USCIB: 29.11/13 ~~HANDLE VIA COMINT CHANNELS ONLY~~

1 February 1955

~~CONFIDENTIAL~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: [redacted]
Prospectuses of Cryptanalytic Training

Reference: USCIB 29.11/12, dated 3 January 1955.

1. In connection with the reference, NSA member of USCIBEC has prepared the enclosed prospectuses of cryptanalytic training courses, which are forwarded for vote sheet approval with a view to sending the approved version to LSIB.

2. In anticipation of a possible future requirement for a similar prospectus along T/A lines, the Director, NSA states, in his covering memorandum (enclosed), his willingness to prepare such a document if the members of USCIB so desire. It is requested that vote sheet replies, which should be returned by 11 February 1955, indicate also your desires in this regard.

3. It is requested that the Army member comment upon the releasability of D/A TM 32-220 mentioned in the enclosed memorandum by the NSA member of USCIBEC.

RUFUS L. TAYLOR
Captain, U. S. Navy
Executive Secretary, USCIB

Enclosure
NSA Serial 546 dtd 24 Jan 1955.

USCIB: 29.11/13 ~~HANDLE VIA COMINT CHANNELS ONLY~~

NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 546

25 JAN 1955

~~CONFIDENTIAL~~

MEMORANDUM FOR THE EXECUTIVE SECRETARY, USCIB

SUBJECT: Prospectuses of Cryptanalytic Training

Reference: USCIB 29.11/12, 3 Jan 55

1. The prospectuses mentioned in the reference have been completed and 40 copies of each are inclosed for distribution to the members of USCIB.

2. In order that a complete list of releasable training materials may be compiled and held in reserve to meet possible future requirements, the Director stands ready to prepare a similar prospectus for T/A training materials, should the Board so desire. Also, it is suggested that the Assistant Chief of Staff, G-2, D/A, be asked to comment on the releasability of DA TM 32-220, "Basic Cryptography," which could be used to provide some of the prerequisite information cited in connection with Inclosures 2 and 3.

(SIGNED)
D. M. AGNEW
Captain, US Navy
NSA Member, USCIBEC

3 Incls:
1. Prospectus of Course in Military Cryptanalytics, Part I
2. Prospectus of Elementary Course in Code Solution
3. Prospectus of the "GRAY" Problem

Enclosure with USCIB 29.11/13 dtd 1 Feb 1955.

~~CONFIDENTIAL~~
Modified Handling Authorized

PROSPECTUS OF
COURSE IN MILITARY CRYPTANALYTICS, PART I

Materials Furnished:

(1) NSA Text "Military Cryptanalytics, Part I" by William F. Friedman and Lambros D. Callimahos (December 1952). CONFIDENTIAL/ MODIFIED.

(2) NSA Problem Book "Course, Military Cryptanalytics, Part I" (May 1954). CONFIDENTIAL/ MODIFIED.

Scope of Course, indicating hours of study and practical application:

Lesson 1. Basic cryptologic definitions. Generalities of fundamental cryptanalytic operations. The frequency distribution and its uses. The monographic Φ (phi) test for determining monoalphabeticity. Collation of garbled intercepts. ... 16 hours of study and practical application.

Lesson 2. Cryptography and cryptanalysis of uniliteral (simple) substitution ciphers with standard and mixed cipher alphabets. Keyword recovery from mixed cipher alphabets ... 20 hours of study and practical application.

Lesson 3. Cryptography and cryptanalysis of simple multiliteral ciphers. Baconian and Trithemian systems. Elementary Baudot systems. ... 24 hours of study and practical application.

Lesson 4. Cryptography and cryptanalysis of multiliteral ciphers involving variants. Analysis involving the use of isologs ... 28 hours of study and practical application.

Lesson 5. Cryptography and cryptanalysis of four-square and two-square digraphic systems. The digraphic Φ (phi) test ... 32 hours of study and practical application.

Lesson 6. Cryptography and cryptanalysis of Playfair ciphers ... 24 hours of study and practical application.

~~CONFIDENTIAL~~
Modified Handling Authorized

Lesson 7. Cryptography and cryptanalysis of polygraphic systems involving large tables. ... 32 hours of study and practical application.

Lesson 8. Cryptography and cryptanalysis of monome-dinome systems and other systems with irregular-length cipher units. Analysis involving the use of isologs ... 60 hours of study and practical application.

Lesson 9. Cryptography and cryptanalysis of syllabary squares and code charts. Coordinate recovery; square recovery. Use of bulk messages. ... 40 hours of study and practical application.

Lesson 10. Cryptography and cryptanalysis of miscellaneous monoalphabetic substitution systems. Concealment systems ... 32 hours of study and practical application.

TOTAL -- 308 hours of study and practical application.

~~CONFIDENTIAL~~
Modified Handling Authorized

PROSPECTUS OF
COURSE IN MILITARY CRYPTANALYTICS, PART I

Materials Furnished:

(1) NSA Text "Military Cryptanalytics, Part I" by William F. Friedman and Lambros D. Callimahos (December 1952). CONFIDENTIAL/ MODIFIED.

(2) NSA Problem Book "Course, Military Cryptanalytics, Part I" (May 1954). CONFIDENTIAL/ MODIFIED.

Scope of Course, indicating hours of study and practical application:

Lesson 1. Basic cryptologic definitions. Generalities of fundamental cryptanalytic operations. The frequency distribution and its uses. The monographic Φ (phi) test for determining monoalphabeticity. Collation of garbled intercepts. ... 16 hours of study and practical application.

Lesson 2. Cryptography and cryptanalysis of uniliteral (simple) substitution ciphers with standard and mixed cipher alphabets. Keyword recovery from mixed cipher alphabets ... 20 hours of study and practical application.

Lesson 3. Cryptography and cryptanalysis of simple multiliteral ciphers. Baconian and Trithemian systems. Elementary Baudot systems. ... 24 hours of study and practical application.

Lesson 4. Cryptography and cryptanalysis of multiliteral ciphers involving variants. Analysis involving the use of isologs ... 28 hours of study and practical application.

Lesson 5. Cryptography and cryptanalysis of four-square and two-square digraphic systems. The digraphic Φ (phi) test ... 32 hours of study and practical application.

Lesson 6. Cryptography and cryptanalysis of Playfair ciphers ... 24 hours of study and practical application.

~~CONFIDENTIAL~~
Modified Handling Authorized

PROSPECTUS OF
ELEMENTARY COURSE IN CODE SOLUTION

**Material Furnished:** "An Elementary Course in Code Solution." National Security Agency (November 1954). CONFIDENTIAL/ MODIFIED.

**Assumed Knowledge:** No text accompanies this course. A prior familiarity with the cryptography of one-part codes and additive encipherment of numerical codes, with the frequently occurring Morse garbles, and with the use of a permutation table for the purpose of degarbling errors is assumed.

**Scope of Course, indicating hours of practical application:** The course consists of three problems to be solved. The scope of each and the time required for solution are as follows:

The AKOMPANI Problem. Initial entry into an unknown one-part code book through the recovery of encoded addresses and signatures; further reconstruction of the code book, capitalizing on its one-part feature and on the stereotyped passages in the message texts ... 24 hours of practical application.

The NABUCO Problem. Degarbling reception errors and clerical errors from the code texts, and recovering the meanings of several new groups. ... 12 hours of practical application.

The NIVELLE Problem. Assuming plain text in additive-enciphered code messages which involve for the most part code groups whose meanings have previously been recovered, and thereby recovering the additive key and the meanings of some new groups ... 8 hours of practical application.

TOTAL -- 44 hours of practical application.

~~CONFIDENTIAL~~
Modified Handling Authorized

PROSPECTUS OF
THE "GRAY" PROBLEM

**Materials Furnished:**

(1) "The GRAY Problem." National Security Agency (1 May 1953). CONFIDENTIAL/ MODIFIED.

(2) "Training Code No. 2 (GRAY)". National Security Agency (April 1948). UNCLASSIFIED.

(3) "Difference Tables for Training Code No. 2." National Security Agency (January 1948). UNCLASSIFIED.

**Assumed Knowledge:** No text accompanies this problem. A prior familiarity with the cryptography of additive encipherment of numerical codes and with the cryptanalytic technique of differencing code groups is assumed.

**Scope of Problem, indicating hours of practical application:** The GRAY Problem is a problem in the cryptanalysis of an additive-enciphered code system involving a known code book. Essentially the problem requires recovering the plain texts of the messages and reconstructing the additive page with its coordinates. ... 24 hours of practical application.