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

~~TOP SECRET~~

What? Where? Why?

by GERALD A. FARR, RO4

EO 3.3b(3)
EO 3.3b(6)
PL 86-36/50 USC 3605

Where?

Why?

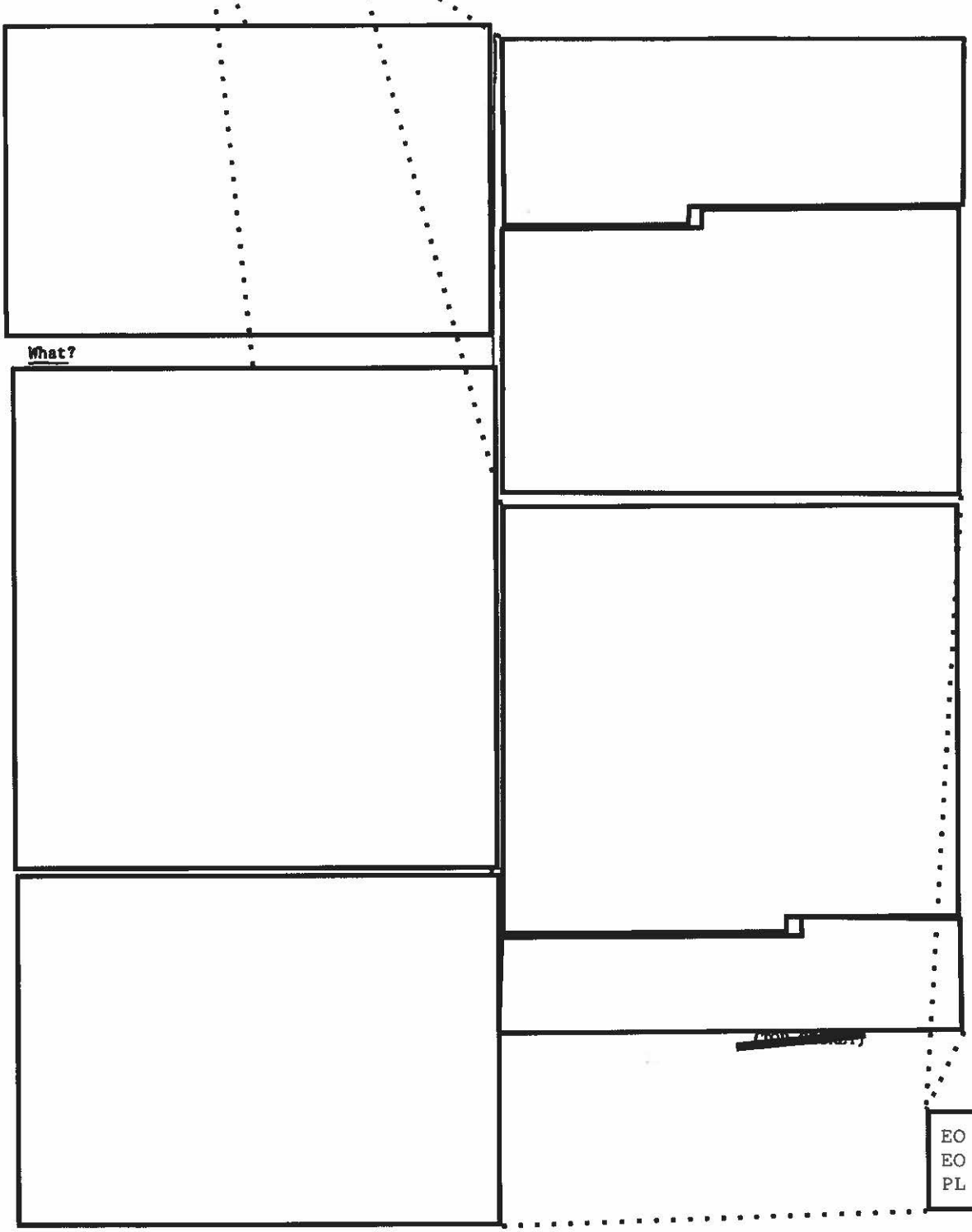
Congress approved the funding of it in the FY71 Military Construction Appropriations Act and construction was begun by a U.S. Navy SEABEE task force in early 1971 and is expected to be completed by late 1975.

~~TOP SECRET~~ HANDLE VIA COMINT CHANNELS ONLY

Declassified and Approved for Release by NSA on 03-10-2021 pursuant to E.O. 13526, MDR Case #109356

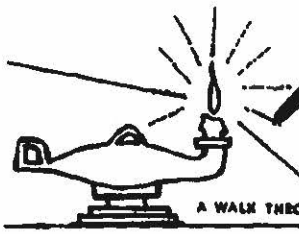
EO 3.3b(3)
PL 86-36/50 USC 3605

~~TOP SECRET~~



EO 3.3b(3)
EO 3.3b(6)
PL 86-36/50 USC 3605

~~TOP SECRET~~



NEW TRENDS IN THE TEACHING OF CRYPTANALYSIS

A WALK THROUGH THE '75 CURRICULUM

BY VIRGINIA C. JENKINS, E13

A major project currently under way in the Cryptanalysis Department of the National Cryptologic School will change the way cryptanalysts of the future learn their trade. Three of the basic cryptanalysis courses will no longer be taught traditionally from the platform in a classroom. They are being redeveloped and written, over a 3-year period, as self-paced instruction courses to be presented in the NSA Learning Centers at Fort Meade (Room 2W165) and FANX II (Room A2A16B). The three courses affected are: CA-011, Survey of Manual Cryptosystems, CA-100, General Cryptanalysis, and CA-120, Survey of Machine Cryptosystems.

As each of the new, self-paced courses is completed, it will be made available in the NSA Learning Centers. Students will do their studying in the Centers, working when they feel like working, and proceeding at their own pace. Some parts of these courses make use of multi-media equipment--TV, slide projectors, and audiotapes. All courses will be available in written form, but often the student will be able to choose his own medium. The instructor's role will be to give individual assistance upon request.

The project to self-pace these courses is halfway into its second year. One course, CA-105, Introduction to Cryptography and Exploitation of Manual Cryptosystems, has already been completed and will be offered soon in the Fort Meade Learning Center. A second course, CA-107, Exploitation of Manual Cryptosystems, is being written now and is scheduled for July 1975 completion. The final two courses, CA-121 and CA-122 (Hagelin and Wired Wheels) will be written between July 1975 and July 1976.

Along with self-pacing the basic courses, the entire cryptanalysis curriculum has been reorganized to show exactly what type of student and job each course is designed to satisfy. There are three levels, distinguished by the first digit of the course designator:

The 000 level consists of Background Courses designed for students who do not do any cryptanalysis in their jobs.

The 100 level consists of Basic Courses designed for students who perform cryptanalysis as all or part of their jobs.

Courses at the 200 level or above are Advanced Courses designed for students whose job is cryptanalysis.

The newly-developed self-paced courses are in the 100 level Basic Courses.

Background

One of the oldest cryptanalysis courses listed in the current NCS Catalog is CA-011, Survey of Manual Cryptosystems. Until about 1966, this course was taken by everyone who wanted to learn about cryptanalysis--aspiring cryptanalysts, linguists, traffic analysts, reporters, and engineers--a most heterogeneous group. It was a 3-week full-time course covering cryptography and simple analysis of manual cryptosystems.

When CA-100, General Cryptanalysis, was written in 1966, all of CA-011 was incorporated into it and a considerable amount of new material (analysis and theory) was added. The course now introduced a new analytic aid, the computer (RYE), to cryptanalysis courses. Originally, CA-100 covered both manual and machine cryptosystems and took 10 weeks full-time to teach from the platform. Eventually the two weeks devoted to cipher machines were split off, expanded, and made into a separate 3-week course called CA-120, Survey of Machine Cryptosystems, leaving CA-100 as 8 weeks of manual cryptosystems plus RYE.

A lot of NSA analysts were trained well by these three courses. But there were some problems with them, due primarily to the fact that the curriculum "just grew," without much planning. One was a high degree of duplication between CA-011 and CA-100. Students did not know which course to take, and the many who took both were understandably bored by the repetition (which also wasted many training dollars). CA-120, in spite of its title Survey of Machine Cryptosystems, has not kept up with the times. Hagelin and Wired Wheels are well represented, but the Shift Register unit is woefully inadequate. Until recently there was no prerequisite for CA-120, and the pertinent polyalphabetic information from CA-100 had to be included again in CA-120. For students who had taken both CA-011 and CA-100 previously, this meant the third exposure to the same material.

In addition to the problems with course content, there were teaching problems as well. The annual heavy student loads for these popular, basic courses consumed a disproportionate amount of instructor time. Typically 71 per cent of the cryptanalysis instructors spent most or all of their time on these 3 courses. This left no time--or energy--to do research and to develop new courses, especially some urgently needed to train the analysts who need multiple disciplines to work on today's complex problems.

Self-paced Courses

The decision to self-pace some of the basic CA courses was made in order to deal with such problems. It provides the opportunity to make many improvements: to modernize the contents of the courses and to arrange them in a sequence designed to build up knowledges and skills progressively. Self-paced courses insure that everyone gets the same basic information: a boon to teachers of advanced courses, who must often reteach what should have been learned in a prerequisite course, but was not. They also mean an end to the wildly heterogeneous classes which are so frustrating to students and teachers alike.

Important revisions in course content will also result. The unnecessary and confusing division into cipher and code has been eliminated. Code takes its rightful place (from the cryptanalytic point of view) as a form of monoalphabetic substitution system. (Actual reconstruction of the code after the initial break-in is not a cryptanalytic process but a cryptolinguistic one.) The traditional but (to me) unnatural split between manual and machine cryptosystems will be scrapped, and machine cryptosystems will be taught as mechanized polyalphabetic substitution. The arithmetic of substitution will be taught in the very first course, and superencipherments will be presented as polyalphabetic substitution with numerical cipher alphabets. Everyone is now required to learn how to use existing computer programs to help solve CA problems. RYE is currently taught but provisions have been made to substitute other systems when RYE is replaced.

These are just a few of the changes brought about by the self-pacing project.

Basic Courses

The courses being redeveloped as self-paced courses are among the basic ones--those taken by anyone who performs cryptanalysis as all or part of his job. The first three listed replace CA-011 and CA-100 and must be taken in sequence. They are prerequisites for all other basic and all advanced courses. Equivalency exams will be available eventually for all these courses. A student who passes an equivalency exam is given credit for the course with a grade of P (Pass). Equivalency exams may be taken only once.

CA-105, Introduction to Cryptography and Exploitation of Manual Cryptosystems (U). SELF-PACED. Terminology, cryptography and basic manual exploitation of manual cryptosystems. Will be offered this fiscal year in the Learning Center at Fort Meade. The student will be given up to 4 months to complete the course.

CA-106, RYE for Cryptanalytic Exploitation (U). (Formerly CA-090.) Use of RYE GUPPY programs as aids in solving cryptanalytic problems. 4 days, 8 hrs/day.

CA-107, Exploitation of Manual Cryptosystems (U). SELF-PACED. Hand and computer exploitation of manual cryptosystems. Will be available in the Learning Centers after July 1975.

The following courses will replace CA-120. They may be taken in any sequence.

CA-121, Hagelin Cryptology (U). SELF-PACED. Cryptography and basic exploitation of Hagelin cryptosystems. Will be available in the Learning Centers after July 1976.

CA-122, Wired-Wheel Cryptology (U). SELF-PACED. Cryptography and basic exploitation of wired-wheel cryptosystems. Will be available in the Learning Centers after July 1976.

CA-123, Shift Register Cryptology (U). (Formerly MA-050.) Cryptography and basic exploitation of shift register cryptosystems. 10 wks, 9 hrs/wk. Prereq: MA-111 or pre-test.

Rounding out the basic courses are some cryptomathematics courses which may be taken at any time after the CA-105--CA-107 block (or equivalent) has been completed.

For non-mathematicians:

CA-110, Introductory Cryptostatistics (U). Theory and use of probability and statistics in cryptanalysis. 2 wks, 40 hrs/wk.

For mathematicians:

MA-145, Modern Probability Theory and Its Applications (U). Theory and use of probability in cryptanalysis. 10 wks, 6 hrs/wk. Prereq: Mathematics through integral calculus.

MA-146, Mathematical Statistics (U). Theory and use of statistics in cryptanalysis. 10 wks, 6 hrs/wk. Prereq: MA-145.

Two correspondence courses in cryptanalysis are also available. Each consists of 10 lessons, and 2 months are given to complete each lesson.

CA-700, Military Cryptanalytics, Part I (U). Monoalphabetic substitution.

CA-701, Military Cryptanalytics, Part II (U). Periodic polyalphabetic substitution.

Advanced Courses

Advanced level courses are designed for the professional cryptanalyst whose job is cryptanalysis. Courses at this level tend to be more closely related to actual jobs, and many use material from live problems in lectures and for student exercises. All but one are taught from the platform and all require some combination of basic courses as prerequisites.

CA-211, Advanced Cryptostatistics (U). SELF-PACED. Intended primarily for the nonmathematician, this course teaches advanced theory and use of probability and statistics in cryptanalysis. (Currently under development; estimated completion is FY 76.)

CA-220, Analysis of Wired-Wheel Cipher Machines (C-XGDS-2). Cryptography and exploitation of wired-wheel cryptosystems and machines; use and analysis of rotor machines to generate teleprinter key. 6 wks, 40 hrs/wk. (TSC-XGDS-2)

CA-250, Key Generation Systems (U). Generation and analysis of prefabricated key (manual, machine, and computer). 8 wks, 20 hrs/wk.

CA-260, Practical Diagnosis (U). Teaches a 5-step process for diagnosing manual cryptosystems, using manual, mathematical, and computer techniques. 8 wks, 40 hrs/wk.

CA-400, Intensive Study Program in General Cryptanalysis (U). Cryptography, diagnosis and analysis of many manual and machine cryptosystems and key generation systems. 18 wks, 40 hrs/wek.

CA-400, Intensive Study Program in General Cryptanalysis (U). Cryptography, diagnosis and analysis of many manual and machine crptosystems and key generation systems. 18 wks, 40 hrs/wk.

For linguists and cryptolinguists:

CA-301, Code Reconstruction (U). Standard bookbreaking tools and techniques, including computer techniques. 5 wks, 24 hrs/wk.

For cryptanalysts with mathematical backgrounds these additional courses are available:

CA-230, Analysis of Hagelin Cipher Machines (S-XGDS-2). Cryptography and exploitation of Hagelin cryptosystems and key, using manual, mathematical and computer techniques. 10 wks, 8 hrs/wk. Prereq: MA-146 and computer programming experience. (TSC-XGDS-2)

CA-240, Shift Register Cryptology for Mathematicians (U). Cryptography and exploitation of shift register cryptosystems. 10 wks, 9 hrs/wk. Prereq: BS in mathematics, engineering or physics, and background in linear transformations.

MA-213, PTAH (U). Intuitive PTAH, computational PTAH, formal PTAH and applications of PTAH. 8 wks, 6 hrs/wk. Prereq: MA-146 and computer programming experience.

MA-250, Theory of Recursive Sequences (U). Generation of linear recursive sequences; plugged registers; dilated registers; Fibonacci and Koken algebra; and non-linear recursive sequences. 6 wks, 10 hrs/wk. Prereq: Background in linear transformations.

MA-302, Applications of Fourier Analysis (U). Linear vector spaces; orthogonal systems; Fourier series; transforms and fast transforms; Laplace transforms; and cryptologic examples. 10 wks, 6 hrs/wk. Prereq: BS in mathematics, engineering or physics.

Background Courses

One cryptanalysis course is designed for students who do not perform cryptanalysis as part of their job but who do need to have a general background in the subject. This course is taken by SR interns, among others.

CA-015, Introduction to Manual and Machine Cryptosystems (U). Terminology, cryptography and some simple exploitation of manual and machine cryptosystems. 4 wks, 40 hrs/wk.

A companion course, CA-013, is currently being offered as part of the general orientation program for newly-hired employees with Limited Interim Clearance.

As the three-year project for writing some self-paced cryptanalysis courses progresses (estimated completion by 1 July 1976), course development will begin to be concentrated on specialized and advanced courses. Two specialized courses at the basic level are already being planned and writing on one of them will begin soon: a course in cryptanalytic documentation including record keeping and report writing. Another course, to teach APL programming with simple CA applications, is also planned.

The Cryptanalysis Department of NCS (E13) welcomes questions about any of these courses or suggestions for new ones. Readers may call 8025 or visit the Department in Room A2A32B, FANX II.

(TOP SECRET UMBRA)

Note:
For a more detailed explanation of the self-paced method, see "Self-Paced Instruction: The Future is Now!" by [redacted] in the August '74 issue.

PL 86-36/50 USC 3605

DEPARTMENT OF GOLDEN OLDIES

A MEDAL FOR HORATIVS

"Hew down the bridge, Sir Consul,
With all the speed ye may;
I, with two more to help me,
Will hold the foe in play.
In yon strait path a thousand
May well be stopped by three:
Now who will stand on either hand,
And keep the bridge with me?"

* * *

"Curse on him!" quoth false Sextus;—
"Will not the villain drown?
But for this stay, ere close of day
We should have sacked the town!"
"Heaven help him!" quoth Lars Porsena,
"And bring him safe to shore;
For such a gallant feat of arms
Was never seen before."

Rome
II Calends, April CCCXL

SUBJ: Recommendation for Senate Medal of Honor

I. Recommend Gaius HORATIUS, Captain of Foot, O-MCMXIV, for the Senate Medal of Honor.

II. Captain HORATIUS has served XVI years, all honorably.

III. On XI March, during an attack on the city by LARS PORSENA of Clusium and his Tuscan Army of ninety thousand (XC) men, Captain HORATIUS, accompanied by Sergeant Spurius LARTIUS and Corporal Julius HERMINIUS, held the entire Tuscan Army at the far end of the bridge until the structure could be destroyed, thereby saving the city.

IV. Capt. HORATIUS valiantly fought and killed one Major PICUS of Clusium in individual combat.

V. The exemplary courage and outstanding leadership of Captain HORATIUS is in keeping with the highest traditions of the Roman Army.

JULIUS LUCULLUS
Commander,
II Legion of Foot

Ist Ind: AG IV Calends, April CCCXL
To : G-III

For comment.

C.G.

IId Ind: G-III
To : G-II

For comment and forwarding.

Change para III, line IV from "saving the city" to "lessened the effectiveness of the enemy attack." The Roman Army was well deployed tactically; the reserve had not been committed. The phrase as written might be construed to cast aspersions on our fine army.

Change para V, line I from "outstanding leadership" to "commendable initiative." Captain HORATIUS' command was two (II) men--only I/VI of a squad.

IIId Ind: G-II II Ides, June CCCXL
To : G-I

Omit strength of Tuscan forces in para III. This information is classified.

A report evaluated B-II states that the officer was Captain PINCUS of Tifernum. Recommend change "Major PICUS of Clusium" to "an officer of the enemy forces."

IVth Ind: G-I IX Ides January CCCXLI
To : XX JAG

Full name is Gaius Caius HORATIUS.

Change service from XVI to XV years. One (I) year in the Romulus Chapter, Cub Scouts, has been given credit for military service in error.

Vth Ind: JAG II Ides February CCCXLI
To : AG

The Porsena raid was not during wartime. The temple of Janus was closed.

The Senate Medal of Honor cannot be awarded in peacetime. Reference is invited to RAR CVII-XXV, para XXI, e.)

The action against the Porsena raid was, ipso facto, a police action.

Suggest consideration for a Soldier's Medal.

VIth INd: AG, XXX IV Calends, April CCCXLI
To : G-I

Concur in para IV, Vth Ind.

VIIth Ind: G-I I May, CCCXLI
To : AG

Soldier's Medal is given for saving lives, suggest Star of Bronze as appropriate.

VIIIth INd: AG III June CCCXLI
To : JAG

For opinion.

Declassified and Approved for Release by NSA on 03-10-2021 pursuant to E.O. 13526, MDR Case #109356

Non - Responsive

IXth Ind: JAG II Calends, September CCCXLI
To : AG

XVII months have elapsed since events described in basic letter. Star of Bronze cannot be awarded after XV months have elapsed.

Officer is eligible for Papyrus Scroll with Metal Pendant.

Xth Ind: AG I October CCCXLI
To : G-I

For draft of citation for Papyrus Scroll w/metal pendant.

XIth Ind: G-I III Calends, October CCCXLI
To : G-II

Do not concur.

Our relations with Tuscany would suffer and current delicate negotiations would be jeopardized if publicity were given to Captain HORATIUS' actions at the present time.

XIIth Ind: G-II VI November CCCXLI
To : G-I

A report, rated D-IV, partially verified, states that Lars PORSENA is very sensitive about the HORATIUS affair.

XIIIth Ind: G-I X November CCCXLI
To : AG

In view of information contained in preceding XIth and XIIth Indorsements, you will prepare immediate orders for Captain Gaius C. HORATIUS to one of our overseas stations.

His attention will be directed to para.XII, RAM, which prohibits interviews or conversation with newsmen prior to arrival at final destination.

SUBJ: SURVEY, REPORT OF
To : Captain Gaius C. HORATIUS, O-MCMXIV, III Legion, V Phalanx, RAPO XIX

Your statement concerning the loss of your shield and sword in the Tiber River on XI March CCCXL has been carefully considered.

It is admitted you were briefly in action against certain unfriendly elements on that day. However, Sgt Spurius LARTIUS and Cpl Julius HERMINIUS were in the same action and did not lose any government property.

The Finance Officer has been directed to reduce your next pay by II and I/II talents, the cost of one sword, officer, and one shield, M-II.

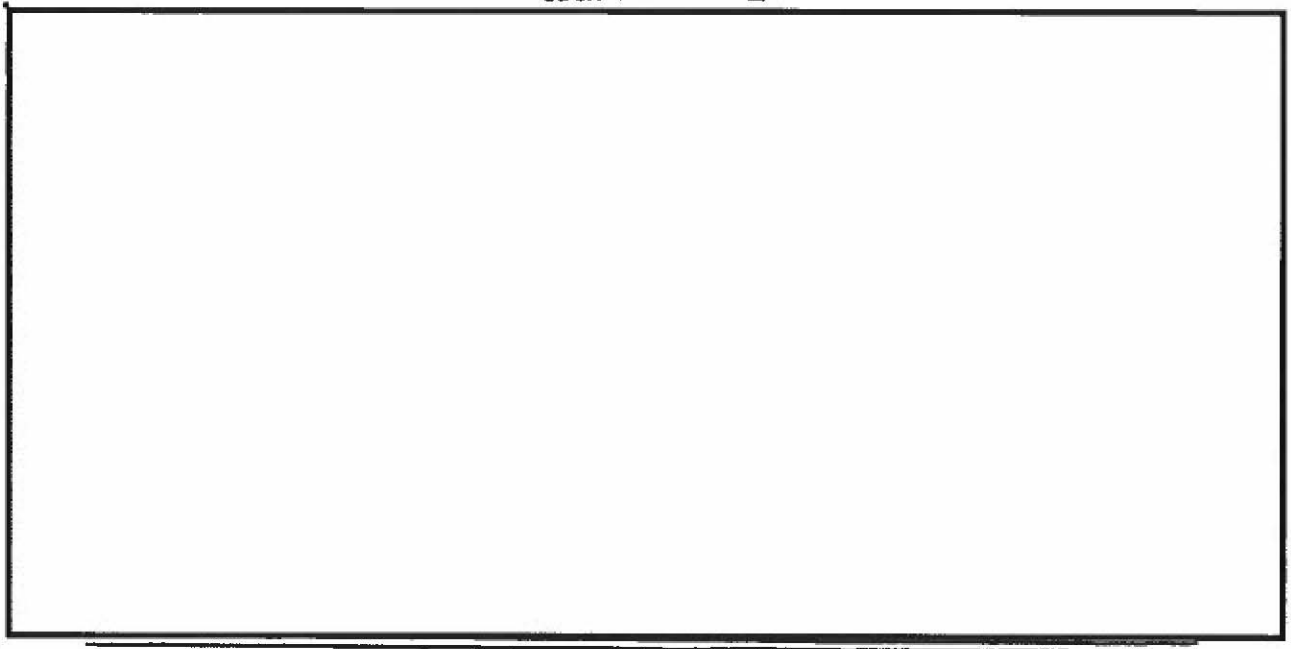
You are enjoined and admonished to pay strict attention to conservation of government funds and property.

H. HOCUS POCUS
Lieutenant of Horse
Survey Officer

P1-Dec 76-53-25039

Non - Responsive

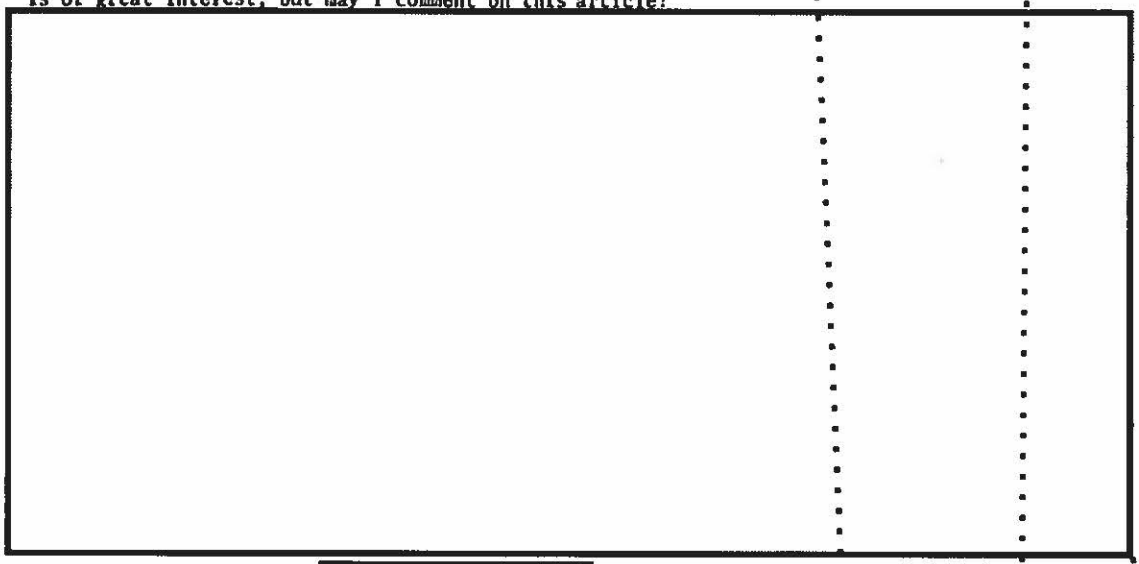
SECRET SPOKE



LETTER TO THE EDITOR

To the Editor, CRYPTOLOG Magazine:

The article in the September issue, "COMINT Analysis of [redacted]" by Derek Craig, is of great interest, but may I comment on this article?



Mr. Craig's analysis [redacted] was a valuable piece of reportage, and I personally enjoyed reading it and learned a lot from it.

Thank you for a very fine new magazine.

(Name withheld by request.)

SECRET SPOKE

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

Declassified and Approved for Release by NSA on 03-10-2021 pursuant to E.O. 13526, MDR Case #109356