STANDARD FORM NO. 64

~~CONFIDENTIAL~~ RELEASE: A61303

Office Memorandum · UNITED STATES GOVERNMENT

TO : Mr. William F. Friedman
S/ASST

DATE: 30 December 1954

FROM : Chief, Training Division

SUBJECT: Conference on Series of NSA Cryptanalytic Texts and Courses

1. You are personally requested to participate in a conference which is to be held in the Director's Conference Room (Rm. 19-244, NSS) at 0900 on 12 January 1955. In this conference you will be asked to consider and evaluate plans for completing the series of NSA basic texts and courses which are to cover the entire field of cryptanalytics.

2. The conference will open with a review of the details of the first text and course which have been completed in this series. Then the presently projected plan for the remaining texts and courses will be outlined, followed by a brief presentation of the general philosophy underlying this series. The Agenda is attached as an Inclosure.

3. Following the formal opening presentation, your views will be elicited concerning the scope of this project and the value of continuing the preparation of this series of texts and courses, both from the standpoint of enhancing the professional stature of Agency personnel and of insuring the preparation of adequate training materials which would be badly needed in case of disaster. The views presented in this conference will become a matter of record, and will be taken into consideration in the establishment of Agency policy.

4. If it is the consensus of the group participating in this conference that the project should be continued and completed in the shortest possible time, a plan for accomplishing this desired end will subsequently be formulated and presented to the Director for approval.

5. Mr. William F. Friedman, S/ASST, will be Chairman of the conference, with the following participating members:

Mr. W. F. Friedman	Col. R. E. Schukraft
Dr. S. Kullback	Dr. L. W. Tordella
Dr. H. H. Campaigne	Mr. F. A. Raven
Dr. R. A. Leibler	Mr. A. J. Levenson
Dr. H. J. Stukey	Dr. R. H. Shaw
Mr. L. D. Callimahos	Mr. F. W. Lewis
	Mr. M. E. Waltz

SHELBY L. PATTERSON
Chief, Training Division

Incl:
Agenda

~~CONFIDENTIAL~~

A G E N D A

OF

CONFERENCE ON NSA
CRYPTANALYTIC TEXTS AND COURSES

(12 January 1955)

Schedule:

0900 - 0902	Introduction
0902 - 0910	Briefing on "Military Cryptanalytics Part I" text and course
0910 - 0920	Briefing on Part II-VI texts and courses
0920 - 0930	Statement of the philosophy underlying this series of texts and courses
0930 - 1045	Discussion
1045 - 1100	Conclusions and recommendations

* * * * *

SCOPES OF PROJECTED NSA SERIES OF TEXTS AND COURSES
ON CRYPTANALYTICS

Military Cryptanalytics, Part I (~~CONFIDENTIAL~~/Modified). Basic terminology and fundamental cryptologic definitions. Cryptography and cryptanalysis of: uniliteral substitution ciphers; multiliteral substitution ciphers; variant systems; polygraphic systems employing small matrices and quadricular tables; elementary teleprinter systems. Fundamental cryptanalytic uses of frequency distributions; "probable-word method" of solution; vowel-consonant analysis; completion of the plain-component sequence; methods of alphabet reconstruction and keyword derivation; "phi test" for determining the mono-alphabeticity of a distribution (monographic and digraphic); tests for matching distributions; analysis involving the use of isologs. Special substitution systems, such as monome-dinome systems, syllabary squares and code charts, and open codes and concealment systems. Basic foreign-language cryptolinguistics. (Prerequisite: none.)

~~CONFIDENTIAL~~

Military Cryptanalytics, Part II (~~CONFIDENTIAL/Modified~~). Cryptography and cryptanalysis of periodic polyalphabetic substitution ciphers; Vigenere, Porta, and other polyalphabetic systems; progressive alphabet systems. Fundamental principles of factoring; "probable-word method" of solution; completion of the plain-component sequence; reduction to monoalphabetic terms when the cipher component is known; theory and applications of direct and indirect symmetry of position; special solutions based on isologs and cryptographic errors. Special types of periodic encipherment, such as Vernam teleprinter encipherment, the "Nihilist" cipher, monome-dinome systems with cyclic additives, periodic digraphic systems, and the "Sphinx" cipher device. The "chi test" for matching distributions; principles of depth reading; basic applications of punched-card tabulating machinery in cryptanalysis; introduction to statistical methods in cryptanalysis; weighting systems applicable to periodic ciphers; Lester S. Hill's algebraic polygraphic encipherment; weather encryption systems; introduction to solution of transposition systems; introduction to aperiodic systems; introduction to traffic analysis; history of cryptology. (Prerequisites: Military Cryptanalytics, Part I).

Military Cryptanalytics, Part III (~~CONFIDENTIAL~~). Cryptography and cryptanalysis of aperiodic polyalphabetic substitution ciphers and repetitive systems. Supression of periodicity by means of irregular-length plaintext groupings, irregular-length key groupings, and plaintext and ciphertext interrupters; methods of lengthening or extending keys; plaintext and ciphertext autokey systems; progressive alphabet systems; solution of indicator systems. Solution of cylindrical cipher devices and strip cipher systems; solution of elementary cipher mechanisms, such as the Wheatstone, Kryha and similar devices. The "kappa test"; weighting systems for the determination of depths; further statistical applications in cryptanalysis; the chi-square test; use of the Poisson Tables and Binomial Tables; diagnostic tests in cryptanalysis. Special solutions based on isologs and cryptographic errors. Applications of RAM equipment and computers in cryptanalysis. (Prerequisites: Military Cryptanalytics, Parts I and II).

Military Cryptanalytics, Part IV (~~CONFIDENTIAL~~). Cryptography and cryptanalysis of transposition, combined substitution-transposition, and fractionating systems. Solution of single transpositions employing various types of matrices; solution of double transposition systems; matrix reconstruction; key recovery; reconstruction of literal keys; revolving grilles and Sacco grilles; special solutions based on isologs and cryptographic errors. Solution of the ADFGVX system; bifid and trifid fractionating systems; polygraphic systems with fractionation. Applications of analytical machine techniques in the solution of transposition systems. (Prerequisites: Military Cryptanalytics, Parts I and II).

~~CONFIDENTIAL~~

Military Cryptanalytics, Part V ~~(SECRET)~~. Cryptography and cryptanalysis of code and enciphered code systems. Solution of one-part and two-part code systems; repaginations; mixed-unit codes; literal and numerical superencryption systems. Additive and subtractive systems, involving normal and mod 10 arithmetic; use of difference tables; conversion square systems; literal superencryption systems; transposed code systems; indicator systems. Solution of enciphered code systems involving unknown codes and unknown encipherments; differencing and other techniques involved in reduction to a basic code; special solutions based on isologs and cryptographic errors; statistical methods and applications of analytical machines in enciphered code solution. (Prerequisites: Military Cryptanalytics, Parts I and II).

Military Cryptanalytics, Part VI ~~(SECRET)~~. Cryptography and cryptanalysis of cipher machines and encrypted transmission systems. Solution of representative literal machine ciphers; key generators; alphabet generators. Solution of literal machines of the Hagelin, Hebern and Enigma types; B-211 and other fractionating systems; indicator systems. Solution of typical cipher teleprinter systems; cryptanalytic approaches in the solution of cifax, ciphony, and civision systems. Typical applications of statistical methods and analytical machine techniques in the solution of literal and non-literal cryptomachines; special solutions based on isologs and cryptographic errors. (Prerequisites: Military Cryptanalytics, Parts I, II, and III).