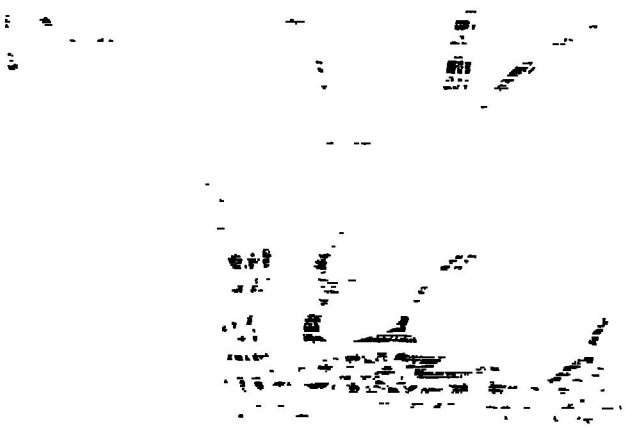
~~TOP SECRET~~

# National Security Agency

## Fort George G. Meade, Maryland



# DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

This is Dragon Seeds.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

Dragon Seeds is both Mother China and her neighbors. Dragon Seeds is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, Dragon Seeds is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

Dragon Seeds is yours. May it grow with you.

The Editors

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor
Minnie O. McNeal

Executive Editor
Robert S. Benjamin

Composition
Helen Ferrone

Copy Editor
Thomas L. Glenn

Biographical Editor
Brooks H. Handy

Rewrite Editor
Geraldine J. Pettie

Education Editor
Marian L. Reed

Special Interest Editor
Ray F. Lynch

Feature Editor
Richard V. Curtin

PRESS CORPS

| | | | |
|---|---|---|---|
| B11 | Carolyn Y. Brown | B42 | Velma Jefferson |
| B12 | Philip J. Gallagher | B43 | Mary Ann Laslo |
| B21 | Gary Stone | B44 | Jack L. Thomas |
| B31 | Jack Spencer | B45 | John E. Uzarek |
| | Thomas M. Beall | B5 | Paul M. Hoagberg |
| B32 | Joe T. Hudson | B62 | [redacted] |
| B33 | Louis Ambrosia | B63 | Jean C. Smith |
| B34 | Thomas L. Wood | B64 | Allen L. Gilbert |
| B41 | James W. Schmidt | B65 | Leona B. Dickey |
| | | | George S. Patterson |


# TABLE OF CONTENTS


| | |
|---|---|
| Captain Joslin's Salutation | 1 |
| Captain Joslin's Biography | 2 |
| Cryptanalysis Through Functional Linguistics..... Donald Lenahan | 3 |
| Recovery of a Viet Communist Callsign System.....Wayne E. Stoffel | 5 |
| Impact of ARDF on Traffic Analysis..... Al Gilbert | 7 |
| The AG-22 and You..... Peggy Barnhill | 9 |
| DDP - Dedupe, Delete and Progress..... Charles Swift | 12 |
| Chinese Voice: Solution to a Dilemma..... L. St. Clair Myers | 14 |
| The Creative Translator.....Tom Glenn | 16 |
| Analyzation of Data .....Dick Curtin | 19 |
| Seedlings | 22 |
| Ask the Dragon Lady | 24 |
| Contributors | 29 |

## GREETINGS FROM CAPTAIN JOSLIN

It is my pleasure to introduce to the B Group readership an informal publication which promises to be informative, imaginative, diversified and, yes, even interesting. As I have already stated in my initial announcement of Dragon Seeds to B Group personnel, I am highly enthusiastic about the project and foresee significant returns to the individual. Likewise, I view it as an excellent opportunity for me to become acquainted with you -- to know what you are thinking, to see what techniques you are exploring, to obtain a better feel for what professional problems confront you and those around you, to see what initiatives you are capable of.

Barriers created by the size of B Group, diversity of interests, formality of reports, and the protection of our information have prevented us from communicating easily and sharing fully many concepts and techniques which are professionally exciting and useful to know. Now is your chance for give and take -- to present your thoughts and ideas, to give others the benefit of your particular expertise and experience, or to have your questions answered by the "Dragon Lady," and to find out what others are thinking. I warmly endorse this new B Group venture and encourage your full participation in making Dragon Seeds a provocative, useful, and enjoyable publication.

H. E. Joslin

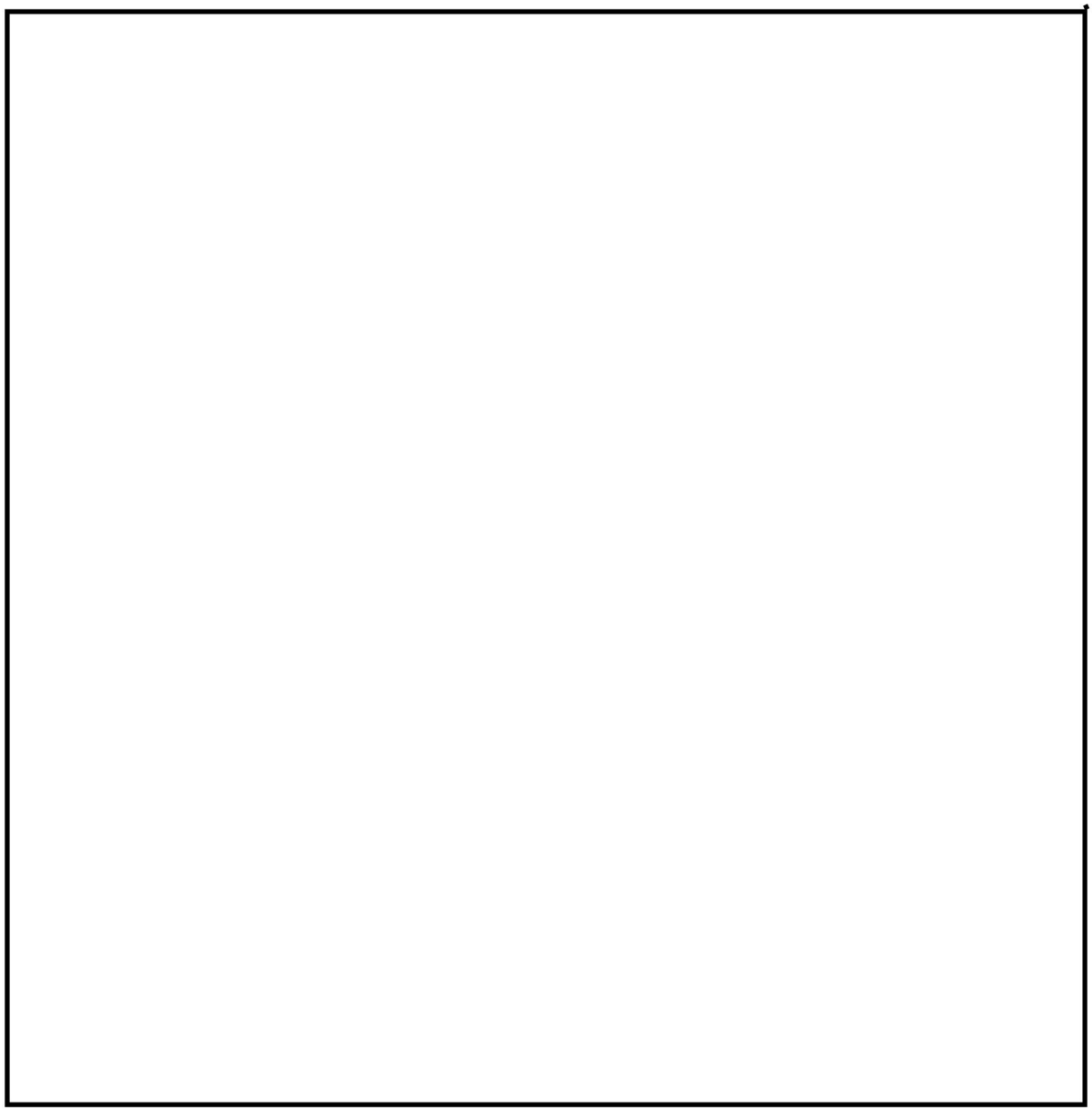
CAPTAIN HAROLD E. JOSLIN, CHIEF B

Captain Harold E. Joslin, USN, brings to B Group the benefit of his 34 years of military service, including a number of key assignments with NSA and the Naval Security Group. Having enlisted in the Navy in 1937, he was serving on Guam as a Second Class Petty Officer in December 1941 when he was captured by the Japanese. (His wife had flown out on the last plane to leave Guam.) After spending 45 months as a POW, he returned to the U.S. in 1945, advanced through the rates to Chief Petty Officer, and was commissioned as an Ensign, USN, in 1946. Captain Joslin is a qualified Interpreter/Translator, having graduated from the Russian language school at Anacostia.

Captain Joslin's career has been highlighted by a number of significant assignments such as Deputy for the Combined Naval Party at GCHQ; Commanding Officer, NSG Activity, Edzell, Scotland; Deputy Director, Naval Security Group Pacific; Assistant Director for Special Operations, Naval Security Group Command; and Deputy Chief of B Group.

CRYPTANALYSIS THROUGH FUNCTIONAL LINGUISTICS

by Donald P. Lenahan, B222



EO 3.3b(3)
PL 86-36/50 USC 3605

[redacted]

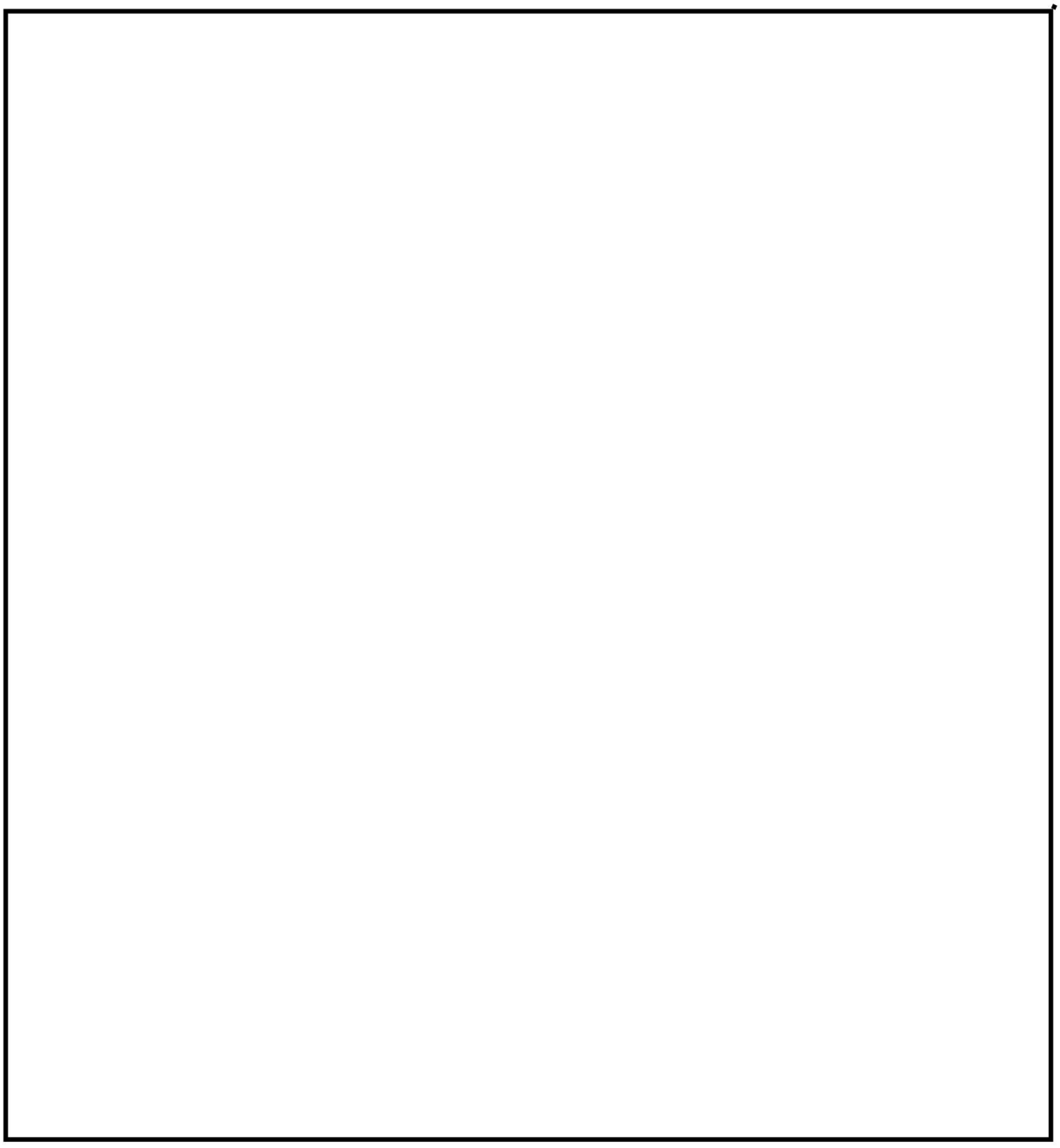
****

"It's no disgrace to be a slave. It's a disgrace to work voluntarily for someone else."

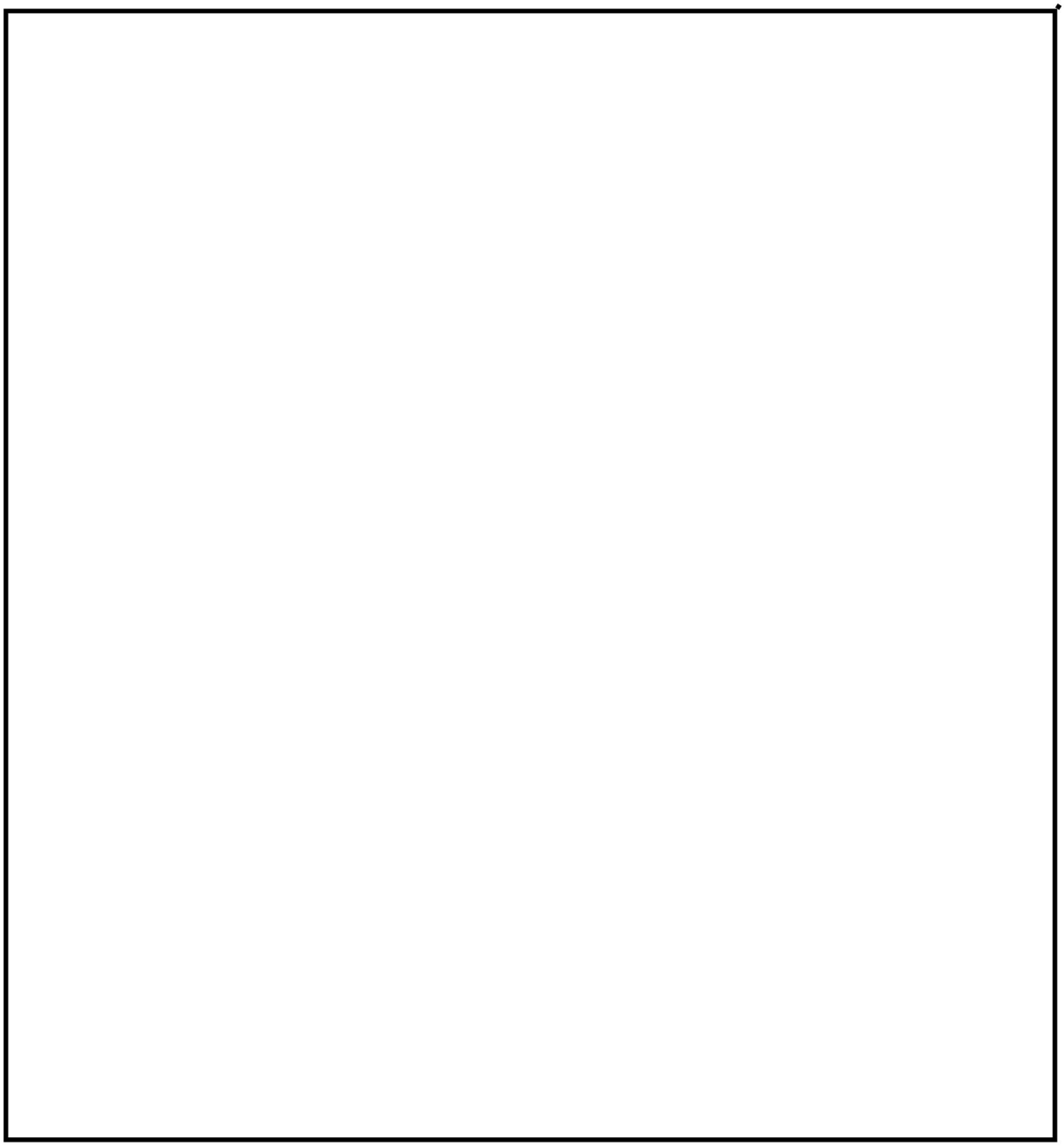
....Cambodian Proverb

RECOVERY OF A VIETNAMESE COMMUNIST CALLSIGN SYSTEM

by Wayne Stoffel, B03



EO 3.3b(3)
PL 86-36/50 USC 3605



THE IMPACT OF ARDF ON TRAFFIC ANALYSIS

by Allen L. Gilbert, B6403, 4787s

The Vietnamese conflict and techniques for collection of signal intelligence developed and employed in that arena have influenced the traffic analytic approach to the Vietnamese Communist problem profoundly. One of the most effective techniques employed on a large scale in Vietnam has been Airborne Radio Direction Finding (ARDF). ARDF, in addition to revolutionizing the direct support of tactical units through timely and accurate locating of enemy units, has almost reversed the traffic analytic approach to maintaining continuity and developing new targets in some areas.

Traditionally, the traffic analyst is faced with the problem of reconstructing a communications complex through recovery of callsign and frequency systems, message externals, schedule activity and those rare compromises made by enemy communicators. This route usually requires close scrutiny and cataloging of the elements of intercept through an extended period of time, with the hope that a transmitter location will be compromised or that medium-range direction finding will suggest a location for the activity. ARDF provides a location within a radius of hundreds of meters rather than a number of miles. The availability of ARDF on target transmitters considerably shortens the period of development for new activities and provides almost instant continuity on targets effecting communications changes.

In Vietnam, the concept of ARDF tasking provides coverage in all areas of hostile troop activity. The Military Assistance Command, Vietnam (MACV) controls the tasking of direction finding aircraft and has divided the target area into smaller areas of known enemy activity as reflected by all intelligence sources. Aircraft are deployed to these areas in support of MACV intelligence sources. Aircraft are deployed to these areas in support of MACV intelligence requirements, and therefore direction finding locations are available almost daily on tactical targets. In this process, a certain number of unidentified transmitters are also located. It is apparent that repeated fixing of an

unidentified transmitter in the same location, even though the callsigns may change periodically, gives a basis for a suspected continuity, as well as a hint as to the unidentified transmitter in an area where continuity has been lost suggests that the unidentified target represents the lost continuity. When aircraft are deployed to a target area on a daily basis, the recovery of the signal environment in the area builds rapidly.

Certainly, all other elements of traffic analysis must then come into play to establish case notations and identifications and ARDF alone does not solve the problem but what an advantageous beginning it provides!

****

*People walking along the halls*
*People leaning on the walls*
*People engaged in conversation*
*Or active in clubs for recreation*
*With all this action and milling mob*
*You wonder who is on the job.*

THE AG-22 AND YOU

BY Peggy Barnhill, B42

A new item of the SIGINT community's stockpile of electronic gadgets is now installed in sufficient quantity to greatly affect the traffic analytic and processing procedures employed at forward field intercept and within B Group.

The gadget, properly referred to as the "AN/GGC-15" but more commonly called the "AG-22," replaces the typewriters or "mills" previously used by manual Morse intercept operators and radiotelephone transcribers. It consists of an electric typewriter with a modified keyboard, a paper tape punch, and in some cases a paper tape reader, all connected to a solid state station clock, the AN/GSQ-53.

The installation of the AG-22 undoubtedly represents only the first of many revolutionary techniques being developed to permit the rapid transfer of intercepted data from overseas sites to a central processing center. The Improved AG-22 Terminal System (IATS) is already being tested at USM-1, Vint Hill Farm Station, Warrenton, Virginia. As each technological advance is made, changes in traffic handling or processing procedures will occur.

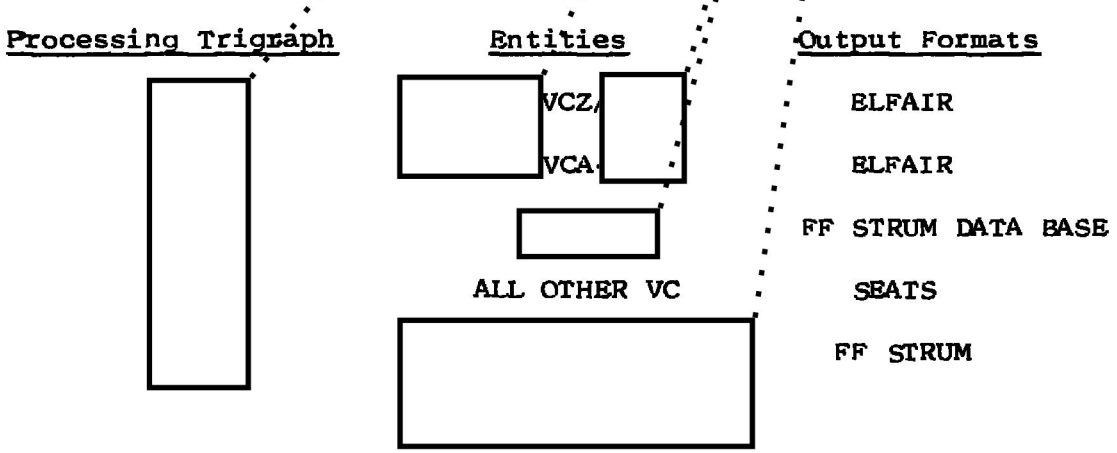
In order to fully understand the impact of the AG-22, it is necessary to examine the equipment and processing developed here at NSA.

The AG-22 produces two outputs. When the operator strikes a key, a character is printed on a page, and simultaneously the corresponding configuration in eight-level code is punched on a paper tape. Thus total intercept is immediately prepared for transmission.

The paper tapes are transmitted via the STRAWHAT data links. There are currently six circuits between NSA and intercept sites in the Far East. These circuits are capable of forwarding data at a rate of 750 and 1500 words per minute.

Thus the development of the AG-22 has resulted in the availability to the analyst of total traffic only a few hours after intercept. The data explosion is considerable. During testing on various CHICOM problems 4 to 5.5 times as much data were forwarded and processed as would be expected normally via STRUM or ELFAIR. To make both computer and analyst processing efficient, it was necessary to employ computer techniques previously thought impractical or simply impossible.

All intercept copied on an AG-22, or prepared in an AG-22 compatible format, is processed through the Generalized AG-22 Processing System (GAP) which is a series of IBM 360 computer programs. The GAP system standardizes coding, identifies record types, assigned a processing trigraph based upon case notation, and provides various coverage accounting and quality control listings. Based upon processing trigraphs, GAP data are directed to various subroutine programs. At present there are five user routines operational for B Group problems:




The outputs generated by the user routines are compatible with the existing manually prepared vehicles but may differ slightly in format. Data for B Group entities other than those listed above are directed to LEFTOVER lists which presents traffic in chronological order as copied.

Each of the user routines has follow-on programs which are run prior to the presentation of the data for the traffic analyst -- usually less than 24 hours after intercept. These programs do

much of the preliminary data sorting and listing required by analysts. Within the [redacted] routine, which has the largest number of users, for example:

1. Callsigns are paged and indicated if predicted for that case.

2. Callsigns are matched against callsigns from all files processed during the last five days. The number of files in which a callsign appeared on the same case will be indicated as well as the number of files in which that callsign appeared on a different case. The differing case will be indicated.

3. Files notated [redacted] are matched against all cased and uncased data for the past five days and if possible, reidentified based on callsign usage. If the match is against uncased data, Arbitrary Case Notations (ACN's) may be assigned based on callsign page usage or two-day continuity.

4. Frequencies and schedules are presented in link increments and the reason for each contact break is entered.

5. Preambles are formatted and in some cases traffic type indicators are inserted.

6. Chatter lines are profiled and weighted to indicate significance.

7. Message address information (PAG's, BSD's, etc.) is isolated and presented in a formatted record.

8. Special records indicating call-up order in multiple call-up are generated.

All this is done because analysts and programmers got together and let their imaginations run away with them. The limits of the computer's ability to perform preliminary analysis has certainly not been reached. As we continue to work with the AG-22 and its output, even more capabilities will be defined. Perhaps some day we may even....

Complete this paragraph in 50 words or less and submit your dreams to Peggy Barnhill, B42.

DDP - DEDUPE, DELETE AND PROGRESS

by Charles W. Swift, B6404

A basic problem that touches every individual in B Group, and probably throughout all Production elements, is the inability to take actions because of missing and misrouted messages. TECHINS 1043 and 1044 provide specific guidance for the routing of information and use of Delivery Distribution Indicators (DDIs) which should assure the proper flow of material; but in practice many problems arise due to a variety of causes.

Instead of seeking out the causes for missing messages, many elements have arbitrarily added DDIs on the theory that if their DDI is on a message they are assured of receipt. Since many DDIs have multiple addressees, this method actually compounds the problem and clogs the machinery designed to provide timely and efficient service to NSA elements.

A recent survey in one B Group office revealed that excess copies of DDP material were being received. One third of the message copies received were tossed away before they reached branch level. Some field stations forwarded technical support messages using DDI combinations that dumped as many as thirty-five copies of the message into the office. At least fifteen copies were tossed away, and only five were really required. Three factors contributed to this situation:

(1) Failure by the field stations to select DDIs according to TECHINS 1043 and 1044. In some instances, the field station had obviously chosen to use multiple DDIs to assure delivery; in other cases the erroneous use had been directed by elements within the office.

(2) Failure to assign qualified and dedicated personnel to distribution functions. Distribution was usually treated as a secondary duty in most elements.

(3) Failure to provide knowledgeable individuals as the focal point for all message distribution problems to assure that distribution personnel at all levels were advised of requirements.

Since "austerity" is the word of the day it would only seem logical that now is the time to isolate costly trouble spots in every facet of operations. We in B Group are in a position to do our part now in respect to the handling of incoming messages. We have started in the right direction by providing for one knowledgeable individual in each office in B to act as the coordinator and authority on all DDI problems, both in-house and field-related. Other actions which should be taken are:

(1) The assignment of qualified individuals to perform distribution functions at all levels.

(2) The constant review and monitoring of DDI requirements by individual elements to differentiate between what is required for job performance and what is just nice to have. The DDI coordinator and the office of primary interest would then be informed of misuses of DDIs and any instances where distribution of material could be reduced or eliminated.

By implementing these procedures a great number of the message copies could be eliminated. This would allow distribution personnel to concentrate more on accurate distribution thereby probably decreasing retransmission requests. A cooperative effort by all elements would relieve the pressure placed on our limited teletype distribution system, thus assisting in the timely receipt and handling of our correspondence.

****

"Though the hen may cackle all day, she can lay but one egg."

....from the Burmese

CHINESE VOICE: SOLUTION TO A DILEMMA

by L. St. Clair Myers, B441

Let's take a close look at NSA's problems in coping with Chinese voice intercept -- one of the least understood and [redacted] problems in the Agency. Spoken Chinese is without doubt more difficult to grasp than the written language. Native speakers are generally the only ones who can fully perceive the tonal differences and understand the subtle colloquialisms inherent in the language. However, the use of native speakers is not, ipso facto, a total solution to the problem. Only rarely is it possible to find one who can put the information down on paper in good English; his usual procedure is to transcribe what he hears into the Chinese characters of his native language, usually in the cursive script, which is a shorthand form referred to as "grass writing." But understanding this form requires a well-trained linguist -- [redacted]

NSA and the Service Cryptologic Agencies (SCA) rely upon the use of military men trained in spoken Chinese who interpret what they hear and put on paper, in English, their translation of what is transmitted. (In NSA these are erroneously called "transcriptions"). Intercept tapes that the military linguists are unable to translate must be sent to [redacted] NSA for translation. Seldom are field-translated "facts" called into question, and the only way that NSA can check their accuracy is to request the original tape from the intercept site -- if it has not been erased after the lapse of the 60 days permitted by current instructions. Few other SIGINT problems accept the risk of erroneous field translations so trustfully.

Few of these young military voice transcribers have worked with the language long enough to develop the vocabulary or experience to cope with colloquial words or phrases that go beyond the routine, stereotyped military language for which they have been trained. Furthermore, neither NSA nor the Service Cryptologic Agencies (SCA's) are likely to expend the time and money required to develop the large number of really expert linguists that are needed at intercept sites to translate (transcribe) voice intercept with the degree of accuracy that NSA's mission requires.

How, then, can the present system be improved? The optimum is to have thoroughly seasoned linguists at the point of intercept; lacking this capability, the system must be geared to the capabilities of the personnel involved. As noted above, professional linguists at the point of intercept are not likely to be provided, so it may be necessary to consider a plan utilizing less qualified personnel and change to a new technique. By using PINYIN [redacted] as a time-saving shorthand device where possible, military linguist transcribers in the field could turn out true transcriptions that retain the original terminology for analysts to check -- if checking is really necessary.

PINYIN is the official CHICOM romanized spelling of sounds in the Chinese language. PINYIN was invented in 1957 for a variety of reasons, both practical and political. [redacted]

Translation of the PINYIN [redacted] is the next problem to be considered. The transcribers could translate the material as they go (or later), either in the right-hand margin or directly beneath the Chinese PINYIN. In my opinion, written translations are not necessary until they become essential for the analyst or reporter's understanding of the transmission, or for inclusion in a SIGINT product report. Visual (mental) translation should be sufficient for most analysts familiar with stereotyped text - and it is not as difficult as one might think. In effect, traffic analysts reading Morse and teleprinter chatter [redacted] are (right now) doing just that -- reading Chinese (even if imperfectly). And if all analysts are thus forced to absorb some slight knowledge of the Chinese language in order to do their job (and do it better), wouldn't this be an additional benefit to the Agency? And who knows how many of these non-linguist analysts might develop into competent linguists after formal training in the language?

THE CREATIVE TRANSLATOR

by Tom Glenn, B61

"It is essential that the captain take steps to assure an attack as soon as possible," the translation read. "No delay will be accepted." I knew that the text in question has been passed in the heat of battle, by a man desperate in the face of imminent defeat and possibly death. It struck me that his language was rather formal for the occasion. The original read, "DAIJ UYS DANHS CHO DWOCJ CANGF SOWMS CANGF HAY LAF CHUR YEEUS CHAAMJ ZIF KHOONG DWOCJ." I would have translated it, "Strike soonest without fail. ((Time)) is of the essence. Any delay will mean failure." The first translation was not wrong. It simply missed the point.

The example is an extreme one (and it has been somewhat altered to protect the guilty), but it is symptomatic of a tendency of translators to smooth out the unruliness of the original, to impose order and business-like calm, to express everything in unruffled government English. When we do this, we destroy the vitality of the original, dehumanize it, and distort it. In so doing, we do our customers a distinct disservice to say nothing of insulting their maturity.

This article, then, is a plea for more creativity in translation. Unlike other disciplines where there is only one right answer, translation plunges the practitioner into the world of ambiguity where there are plenty of wrong answers and many right ones. The choice of the most nearly accurate answer depends not on dictionaries, grammars, and TECHINS, but on intelligence, emotion and understanding. For translation is rooted in language, which is first and foremost a sensual thing irretrievably tied to feelings in the chest, throat, mouth, nose and ears, and heavy with emotional cues. But language is also our primary means of information communication and bringing minds out of darkness. And as any linguistics student will tell you, language is erratic, syncretic, and dynamic. In coping with such an animal, creativity -- the ability to deal with the unknown and find new answers -- is simply necessary.

There is nothing particularly revolutionary in any of the foregoing. But, surprisingly, we largely ignore the need for creativity in translating. Our rule-ridden procedures with programmed solutions for all eventualities are in part to blame. We have sought, as most organizations do, to take the the uncertainty out of our daily work by promulgating proper procedure appropriate to whatever circumstance. For translating it is a futile effort. For no matter what the girth of our guides, glossaries, grammars, dictionaries, memos, lexicons, manuals, and primers, we cannot replace inventiveness with rules. But since we have tried so valiantly to do so, we can hardly blame our translators for believing that modalite is always translated as "procedures," or that 利 用 invariably means "exploit." What we have done, in effect, is make admirable progress in achieving machine translation from human beings.

Fortunately, it doesn't work. One reason is that words mean such different things to different people. As an Irish nurse once explained to me, "the screw" in the British Isles is slang for "wages." Similarly, "Defense de trepasser," as a sign on a cemetery gate in Canada announces means "no trespassing," not "no dying;" in the same part of the world, "chars usages" means "used cars," not "shopworn chariots." The influence of Americans on the nations of Southeast Asia has produced new hybrids. A sign in Saigon warns "Pas de fumer n'est permis" -- a French version via Vietnamese of the redundant military English, "No smoking allowed." In some oriental languages it is impolite to answer "no" to a superior. Thus, a Vietnamese who worked for me in Saigon, in trying to adapt to American casualness, answered most of my questions, "Da khong a" -- "Yes, no, sir." In English, "no doubt" often means there is some doubt; "fat chance" means "small likelihood;" and "Surely you don't mean that" means, "My God! You mean that!"

Despite these and other problems, translators persist in trying to program themselves. We could help them in three ways. First, we should emphasize mastery of English, a factor in translation we have overlooked with dogged consistency. First rate translation, after all, requires a profound understanding of the way English works, how it can be driven, shaped, cut, and tooled to make it catch the sense and feeling of the original.

Second, we should train translators -- and especially B Group translators -- to become comfortable enough in the foreign language that they can sever their dependence upon English to understand foreign texts. In essence, translators should be able to read a sentence in the target language, understand it without reference to English, and only then take up the question, "How do we say that in English?" Aids to reaching this stage are a good ear well tuned to the sound of the target language, a willingness to grasp at the basic meaning of a word which has no equivalent in English ("lai" in Vietnamese, for example, has only one meaning, not the half dozen dictionaries give), and ability to think without recourse to words. "Voila," can best be understood in terms of gesture and facial expression; "Khoi" in terms of picture of a circle and things outside it.

Third, we should encourage cross training of linguists, ideally in related languages. Chinese is the Latin of Southeast Asia; knowledge of Chinese is a valuable asset to Vietnamese, Korean, and Japanese linguists who must struggle with borrowed words often very difficult to translate. Thai and Lao are closely related. And so on.

Finally, and perhaps most important, translators must learn to unleash their minds. Rote translation works for some texts all of the time and all texts some of the time, but not for all texts all of the time. It is at this juncture that creativity -- the choice of right phrase or word in English to match the thought and flavor of the original -- becomes crucial.

****

"A translator hath nede to lyve a clene lif, and be ful devote in preiers, and have not his wit occupied about wordli thingis, that the Holi Spiryt, the autour of wisdom and kunnyng and truthe, dresse him in his werk and suffre him not for to erre."

.....Wyclif

ANALYZATION OF DATA

by Richard V. Curtin, B11

An analyst should first study data in its original form looking for obvious or significant points. By all standards it is most important that an analyst look for virtually any and all signs of unusual conditions which could occur in any form, in any data.

Customarily a thorough analysis is a primary goal but prior to any thorough analytic study, much can follow from initial scanning of data looking for virtually any important sign or signs. Do this first! From this point, particularly having run out of initial scanning of data, an analyst who works with traffic should dirty his hands by actually handling and sorting traffic in its original hard copy form.

Going through traffic, occasionally voluminous amounts of traffic, is a duty of all analysts. Having to do this has its applications to follow-on analysis. In this follow-on analysis many sound conclusions may solidify by improving facts first found during initialization. Just to avoid confusion, analysis is not sorting traffic -- it is a logical accounting for all individual parts of a main body of data.

Knowing functions and limits of said individual parts is important. Looking at all parts individually and as a group is also most important. Missing parts could focus on basic primary origins of data. Non-association of parts could add support to analysis also.

Odd or unusual conditions should aid in producing a working copy of an original body from which your data was forthcoming. Primarily, in addition to analysis of data, an analyst must list all significant facts for historical background information. Quick logical draw back of this information is an important point in analyzation. Random approach to draw back of data is not satisfactory in most situations.

Should various arts and skills apply, an analyst must vary his attack accordingly. This is a sign of a good analyst -- pliability or adaptability to situations and changing conditions. Until an analyst displays this quality in his analysis, an analyst is not functioning at a maximum standard.

Vital to all analysis is a thinking analyst, with ability to occupy his mind with various and sundry points. Which point to disavow or disclaim and which to follow-up is not always obvious. X-ray vision would aid any analyst, in both scanning of data and looking into goals of tomorrow.

You, as an analyst, occupy a vital position in an analytic community -- much of your analysis is original with no duplication by co-analysts, thus your analysis is primary to analytic community goals and missions. Z-groups and A-groups of valid data groups should aid cryptanalysts in locating indicator or discriminant groups and in turn aid in important cryptologic findings.

(Did you do any analysis of this data?)

(Editor's note: We will have further comment on this article in the December issue of Dragon Seeds.)

****

PLAIN ENGLISH

One should hyperesthetically exercise macrography upon that situs which one will eventually tenant if one propels one's self into the troposphere.

Look before you leap.

## CRYPTO-SCRAMBLE

*Richard Atkinson*

**Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.**

1. B I L L I T E A R
   _O_ _ _O_ _ _
   **Substitution method involving two cipher characters for one plain character.**

2. T R I P E B A I T
   _O_ _ _ _ _O_
   **System in which the cipher units may be *divided into two separate parts, each with* clearly defined functions.**

3. A G R I D C H I P
   O_ _ _ _ _ _ _ _
   **Substitution method in which the plaintext *units are treated as pairs of characters.***

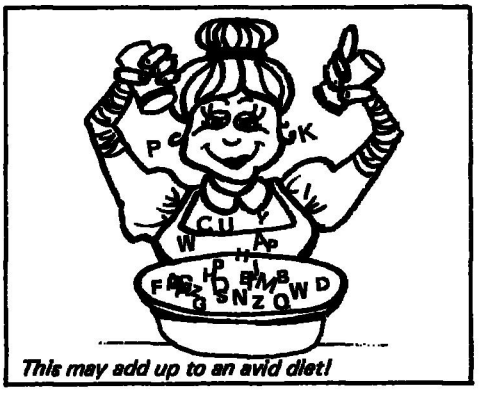
4. V A I N S T A R
   O_ _ _O_ _ _
   **Two or more cipher symbols which have the same plain equivalent.**

5. A N A I D
   O_ _ _ _
   **RYE program which produces digraphic distribution and statistics.**

**Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.**

**Print CRYPTOANSWER here**

_ _ _ _ _ _ _ _ _



*This may add up to an avid diet!*

# SEEDLINGS

----The 10th Professional Qualification Examination in Cryptanalysis will be given on Monday and Tuesday, 15 and 16 November 1971. Personnel who wish to take any or all parts of the examination should contact the CACP office, Room 3A116, 3868s by 5 November 1971. Anyone interested in attending prep sessions for the examination should contact Al Verbitz, B03, on 5296s.

****

----PQE #5 will be administered by the Traffic Analysis Career Panel in the north side of the NSA FM cafeteria on Monday, Tuesday and Wednesday, 6, 7, and 8 December 1971. A new TACP study outline has been prepared for distribution to all aspirants. To ascertain eligibility, candidates should submit PQR's, addenda, and reports to the TACP office, Room 1C190, by 5 November 1971.

****

----The Language Career Panel is investigating the possibility of requiring all candidates for certification to demonstrate their ability to understand their target language as spoken formally. The requirement would not be rigidly imposed for several years (1975 is being mentioned) to allow for the arrangement of proper training.

****

----"The SEATS Message Log - Building a Cryptanalytic Tool," published by B65 is an excellent summary of the current SEATS processing cycle. Although written for cryptanalysts, traffic analysts who'd like to understand more of the processing behind-the-scenes can learn from this well-written report. It's B65-SSR-02-71 dated 15 August published by B654.

****

----A compilation of various briefings given during the February 1970 "Traffic Analysis Mechanization Forum" was published recently. Twenty-four briefings were delivered at the

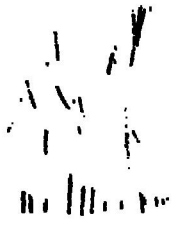
forum including four B Group presentations: "Introduction to T/A Mechanization," R.S. Benjamin; "Southeast Asia" by Fred Mason and Dick Alexander, and "Vineland" by Dick Wilschke. Copies may be obtained from Mrs. Gloria Chiles, P14, 5868s.

****

----Virginia Jenkins, B13, who is developing the new course, "Practical Diagnosis" - CA 260, which deals with the cryptanalysis of hand systems and cipher devices and features operational problems, is soliciting input from B Group. Of particular interest are cipher systems employing non-cyclic additives, and rail-fence or grill transposition.

The pilot class in CA-260 was held between 15 March and 17 May 1971. The next class is scheduled for March 1972. Persons interested in attending or who have subjects for inclusion may contact Virginia Jenkins on 8-8016s.

****



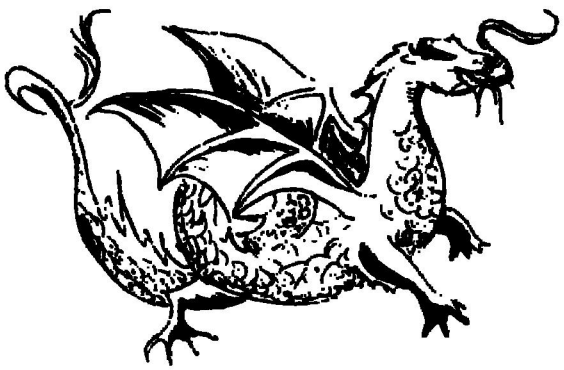
----The Council of Learned Organizations (CLO) is planning a symposium to acquaint the NSA community with the interrelationships that exist among the major cryptologic disciplines, with computer serving as a unifying theme, by means of lectures, exhibits and tours. The event is scheduled to take place in March 1972.

****

----In an effort to cultivate professional linguistic activity throughout the cryptologic community, the Crypto-Linguistic Association is encouraging the formation of Special Interest Groups. For particulars, contact Dr. Amelia Murdoch, 4767s.

****

Articles for publication may be submitted through Division Press Corps members or directly to DRAGON SEEDS, B03.



EO 3.3b(3)
PL 86-36/50 USC 3605

ASK THE DRAGON LADY

Dear Dragon Lady:

In planning the itinerary for [redacted] forthcoming visit to PEKING please try to arrange an opportunity for him to visit the Gate of Heavenly Peace in the old city of PEKIN[redacted].

If the time can be found, he should also visit PEIP'ING, [redacted] particularly for a view of the T'IEN AN MEN and its striking architecture.

During the period of his visit he might be able to arrange a side trip to both PEICHING and BEIJING enroute to or from the airport.

During the [redacted] stop at CANTON a short sightseeing trip around KUANGCHOU and GUANGZHOU should also prove interesting.

LAWRENCE ST. CLAIR MYERS
B441, 4637s

****

The Dragon Lady received the following two letters referring to problems of terminology, so she passed them on for authoritative comment to our A-number-one glossarist, the Guru and Caudillo of the Dundee Society, Lambros Callimahos.

Dear Dragon Lady:

What is high-grade traffic?

Is it that type which is machine enciphered? If so, why do areas with no machine enciphered traffic categorize some of their traffic as such? Is it the type in which an additive is applied to an already enciphered text? What if the generation method of the additive stream is exploitable? Is it user-related?

These are just a few of the ambiguities I have encountered. The BASIC CRYPTOLOGIC GLOSSARY, June 1965, defines high-grade as "Of a cryptosystem, offering relatively great resistance to cryptanalysis." How does one measure "relatively great resistance?" Is it in the eye of the beholder? If so, then all of the above truly be high-grade.

Can you offer a more precise meaning for this oft used term?

CAROLYN Y. BROWN
B1122

Dear Carolyn:

In answer to your question, let us examine for a moment three definitions as found in the first (1955) edition of the Basic Cryptologic Glossary:

"low-grade, adj. Pertaining to a cryptosystem which offers only slight resistance; for example: (1) Playfair ciphers, (2) single transposition, (3) unenciphered one-part codes."

"medium-grade, adj. Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example: (1) strip ciphers, (2) double transposition, (3) unenciphered two-part codes."

"high-grade, adj. Pertaining to a cryptosystem which offers a maximum resistance to cryptanalysis; for example: (1) complex cipher machines, (2) one-time systems, (3) two-part codes enciphered with an additive."

These definitions were dropped from the second (1965) edition,

because obviously the relative security of a cryptosystem is in the eye of the beholder: a single transposition cipher may well be a high-grade system (as for example a certain German World War II cipher); and a "one-time" system may be low grade if the Fibonacci generating-group, even if randomly chosen, is sent in the clear as the A1 group of the message. A two-part code enciphered with an additive book may be a high-grade system if the code book is unknown, the additive book large, the indicator groups enciphered, and the cryptoperiod changed frequently; but if the code book is known, the additive book small, the indicators sent in the clear, and the keys in effect for a long period, the system would probably qualify as a low-grade system. All of the foregoing remarks apply to our cryptanalysts; a cryptanalyst from an emerging African republic might find it impossible to cope with a Playfair cipher, and so as far as he was concerned it would be a high-grade system. And so, Carolyn, the definitions for low-, medium-, and high-grade cannot be made more specific, since they are so subjective.

****

Dear Dragon Lady:

I am a newcomer to the world of manual cryptosystems and the jargon has me completely confused. There is a definite terminology gap between "the honorable elders" and the neophytes like myself who have just completed basic CA courses. In fact, there even seems to be a terminology gap between the different training courses (i.e., CA-100, CA-400, CY-100).

For example, what is biliteral substitution? The 1965 edition of the Basic Cryptologic Glossary defines it as "encipherment by substitution methods in which the cipher text units are pairs of characters." What about the plaintext units? If the size of the plaintext unit is larger than one element (medial plus final or medial plus final plus tone) is it not now digraphic? Suppose variants are employed on a digraphic system (where plaintext unit size is larger than one) is the system digraphic with variants, code chart with variants, or is it all lumped under biliteral with variants?


Is a dinomic system included under biliteral or digraphic .... or both?

And finally, why has the term "uniliteral" replaced the term "monoalphabetic" which is universally recognized and accepted? How does one refer to the basic units of cipher? "Unilits?" "Bilits?" Where is the new crypt glossary?

HELP!!

DAVID J. SHEPARD
Hll

Dear David:

First of all, David, you must realize that some "honorable elders" are just older, but not necessarily wiser: we have some first-class technicians who would flunk freshman English. Again, the terminology gap between different training courses is a function of the glossarial erudition of the particular instructor. Now for your compound question.

In biliteral substitution the cipher elements are pairs of characters, regardless of the size of the plaintext elements (which may be single letters, pairs of letters, or even units of larger size); in digraphic substitution the plaintext elements are indivisible pairs of characters, regardless of the size of the cipher elements (which may be, for example, pairs of letters, trinomes, or other combinations). A Playfair cipher is digraphic (because the plaintext elements are indivisible pairs of letters), biliteral (because the cipher elements are pairs of letters), and monoalphabetic (because there is a one-to-one correspondence between plain and cipher equivalents)--although the latter should not be stressed lest it confus young, impressionable minds or incense older, stultified ones.

A "digraphic system with variants" is self-explanatory, as is "code chart with variants" if a code chart were involved; "biliteral system with variants" would usually imply variant coordinates in connection with some kind of a cipher square. A "dinomic system" is either a biliteral system, or one in which plaintext dinomes are subjected to further cryptographic treatment.

A simple substitution cipher is monographic (because the plaintext elements are single letters), uniliteral (because the cipher units are single letters), and monoalphabetic (for reason given above). Cipher elements are called "characters," "digraphs," "trigraphs," etc. The third (1971) edition of the Basic Cryptologic Glossary, which has just been completely revised, should be printed and distributed during November.

Any further questions?

****

"It is only when there is some mortal deserving of being delivered that the single live hair of the most excellent Buddh protrudes itself and stands forth in a straight line from between the eyebrows."

---the Manual of Buddhism

CONTRIBUTORS

PEGGY BARNHILL, a data systems analyst in B42, is a 1966 graduate of Marywood College, Scranton, Pa. She completed the SR Intern program in 1970 and is currently working on the software specifications for the AG-22 processing system within B Group.

DICK CURTIN, Deputy Chief, B11, entered on duty with NSA in 1950. After initially working on the Soviet problem, he was selected for the first class of CY-100 and subsequently became involved in cryptanalytic attack on various A, B, and G problems. He received an NSA scholarship to complete his bachelor's degree in mathematical statistics from the George Washington University. Mr. Curtin is certified by the CA, TA, Data Systems, and Mathematics Career Panels.

AL GILBERT, B6403, came to NSA in 1966 after retiring from the Army Security Agency as a CW3. While in ASA, he served in Europe, the Far East, SE Asia, and at NSA, working at various times as reporter, traffic analyst, Russian linguist and cryptanalyst. Mr. Gilbert, who is professionalized as a Special Research Analyst, has worked on the Vietnamese Communist military problem since 1966.

TOM GLENN, Deputy Chief, B61, has a total of thirteen years experience with ASA and NSA on the Vietnamese problem. He is a professionalized special research analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-1965, 1967-1968 and 1969, he has been involved in traffic analysis, cryptolinguistics, intelligence analysis, and - most significantly - in the management of the SIGINT reporting effort on the Vietnam war.

DONALD LENAHAN, a cryptanalyst in B22 on the CHICOM [redacted] problem, entered on duty with NSA in 1967. He completed the CA intern program with assignments in A, B and G Groups, and is professionalized as a cryptanalyst. He holds a B.S. in German from Manhattan College and is working on a master's degree at Georgetown University.

EO 3.3b(3)
PL 86-36/50 USC 3605

EO 3.3b(3)
PL 86-36/50 USC 3605

L. ST. CLAIR MYERS, CHICOM bookbreaker and [redacted] Coordinator in B44, is also a qualified bookbreaker and cryptolinguist in Russian and Japanese. During his U.S. Navy service (1941-1966) he rose to the rank of Commander and served as Chief of the CHICOM [redacted], Officer-in-Charge of various NSG activities, and Chief of [redacted] and NSAPACREP Korea.

WAYNE E. STOFFEL, B03, began his cryptologic experience in 1946 with a three-year tour in the Army Security Agency. At NSA he worked on the Soviet problem until 1954 and on Asian targets thereafter. Mr. Stoffel was a member of the TA Career Panel from 1965 to 1971 and has been an associate editor of COMMAND since 1968. He holds a B.S. degree in physics from Johns Hopkins University and is certified in the TA, CA, SRA, and Physical Science Career Fields.

CHARLES SWIFT, B6404, served four years in the Air Force Security Service as a traffic analyst on CHICOM [redacted] and on the Vietnamese Communist problem during the pioneer stages of SEATS. Following his conversion to civilian employment at NSA in 1966, he has worked in the Vietnamese Communist support division, and has recently been reassigned to B61.

PL 86-36/50 USC 3605

*Remember !*

*It's classified*

~~TOP SECRET~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~