SECURITY CLASSIFICATION (If any)

DISPOSITION FORM

~~TOP SECRET~~

FILE NO.	SUBJECT	
	Lecture to be given to the ASA School at Carlisle, Pa., on Thursday, 22 June 1950	

TO	FROM	DATE	COMMENT NO. 1
AFSA-14 THRU: AFSA-02	AFSA-02A2	19 June 1950 F. B. Rowlett/383/jmw	

1. I propose to divide the two-hour lecture period into two parts as follows:

Part I: (approximate time--40 min.)
Subject: Functions of a modern COMINT organization with emphasis on cryptanalysis.

Part II: (approximate time--1 hour)
Subject: An actual example of advanced cryptanalysis--The Japanese diplomatic cipher machines.

The remaining twenty minutes will be devoted to a break and question periods.

C O P Y

2. An outline of the first part of the proposed lecture is appended hereto as Tab A. The classification of the subject matter is at most SECRET, and will depend upon the examples cited. A series of thirteen charts form the basis for this lecture, and they are explained by a running discussion. The discussion is from memory.

3a. The second part of the lecture deals with the historical cryptanalytic aspects of the Japanese Red and Purple machines up to the time of Pearl Harbor. No reference will be made to the post Pearl Harbor use of the Purple machine.

b. I propose to undertake a general discussion of the actual cryptanalytic principles involved in the solution of these machines and will present either photographs or original copies of work sheets as appropriate. I shall disclose the cryptographic principles of the machines and indicate the cryptanalytic attack which was actually successful on each machine.

c. The discussion will be from memory and I will use a blackboard to supplement the photographs and work sheets in explaining the cryptologic principles involved.

d. An outline of Part II of the lecture is appended as Tab B. The material to be presented was classified secret in 1941.

/s/ Frank B. Rowlett
FRANK B. ROWLETT
Technical Director
Office of Operations

COPY

NME FORM NO. 96

SECRET

TAB "A"

OUTLINE

Part I

A. The basic missions of AFSA are:

1. Communication Intelligence

2. Communication Security

3. Communication Research and Development

B. Definition of Intelligence Mission of AFSA

C. Statement of primary objectives of Communication Intelligence

D. Intelligence Requirements

1. Definition

2. Consumers

a. CIA

b. ONI

c. State Department

d. Air Force Intelligence Division

e. Army Intelligence Division

f. Federal Bureau of Investigation

3. Type

a. Long range

b. Current (monthly)

c. Spot

E. Intercept (touched on only in reference to crypt-analysis.

COPY

SECRET

F. Processing

1. Traffic Analysis

a. Objective of Traffic Analysis

b. Elements of Traffic Analysis

2. Cryptanalysis

a. Objectives of cryptanalysis

1. Determine strength and weakness of Cryptographic systems

2. Effective exploitation and solution of foreign cryptographic systems

3. Development of security precautions for U. S. systems

4. Production of communication intelligence

b. Elements of cryptanalysis

1. Diagnosis of internals

2. Techniques of attack

3. Key recovery

4. Production

3. Translation

a. Code recovery

b. Analysis and reporting of plain text

c. Translation of messages

4. Ancillary Services

a. Photographic laboratory

b. IBM-RAM

c. Collateral information

G. Summary and Questions

SECRET

TAB "B"

SUBJECT: Outline of lecture on advanced problem cryptanalysis using the Japanese Diplomatic Communications as an example.

Part II A

1. Introductory Remarks

2. Red Machine

   a. First appearance of Japanese cipher traffic noted in 1923.

   b. Discussion of external characteristics of messages.

3. First serious effort of solution in October 1936 established the following:

   a. Text definitely cipher

   b. Repititions

   c. Change, nature unidentified, took place on 1st, 11th, and 21st of each month.

   d. The basic keying element produced cycle which apparently was greater than the length of the longest message.

4. First message read.

   a. Message of December 21, 1933 of approximately 2,000 characters.

   b. Basic Vowel relation

   c. Analysis of December 1-10 traffic 1936.

   d. Determination of the "skips."

COPY

e. Recovery of sequence

Part II B

1. Purple Machine

2. New machine mentioned in Japanese traffic.

   a. Effective date.

   b. First message received.

3. Preliminary examination.

   a. "Six's" and "Twenty's"

   b. Recovery of "Six's"

   c. Nature of substitution

4. Attack on the "Twenty's"

   a. Partial decipherment of all traffic.

   b. Difficulties encountered

5. Absence of Repetition

   a. Non-repetitive phenomena

   b. Tentative conclusions

6. Recovery of "Twenty's"

   a. Discussion of homologs

   b. Reduction of 2 messages to the same base.

   c. Discovery of symmetric sequences

   d. First translations

7. Completion of solution

   a. Indicator study.

   b. Discussion of the machine

8. Special concluding remarks.

a. Interesting examples.

b. Cryptanalytic estimate of the problem.

SECRET

LIST OF PHOTOGRAPHS TO BE SHOWN IN

CONNECTION WITH PART II

1. Clipping from Washington Post, 8 December 1941 "Japanese emissaries set fire to papers in Embassy grounds."

2. Clipping Washington Daily News, 10 December 1941 "What was in Jap's Trunks?"

3. Japanese Red Machine Commutator Photograph of actual parts of original Japanese machine.

4. Second view of Japanese Red Machine Commutator (see 3 above)

5. Third view of Japanese Red Machine Commutator (see 3 above)

6. American built analog of Japanese Red Machine, view 1

7. View 2 of 6 above

8. View 3 of 6 above

9. Selector switch (Six's) from original Japanese Purple Machine (Picked up in Berlin)

10. Selector seitch (Twenty's) from original Japanese Purple Machine (Berlin)

11. Another view of switch (Twenty's) shown in 9 above.

12. Photograph of Plugboard of original Purple machine.

13. View of selector switch from original Purple machine showing wiring and index mechanism.

14. Another view of Switches of 11 above

15. American built Analog of Japanese Purple Machine (view 1)

16. View 2 of 15 above.

17. View 3 of 15 above showing details of cryptograph

COPY

SECRET

18. View 4 of 15 above showing wiring of selectors

19. View 5 of 15 above showing detail of Six's and Twenty's.