mr. Callimahos, who participated at the dedication, my remarks got a blank stare.

It was then that I reached this shattering conclusion:

Designation of the NSA Auditorium as a memorial to Mr. Friedman had nothing to do with my suggestion!

BUT WAIT! That was 15 years ago. There's more . . . .

As I write this, it's late 1990, and I have just finished attending the agency's first "Cryptologic History Symposium," presented by NSA's Center for Cryptologic History (CCH). P.L. 86-36

"Bob! Long time no see. We were just talking about you a few days ago," [redacted] an old friend and CCH staffer also at the Symposium, said to me during a Symposium break. He went on to say something like "Tom Burns and I were looking at one of the Center's files containing material about you."

What was he possibly talking about? A trip to the Center produced the answer. There, in an aging file, was a November 1974 Memorandum signed by the Director, General Allen, addressed to ADIL, CNCS and ADPS, reading:

1. Attached is a suggestion for designating the NSA Auditorium as "The William F. Friedman Auditorium". . . .

2. For ADIL: Please arrange a plaque and painting of Mr. Friedman for the entrance of the Auditorium.

3. For CNCS: . . . investigate that aspect of the suggestion concerning photos, awards, publications, and other memorabilia . . . .

4. For CNCS/ADPS: . . . Since November is the fifth anniversary of Mr. Friedman's death, I hope we may be able to accomplish this action sometime this month.

And what was the Attachment? You're so right! It was a copy of the August 15 personal memo I sent to Mr. Buffham.

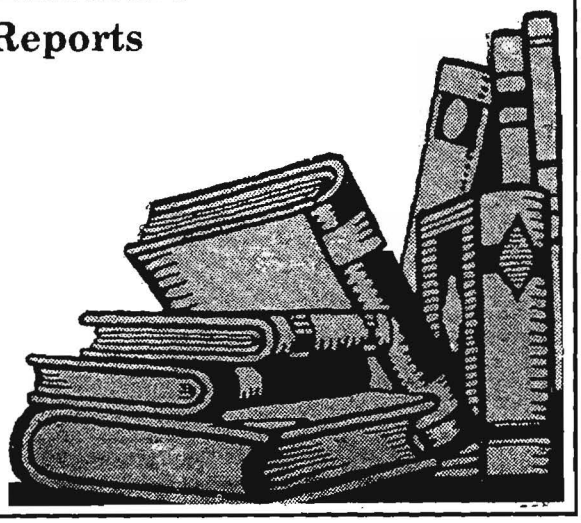
Now you know how the Friedman Auditorium DID get its name—and, finally, so do I.

□

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

Technical Literature Reports



Reported by: David Harris

Editor's Note: This material was submitted by the late author to be published in CRYPTOLOG as space permits. See "David Harris: In Memorium," 1st Issue 1990.

(U) Duncan Buell (1987) "Factoring: Algorithms, Computations, and Computers," *Journal of Supercomputing*, 1(2), pp. 191-216.

(U) M. C. Wunderlich & H. C. Williams (1987) "A Parallel Version of the Continued Fraction Integer Factoring Algorithm," *Journal of Supercomputing*, 1(2), pp. 217-230.

~~(C)~~ This issue of the *Journal of Supercomputing* was distributed free by Kluwer Academic Publishers at the AMS meeting in Providence.

Duncan's paper discusses "the computational structure of the most effective methods for factoring integers and the computer architectures--existing and used, proposed, and under construction--which efficiently perform the computations of these various methods." "The intent of this article is to use factoring and computers for factoring to provoke general thought about this matching of computer architectures to algorithms and computations."

(U) The article serves as a summary of some factoring algorithms and their implementations, especially parallel ones. The Wunderlich-Williams article is a description of an implementation of a parallel version of CFRAC on the MPP, together with a case study of the factorization of a 60-digit integer.

(U) James Reggia & Granger Sutton (1988) "Self-Processing Networks and their Biomedical Implications," *Proceedings of the IEEE*, **76**(6), June 1988, pp. 680-692.

(U) This is a survey paper on neural networks in medical applications. It may serve as a general introduction for the novice to the topics of neural nets, perceptrons, associative memories, Hebbian learning rules, energy minimizing networks, etc. It has a useful bibliography.

(U) Douglas Jones (1988) "Application of Splay Trees to Data Compression," *Communications of the ACM*, 31(8), August 1988, pp. 996-1017.

(U) The purpose of data compression is to improve the efficiency with which data can be stored or transmitted by reducing the redundancy of its representation. A compression algorithm takes the source data and produces a compressed text. It is undone by an expansion algorithm. Static probability models for strings of text have their limitations when applied to many different sources of text. Adaptive Huffman codes using tree balancing schemes is one way to handle this problem. Adaptive arithmetic compression algorithms are another.

(U) The paper describes the use of generalized splay trees to construct adaptive algorithms that are extremely fast and compact. When applied to Huffman codes, splaying (or a variant of it) yields a locally adaptive compression algorithm

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

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012034

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

~~CONFIDENTIAL~~

that is simple and fast, although not optimal in terms of compression. When applied to arithmetic codes, splaying yields near optimal compression and asymptotically optimal time. Finally the paper notes that as in other adaptive schemes, the loss of one bit from the compressed stream is catastrophic. The author says there is a need for research on ways to protect against such problem. He also suggests the possibility of using such compression schemes in cryptography.

(U) G. Brassard & S. Kannan (1988) "The Generation of Random Permutations on the Fly," *Information Processing Letters*, **28**, pp. 207-212.

~~(C)~~ The paper offers three different solutions to the problem of generating a random permutation when only a small but unpredictable subset of its domain is ever to be queried. Building the permutation on the fly allows one not to do the work of deciding on a value for the permutation until that value is requested. The choice among the three depends on the available time and space. Two new data structure techniques are introduced, continuous rehashing and a balanced tree scheme.

(U) William Kocay (1988) "Groups & Graphs, a MacIntosh Application for Graph Theory" *Journal Combinatorial Mathematics & Computing*, **3**, April 1988, pp. 195-206.

~~(C)~~ One difficulty is that CAYLEY is an all-purpose package that is difficult to modify, and is buggy. The user just calls CAYLEY and depends on it to do the proper thing. This is far from ideal for use as a research tool. One would like to be able to go in and modify code to try things out. Since the parts of CAYLEY are interdependent, the designers of CAYLEY could not let this happen.

~~(C)~~ Groups & Graphs is a software package designed to overcome these difficulties. It is a research tool for manipulating graphs on a computer screen, and for computing with them and their automorphism groups. It does not have the enormous scope of CAYLEY, but is portable, and relatively friendly to the researcher. This article describes the structure of the package, and some of its algorithms. Many computational problems can be converted into problems about the automorphism group of a graph, and so this package might be helpful in clobbering them. For example, the package has an algorithm for often finding Hamiltonian paths or cycles. Such cycles have importance in generalizations of Gray code problems. This is the basic paradigm described by both Aschbacher and Luks at the Providence meeting.

(U) Richard Thomas (1988) "Cayley graphs and group presentations" *Math Proceedings of the Cambridge Philosophical Soc.*, **103**, May 1988, pp. 385-7.

~~(C)~~ The goal is to come up with improved architectures for parallel processing. The Cayley graph of a group G with a given set of generators has as points the elements of G, and two such points are adjacent in the graph if one is gotten from the other by multiplication by one of the generators. The routing problem on the graph can then be reduced to a type of word problem in the group. The possibility of finding efficient means of routing between the nodes of the graph is one recommendation for using Cayley graphs. There is however a tradeoff between graphs with large numbers of vertices

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

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

DOCID: 4012034
EO 1.4.(c)
P.L. 86-36

and the need either to have many interconnections or extremely long communications routes. One is interested in finding Cayley graphs of a given number of vertices that are optimal for communication between nodes. The purpose of the Thomas paper is to study groups with a certain kind of presentation and homomorphism, and obtain bounds on the number of generators in the presentation and the order of the group.

(U) Richard P. Lippmann (1987) "An Introduction to Computing with Neural Nets," *IEEE ASSP Magazine*, April 1987, 22 pp.

(U) At an R51 tea on neural nets technology, this paper was recommended as an excellent source (along with the book by Rumelhart and McClellan) for beginners wishing to learn about neural nets. The paper is elementary and expository.

(U) David H. Bailey (1988) "Extra High Speed Matrix Multiplication on the Cray-2," *SIAM J. Sci. Stat. COMPUT.*, May 1988, **9**, no. 3, pp. 603-607.

(U) Ravinderpal Sandhu (1988) "Cryptographic Implementation of a Tree Hierarchy for Access Control," *Information Processing Letters*, **27**, pp. 95-98.

(U) We are given a computer or communications network where users are classified into a rooted tree of security classes. Each user is assigned a security class, called his clearance. Each file or message is assigned a security class called its sensitivity. We want users to have access only to that information whose sensitivity is consistent with their clearances. Sandhu intends to design a system for achieving this using a conventional cryptosystem such as DES. Each security class has a distinct key. Items are encrypted according to their security class and stored in encrypted form, with the security class name appended. Only users with access to the class key will be able to decrypt and read the item.

(U) The problem is to assure this desired access to key. Sandhu describes a method due to Akl and Taylor. This method has many advantages, but the terrible disadvantage is that when a new security class is added, new keys need to be computed for many of the existing security

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

)OCID: 4012034

classes, and existing items must be either re-enciphered, or all previous keys stored. The author presents a new solution to access control, at least in the special case of a rooted tree hierarchy of security classes, using one-way functions. The root is assigned an arbitrary key. One assumes that one has a family of "independent" one-way functions, one for each value of a parameter p. If b is an immediate child of c, then the key of class b is the value of the one-way function, with parameter p the name of class b, applied to the key of class c. Sandhu believes he can construct families of such one-way functions that are sufficiently independent to guard against users pooling their keys to recover keys to compartments they do not have, but he cannot prove this.

(U) J. Skorin-Kapov & F. Granot (1987) "Nonlinear Integer Programming: Sensitivity Analysis for Branch and Bound," *Operations Res. Letters*, **6**, no. 6, December 1987, pp. 269-274.

(U) The authors attempt to evaluate the sensitivity of solutions of non-linear integer programs to small changes in the right hand side or objective function coefficients. Such sensitivity analysis has been done in the case of linear integer programming. The authors assume the non-linear integer program has a relaxation to a continuous problem that is a convex program, such that the Kuhn-Tucker constraint qualification applies (as for example it will if the constraints are linear). This lets them make use of the dual non-linear program. Computational results are given for an example with a quadratic objective function, linear constraints, and 0-1 random variables. The point is to get an idea of what additional information to keep along the way in the enumeration tree in order to be able to bound the optimal value of a perturbed problem.

(U) Patrice Philippon (1988) "A propos du text de W. D. Brownawell: "Bounds for the degrees in the Nullstellansatz"," *Ann. Math.*, **127**, pp. 367-371.

(U) Philippon shows that the major result of Brownawell's paper making the Nullstellansatz effective also follows from a 1986 paper by Philippon. Further, when the ground field is a number field, one gets an explicit formula for the constant appearing in the theorem..

(U) D. G. Rogers (1988) "An Arithmetic of Complete Permutations with Constraints, I: An Exposition of the General Theory," *Discrete Mathematics*, **70**, 219-240.

(U) D. J. Champin & D. G. Rogers (1988) "An Arithmetic of Complete Permutations with Constraints, II: Case Studies," *Discrete Mathematics*, **70**, 241-56.

(U) Let N be an set of m integers, ordered by increasing size. The set N is symmetric if -n is in it whenever n is in it, and $-n_i = n_{m-i+1}$, for all i. N is central if it consists of those integers less than some c in absolute value. The purpose is to study the group S of all permutations of such sets N. The permutation π is said to be complete if the difference π-e, where e is the identity. If S contains complete permutations, then N is called an integral base.

(U) The purpose of these papers is to develop a theory of complete permutations, especially on central N or symmetric N or similar types of N. The arithmetic of complete permutations of symmetric integral bases turns out to be similar to the arithmetic of perfect systems of difference sets. Perfect systems of difference sets are in fact an abundant source of complete permutations. A constraint on a complete permutation is a specification of its behavior on a subset.

(U) Joseph Silverman (1988) "Computing Heights on Elliptic Curves," *Math. Computation*, **51**, July 1988, pp. 339-358. P.L. 86-36

(U) [redacted] told me about this paper on how to compute the canonical height of a point on an elliptic curve over a number field. Tate gave a rapidly converging series for computing Archimedean local heights for real absolute values. Silverman generalizes these methods to work for complex absolute values, and gives an efficient procedure for calculating local heights at non-Archimedean places. Thus, we can

DOCID: 4012034
EO 1.4.(c)
P.L. 86-36

effectively compute heights over number fields having complex embeddings.

(U) This is potentially an important step in improving our ability to do computational work on elliptic curves. For example, heights are used in Zagier's algorithm for finding the integral points up to large bounds. The canonical height of P can be defined in terms of a limit of heights of 2-power multiples of the point (that is roughly the number of digits in the coordinates of the point and its multiples.) It is not practical to compute it as a limit, but one can write the canonical height as a sum of local heights, one for each absolute value on the number field. These local heights are what Silverman teaches us to compute. Computer-suitable algorithms for these local heights are included. Some examples of computing canonical heights of points on explicit elliptic curves are also included. For example, on the elliptic curve $y^2+21xy+494y = x^3 + 26x^2$, the point $P=(0,0)$ has canonical height 0.010492061 . . .

(U) Robert M. Kuhn (1988) "Curves of Genus 2 with Split Jacobian," *Trans. AMS*, May 1988, **307**(1), pp. 41-49.

[redacted]

[redacted]

(U) William Gardner (1988) "Simplification of MUSIC and ESPRIT by Exploitation of Cyclostationarity," *Proc. IEEE*, **76**(7), July 1988, pp. 845-7.

(U) This note says that the problem of dealing with direction-of-arrival (DOA) location with antenna arrays via eigenstructure methods, as in the algorithms MUSIC and ESPRIT, can be simplified by exploiting a property of modulated signals called cyclostationarity.

(U) The advantages gained include a reduction in the size of the array and thus a reduction in SVD computation work. The disadvantages are that frequency parameters, such as carrier frequency or baud rate, must be known or measured, the integration time for correlation measurement is longer, and a different correlation matrix must be estimated for each signal of interest. Eigenstructure methods are intended to allow the individual DOAs of interfering signals to be determined provided the number of sensors in the array exceeds the number of signal sources.

(U) A brief description of MUSIC and ESPRIT is included. The modified methods should work on such bauded or carrier modulated signals as radar or radio communications. The balance of the advantages and disadvantages for a particular problem will dictate whether the proposed new methods should be used in place of MUSIC and ESPRIT.

(U) J. E. Olson (1987) "A Problem of Erdös on Abelian Groups," *Combinatorica*, **7**(3), pp. 285-289.

[redacted]

DOCID: 4012034

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

~~CONFIDENTIAL~~

EDITORIAL POLICY

A Letter to the Editor in this issue prompts this brief restatement of editorial policy.

CRYPTOLOG's criteria for publication are very like those of *Cryptologic Quarterly*: articles may be on any theoretical, doctrinal, operational, managerial, or historical aspect of cryptology.

But CRYPTOLOG is a more informal publication, and does not demand, as *CQ* does, that the articles "... make a genuine contribution to cryptologic literature." It asks only that they be useful or interesting. Nevertheless, it does require that facts are accurate and that the writing is clear. As for controversy, CRYPTOLOG thrives on it! But please, not the cryptologic equivalent of "the moon is made of green cheese": factual error is not controversy.

About classification: material up to and including TSC may be published, but not if there are additional caveats.

Preferences? Classified over unclassified (that's the justification for CRYPTOLOG's existence, after all!); technical over non-technical; shorter over longer.

Also, most welcome are conference and seminar reports, book reviews, software and hardware reviews, technical literature reports.

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

And letters. We dote on Letters to the Editor. Readers do too.

unclassified

Notice to Subscribers

Distribution of this Issue reflects changes received by COB 26 October 1990

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4012034

BOOK REVIEW

Doublespeak (From "Revenue Enhancement" to Terminal Living" - How Government, Business, Advertisers, and Others Use Language to Deceive You), William Lutz, Harper & Row, Publishers, New York, 1989.

P.L. 86-36

Reported by [redacted] *P16*

As the featured guest speaker at the Cryptolinguistic Association's annual banquet in May, William Lutz spoke to the audience about his research and experiences that led to the publication of his book, *Doublespeak.* I became intrigued by the examples he cited. Immediately that afternoon, I purchased a copy of his book to read for myself about the things he was describing to the audience:

> Doublespeak is language that pretends to communicate but really doesn't. It is language that makes the bad seem good, the negative appear positive, the unpleasant appear attractive or at least tolerable. Doublespeak is language that avoids or shifts responsibility, language that is at variance with its real or purported meaning. It is language that conceals or prevents thought; rather than extending thought, doublespeak limits it.
>
> Doublespeak is not a matter of subjects and verbs agreeing; it is a matter of words and fact agreeing. Basic to doublespeak is incongruity, the incongruity between what is said or left unsaid, and what really is. It is the incongruity between the word and the referent, between seem and be, between the essential function of language--communication--and what doublespeak does--mislead, distort, deceive, inflate, circumvent, obfuscate.

Thus does the author define the subject of his book which is a bountiful collection of examples drawn from a variety of sources that touch every facet of our daily lives: media, advertising, business, professions, government, military, politicians. While Mr. Lutz' message is timely, readable, entertaining and amusing, it is also sobering, at times shocking, and generally disturbing, if not outright disgusting.

Mr. Lutz devotes a considerable portion of his book taking government and politicians (at all levels and the world over) to task for their abusive use of doublespeak. What is most disturbing about *Doublespeak* is that, as government employees we are a part of the problem he describes. When we or our political and executive leaders use doublespeak in dealings with the public or subordinates or with each other, it reflects poorly on everyone in government service.

As members of the intelligence community we have an obligation even greater than that of the ordinary responsible citizenry to understand correctly what is being communicated to us, to act on the basis of an accurate comprehension of the facts, and to communicate to others accurately and clearly. But as the author all too clearly demonstrates, we are constantly bombarded by messages that are, sometimes intentionally, designed to "mislead, distort, deceive, inflate, circumvent or obfuscate." And, unfortunately, we do not always have the time and resources to strip away the doublespeak and receive the true message.

Readers should come away from reading *Doublespeak* with a new appreciation for and dedication to communicating more clearly, accurately, and honestly. I urge you all as professionals in the intelligence business to take this book to heart while you are churning out bureaucratic prose of any sort.

~~FOR OFFICIAL USE ONLY~~

How to Edit a Scientific Journal, by Claude T. Bishop. ISI Press, Philadelphia, 1984. $14.95.

Reviewed by: [redacted] *P16*

Every NSA editor of any type—scientific, end-product, newsletter—should have a copy of this excellent book. Authors and Publishers should read it too, so they might have some notion of what is expected of them. In just 132 pages Bishop has provided a do-it-yourself manual on every aspect of publishing a periodical. He spells out the responsibilities and duties of editors and of authors as well. He offers sample guidelines for referees, for reviewers and authors, and even, sample letters. His purpose in writing this book was to provide guidance to scientists who are not professional editors and who would likely "end up learning the business by hard and sometimes bitter experience."

The austere title gives no clue that this is a fun book to read. Bishop illustrates his points with zany scenarios, but he is dead serious about quality in professional journals. He points out that maintaining standards "rests squarely in the hands of editors, who decide what will be published." He is concerned that the pressure to publish is resulting in the proliferation of trivial periodicals—that serious scientists soon ignore. By applying a significance factor, he finds that of the 90,000 or so journals, only 8,000 need be considered: the remainder clog retrieval systems with GIGO (garbage in, garbage out).

Editors must also exercise great care in selecting editorial boards, referees and reviewers and in preparing guidelines for them, because the review process plays a key role in assuring that what is published constitutes a reliable record. It can save the reputation of authors, reviewers, editors, and the publication itself. Bishop cites a letter to the editor from an author grateful for the rigors of the review process:

> After discussions about the referees' reports, your Associate Editor agreed to seek the opinion of a third referee as arbitrator. This referee found a major error in the theoretical part, which escaped 4 authors, 2 previous referees and the Associate Editor! My gratitude is boundless; I was saved from a very embarrassing situation.

But more than embarrassment can result. In a seminar on ethics during the International Technical Communications Conference (Chicago, 1989) we discussed the responsibility of the editor who accepted a paper on a treatment for an eye problem and overlooked the fact that the researcher had not followed protocol for testing on humans. Moreover, the editor uncharacteristically endorsed the treatment. Later an ophthamologist friend filled me in on the rest of the story. The researcher went on to another university, patented the medication, and got millions from investors. But other researchers could not duplicate the results. Evidently he had cooked the books besides violating protocol. So now FDA, SEC and IRS are after him. Suits and countersuits have been filed. The reputations of all the individuals and institutions involved are affected. All this because of an editor's oversight compounded by an error in judgment. A diligent editor would have stopped the researcher in his tracks.

The chapters on the literature of science, editors, editorial boards, the review process, referees, ethics, and record keeping are of particular interest to us at NSA. Of lesser practical application are the chapters on copy processing and printing, and on post-printing activities, for NSA has its own rules. But they do offer considerable insight to the processes, and a wealth of terminology; editors will find these chapters invaluable in dealing with both NSA and commercial printers. □

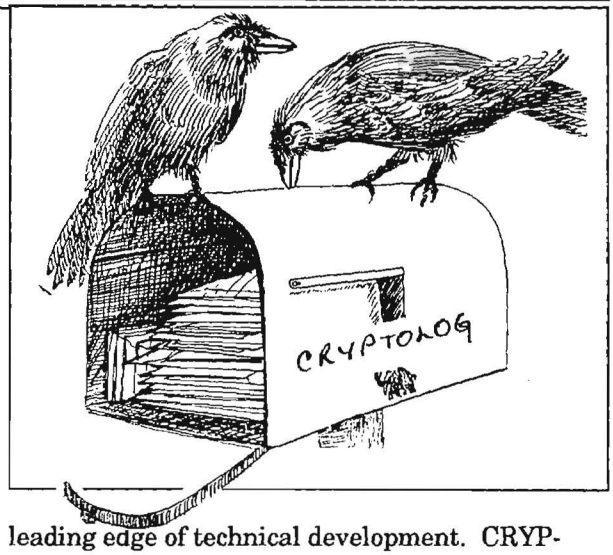
DOCID: 4012034
E.O. 1.4.(d)
P.L. 86-36

To the Editor:

As but one member of what must be a legion of CRYPTOLOG readers, I always felt that this publication was intended as a vehicle through which authors could share with others selected technical expositions relating to our mission. Expositions which not only explained "tried and true" methods of cryptology, cryptography, traffic and signals analysis, and other "technical" fields, but also documented and detailed new and innovative approaches to the problems we face in those fields.

Therefore, I was puzzled to see so many articles dealing with managerial problems, individual perceptions of Agency programs and explanations of corporate policy being published in the most recent magazine. Among the ten major articles contained in the CRYPTOLOG 2nd Issue 1990 I counted only two—"Planning for the Millenium" (sic), and [redacted] which were true technical dissertations. Six of the remaining eight articles—"A Perception of the Tech Track", "NSA/CSS and Counternarcotics", "Reassimilation", "Excellence through Evaluation", "Expert VLSI Designer Hired for Three Days", and "Rebuttal"—are not technical treatises and would seem more appropriate as submission for some other publication, such as the Agency's *Quarterly Management Review* (*QMR*). Each of these six easily fit into the *QMR*'s Quarterly Management Topic, Human Resources, and/or Telecommunications and Computer Services categories. The remaining two articles—"The Need for Intelligence" and "Balloon-Int, Civil War Style"—are perfect candidates for the historical publications of the NSA archives researchers.

As an internal publication aimed at serving our employees in the technical fields, CRYPTOLOG provides a valuable service. Surely our technical experts can provide the technical articles CRYPTOLOG should be carrying, and in quantities sufficient to warrant publication of more than two issues per year. We are a unique organization replete with talent and full of important achievements. Indeed, some of what we do is on the



leading edge of technical development. CRYPTOLOG deserves better support in terms of input from our technical professionals, and should be reporting more of what they are achieving. Non-technical articles of the type noted above should be addressed to, and published in other, more appropriate Agency vehicles.

P.L. 86-36

Don't you agree?

[redacted] *Chief, L1*

The Editor replies:

If there aren't more technical articles in CRYPTOLOG, it's not for want of trying!

Actually, we do get a lot of technical articles over the transom and through solicitation that we do not publish. Sometimes it's because they are prizewinners in essay contests and automatically go to *Cryptologic Quarterly* for consideration, and increasingly, it's precisely because they are about "new and innovative approaches"—advanced techniques that are closely held. Sorry, Fred, you won't be reading about them in CRYPTOLOG.

But you are right. We are getting more non-technical than technical articles, and especially, a flood of management articles of a general nature, to the point that I've had to resort to a printed rejection form! Why is this? I believe it's because the fashion in the agency is but a half-beat behind that in the outside world. Just as in universities there are fewer PhDs in physics and math and

~~FOR OFFICIAL USE ONLY~~

more MBAs, so at NSA anyone who can is disdaining the tech track for management. It's simply a matter of more reward for less effort. So ambitious tech types write on management or non-technical subjects as a way of planting the flag.

I haven't given up, though, and I continue to buttonhole everyone who might possibly contribute a technical article. I hereby make a plea to whom it may concern. (Thanks, Fred, for giving me this opportunity.)

As for publishing the cited "management" articles in *QMR* and the "historical" articles in historical publications, the persons in charge of those publications think differently, as you will read in their responses. In any case, the line between managers and technicians is blurred. Technicians do not work vacuum-packed in monastic cells solely on tasks handed down from above, but participate in decision-making and in the running of the agency. They sit on promotion boards, reorganization task forces, career panels. They order dictionaries and software. They provide grass-roots input to multi-million-dollar computer systems. They hire a specialist for a one-shot job. In short, they do management things.

CRYPTOLOG is somewhat more than a medium for technical exchanges among technical types. As Gen. Wolff, then DDO, set forth its charter in "A Letter of Introduction" in the first issue, ". . . its level of informal exchange invites short articles and letters on any subject." The editors have interpreted "any subject" to mean anything pertaining to NSA. And so it provides individuals, be they managers or technicians, a forum for indulging in speculation; for advancing futuristic notions; for query and challenge. It has become neutral ground where managers and technical types can meet, discuss, and argue with one another, having first checked their shoulderboards at the transom.

From the Founding Publisher

There is some, but not much, merit to [redacted] argument. I agree that most of what is published in CRYPTOLOG ought to be by technicians, about technical things, for technicians. But there is room for much else under that umbrella. The technicians' view of such management programs as the technical track is very different from that of generalists; it needs to be articulated. Pate's piece does it well. There is plenty of room for history in the CRYPTOLOG; the archivists will certainly welcome the material for their histories. Similarly with other articles mentioned. From what I recall of the *QMR*, it is simply not a vehicle for any of the articles in that issue.

William Lutwiniak, P1, (Retired)

Amicus Curiae *reponse to* [redacted]

Editors' lots are not always happy ones. Some readers adore their publications, some abhor them, other readers take what they can get. Mr. [redacted] observations about the last issue of CRYPTOLOG were certainly written out of concern for the quality of technical publication in the Agency. And it is true that the articles he points out are not strictly technical in the sense that we usually define the term, i.e., signals analysis, cryptanalysis, computer science, etc. We can look at this situation from two directions, however. First, and not meaning to be flip, an editor doesn't always receive a good supply of the kinds of articles he or she would like, in this case items of a more "technical" nature. The editor, however, still wants to publish matter of value to his or her readership. This brings us to the second point: Articles which address not-so-technical subjects but which are perhaps peripherally related and therefore still have value to the work force should not be shunned because they do not meet our tight definition of what is a technical subject.

Somewhat in this light, I couldn't agree more with [redacted] statement that ". . . our technical experts can provide the technical articles CRYPTOLOG should be carrying . . ." The same observation could be made about

P.L. 86-36
DOCID: 4012034

Cryptologic Quarterly, the journal I am privileged to edit. The fact is, however, because of busy schedules, lack of enthusiasm for writing, minimal awareness of the existence of publication vehicles, or a hundred other reasons, Agency employees don't submit articles in the volumes we editors would like to become accustomed to. Many of those who do send us articles, though they don't necessarily contribute technical "treatises," still write about topics that interest a large segment of the NSA population who don't have access to the *Quarterly Management Review* or other publications, which, while "more appropriate," do not receive the wide distribution that would make the information they contain even more useful.

A word about [redacted] reference to what the "NSA archives researchers" should be writing. First of all, [redacted] may or may not be aware that the archivists and the researchers (read "historians") are now organizationally two different groups. The historians, my organization, while personally interested in topics like "The Need for Intelligence" and "Balloon-Int," would not be inclined to write about them. The first would need much more elaboration and in-depth research to make it worthy of a cryptologic history monograph or even an article for *Cryptologic Quarterly*. The second, while fascinating and even amusing, does not carry a cryptologic theme and therefore would not be fuel for any cryptologic historian's production. Our criteria for publication of material as a monograph or as a *Quarterly* article include (to quote from the *CQ*'s title page) whether or not the article (or monograph) is of sufficient substance and interest to make a genuine contribution to cryptologic literature. By the way, *Cryptologic Quarterly* articles may be written (again, to quote) on any theoretical, doctrinal, operational, **managerial**, or historical aspect of cryptology. Although I have not seen an expressed editorial policy for CRYPTOLOG, I believe that it is implicitly very similar.

CRYPTOLOG and *Cryptologic Quarterly* are at their hearts technical journals. Both publications recognize, however, that not only should we as cryptologic professionals be concerned with the narrow (i.e., technical) aspects of cryptology, but we should also have an abiding interest in the broader issues that affect the cryptologic effort. To ignore those broader issues is to make us less than we can be.

Barry Carleen, D91,
Executive Editor, Cryptologic Quarterly

From QMR:

I am responding to [redacted] suggestion that six articles on management published in 2nd Issue 1990 are more suitable for the *Quarterly Management Review* (*QMR*) than for CRYPTOLOG.

A few words are in order about *QMR*. It serves as a management tool which tracks performance trends within the Agency. Information that is placed in the *QMR* is factual and presented in graphic and/or narrative form, limited in both length and amount of detail. It is not intended to provide an analysis of the data or to present personal opinions. Rather, the data illustrate the status, trends, comparisons and accomplishments of ongoing and new activities in a graphic or statistical manner for individual management analysis. Also included are topics that are of general interest to, or impact on, a wide segment of Agency management, but again, factual in nature.

Historically, CRYPTOLOG has offered an opportunity for individuals to contribute opnions, to relate experiences, and to share knowledge on a variety of subjects. The articles mentioned fall in this category. Therefore the several individuals involved in preparing the *QMR* read and appreciated the articles cited and were not perturbed that they were published in CRYPTOLOG. The article "Excellence through Evaluation" would be a suitable for QMR if the contents were factually oriented and summarized in one or two pages.

[redacted] *Chief, N313,*
QMR *Coordinator*

[redacted]

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

DOCID: 4012034

Golden Oldie

HIAWATHA DESIGNS an EXPERIMENT

1
Hiawatha, mighty hunter
He could shoot ten arrows upwards
Shoot them with such strength and swiftness
That the last had left the bowstring
Ere the first to earth descended.
This was commonly regarded
As a feat of skill and cunning.

2
One or two sarcastic spirits
Pointed out to him, however,
That it might be much more useful
If he sometimes hit the target.
Why not shoot a little straighter
And employ a smaller sample?

3
Hiawatha, who at college
Majored in applied statistics
Consequently felt entitled
To instruct his fellow men on
Any subject whatsoever,
Waxed exceedingly indignant
Talked about the law of error
Talked about truncated normals,
Talked of loss of information,
Talked about his lack of bias,
Pointed out that in the long run
Independent observations
Even though they missed the target
Had an average point of impact
Very near the spot he aimed at
(With the possible exception
Of a set of measure zero.)

4
This, they said, was rather doubtful.
Anyway, it didn't matter
What resulted in the long run;
Either he must hit the target
Much more often than at present
Or himself would have to pay for
All the arrows that he wasted.

5
Hiawatha, in a temper
Quoted parts of R. A. Fisher
Quoted Yates and quoted Finney
Quoted yards of Oscar Kempthorne
Quoted reams of Cox and Cochran
Quoted Anderson and Bancroft
Practically in extenso
Trying to impress upon them
That what actually mattered
Was to estimate the error.

6
One or two of them admitted
Such a thing might have its uses
Still, they said, he might do better
If he shot a little straighter.

7
Hiawatha, to convince them
Organized a shooting contest
Laid out in the proper manner
Of designs experimental
(Mainly used for tasting tea, but
Sometimes used in other cases)
Randomized his shooting order
In factorial arrangement
Used in the theory of Galois
Fields of ideal polynomials
Got a nicely balanced layout
And successfully confounded
Second-order interactions.

8
All the other tribal marksmen
Ignorant, benighted creatures,
Of experimental set-ups
Spent their time of preparation
Merely shooting at a target.

13 July 1967

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4012034

9

Thus it happened in the contest
That their scores were most impressive
With one solitary exception
This (I hate to have to say it)
Was the score of Hiawatha,
Who, as usual, shot his arrows
Shot them with great strength and swiftness
Managing to be unbiased
Not, however, with his salvo
Managing to hit the target.

10

There, they said to Hiawatha,
That is what we all expected.

11

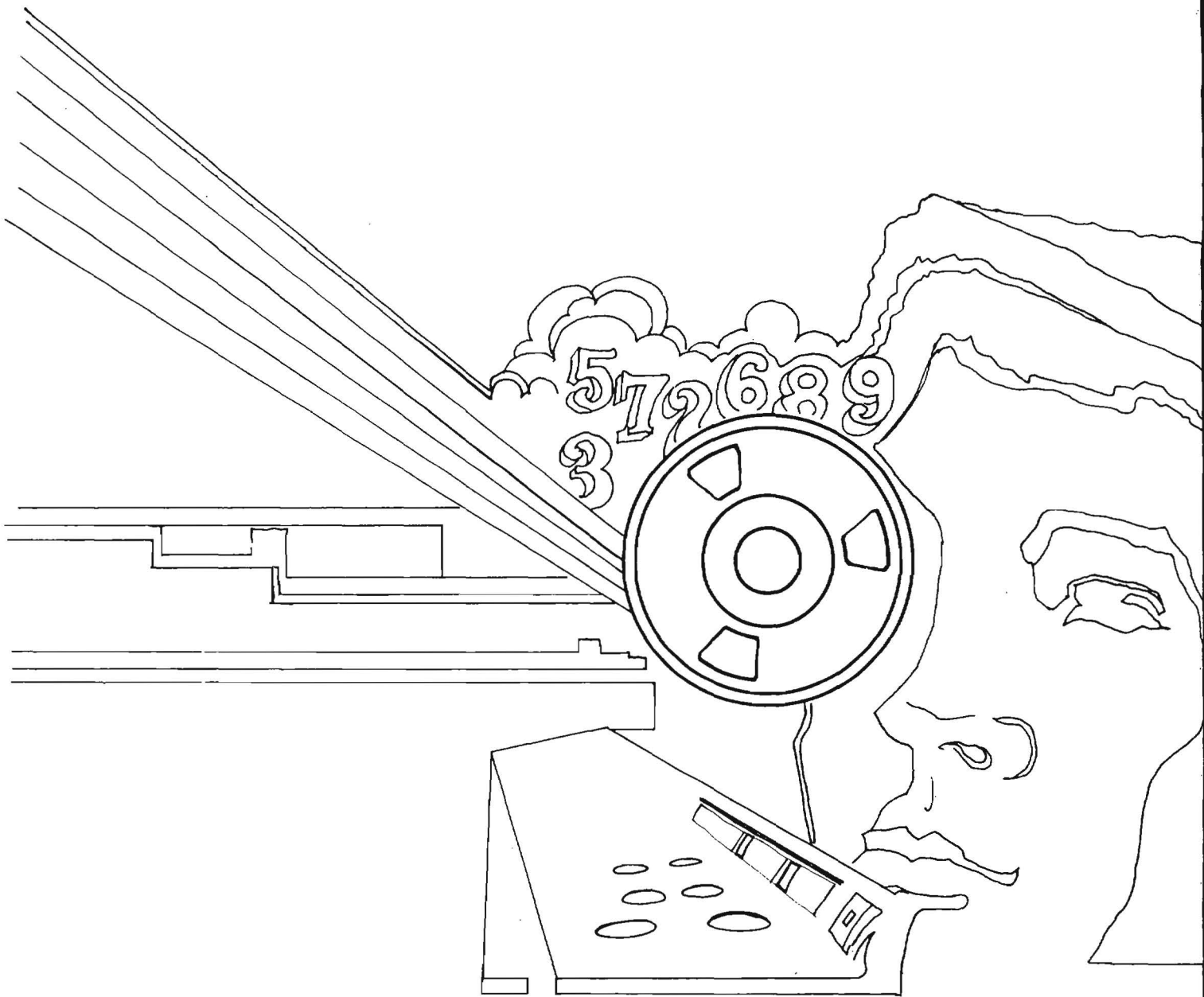
Hiawatha, nothing daunted,
Called for pen and called for paper
Did analyses of variance
Finally produced the figures
Showing beyond peradventure
Everybody else was biased
And the variance components
Did not differ from each other
Or from Hiawatha's
(This last point, one should acknowledge
Might have been much more convincing
If he hadn't been compelled to
Estimate his own component
From experimental plots in
Which the values all were missing.
Still, they didn't understand it
So they couldn't raise objections.
This is what so often happens
With analyses of variance.)

12

All the same, his fellow tribesmen
Ignorant, benighted heathens,
Took away his bow and arrows,
Said that though my Hiawatha
Was a brilliant statistician
He was useless as a bowman.
As for variance components
Several of the more outspoken
Made primeval observations
Hurtful to the finer feelings
Even of a statistician.

13

In a corner of the forest
Dwells alone my Hiawatha
Permanently cogitating
On the normal law of error
Wondering in idle moments
Whether an increased precision
Might at the risk of bias
If thereby one, now and then, could
Register upon the target.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~