SECURITY CLASSIFICATION (If any)

DISPOSITION FORM

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

FILE NO.	SUBJECT Plans for Preparation of Cryptanalytic Textbooks

TO	FROM	DATE	COMMENT NO. 1
Mr. Friedman S/ASST	TWO	14 Feb 55 Dr. Jaffe, 60455/lrw	

1. On 12 January 1955 you participated in a conference to consider a plan for the development of a series of textbooks designed to serve as a basis for the training of cryptanalysts. You were informed that the first volume, dealing with the analysis of various elementary types of substitution systems and some basic notions of statistics, had been (except for final revision) completed. This volume is classified CONFIDENTIAL/Modified. You were also informed that the plan called for the preparation of five additional books, devoted respectively to:

a. Periodic polyalphabetic ciphers, elements of transposition solution, depth reading.

b. Aperiodic polyalphabetic substitution ciphers, cryptomathematics.

c. Transposition, combined substitution-transposition and fractionating systems.

d. Code and enciphered code systems.

e. Cipher machine and encrypted transmissions systems.

It was proposed that the second volume be classified CONFIDENTIAL/Modified, the third and fourth CONFIDENTIAL, and the last two SECRET.

2. The conferees agreed that it was not possible for them to evaluate the proposal fairly until they could see it in the context of the total Agency training plan.

3. The purpose of this D/F is twofold: first, to comply, insofar as possible at this time, with their request that the Training Division prepare such a plan; and second, to request the concurrence and/or comments of the addressees with the statements of principle and proposals for action. If the replies indicate that a second meeting is desirable, one can be held.

4. A completely formulated training plan for analysts would include a detailed plan for a progressive series of courses and job assignments. Such a program is desirable and should be developed on a scale larger than obtains now, but it is not yet possible to set it down.

5. However, whatever the nature of the training plan arrived at, such a plan will have to be based on certain general principles. These are:

a. That the successful development of analysts requires a combination of formal training and work experience.

SUBJECT: Plans for Preparation of Cryptanalytic Textbooks

b. That formal training can best be done through the medium of carefully planned courses, designed to further the ability of the student to cope with problems of ever greater variety and of increasing complexity.

c. That such courses should be based on text-books so designed that they will:

(1) Include a consideration of every general class of problem that is likely to be met in operations.

(2) Carry the student progressively from the simpler to the more complex ideas and processes.

(3) Supplement the instructions of a teacher.

Formal training now takes, and probably will continue to take, the following forms:

a. Training in Fundamentals.

b. Advanced General Training.

c. Advanced Special Training.

Textbooks and courses should, therefore, be designed for use at these levels.

6. The following tabulation sums up the requirement as now conceived:

a. Level I - Fundamentals.

Purpose: To acquaint students with cryptanalysis of elementary forms of substitution and transposition systems, and to equip them with the basic mathematical and statistical tools.

Materials Required: Textbooks (the present Crypt I and the projected Crypt II). Courses and problems. (The existing course based on Crypt I, plus other problems as required.)

Classification: CONFIDENTIAL/Modified.

Utilization: NSA School, NSA operational organizations, Service Schools, Reserve units, Extension courses. Other.

Preparation: Training Division.

b. Level II - Advanced General.

Purpose: To equip students to make contributions to the analysis

of problems likely to be encountered in operations. To acquaint them with a wide variety of problems and the best methods of attack.

Materials Required: Textbooks and courses, with associated problems. (Basis of expositions and problems may be either real or simulated situations, the choice to depend on pedagogical considerations.)

Classification: No upper limit. May be TOP SECRET Codeword.

Utilization: NSA operational organizations (or School if circumstances permit). Service field units.

Preparation: Training Division.

c. Level III - Advanced Special.

Purpose: To prepare students to work on the analysis of specific operational systems.

Materials Required: Descriptions of systems and discussion of methods of attack. Problems designed to illustrate procedures.

Classification: No upper limit. May be TOP SECRET Codeword.

Utilization: NSA operational organizations.

Preparation: Operational elements with Training Division collaboration as requested.

7. In view of the sentiments expressed by many of the conferees, Training Division has made the decision to devote the full efforts of Mr. Callimahos and Mr. Cefail to the final publication of Crypt I and the writing of Crypt II. This work will be done in an operational area at Arlington Hall Station so that the writers may have as close contact as possible with analysts working on operational problems.

8. It is contemplated that Mr. Callimahos will discuss with appropriate officials plans concerning the sequence and content of the other texts to be written. The decision as to the amount of effort to be devoted to these books will be made on the basis of these discussions.

9. If it is decided that more speed is required than can be guaranteed by the resources of the Training Division, operational components who have special requirements should give consideration to preparing the appropriate

SUBJECT: Plans for Preparation of Cryptanalytic Textbooks

formal training documents, which might later be considered for inclusion in textbooks.

SHELBY L. PATTERSON
Chief, Training Division