LECTURE IV

How I came to be a cryptanalyst. Riverbank - the unofficial Black Chamber. The School of Cryptography.

Colonel George Fabyan

Studying cryptology

U.S. had no organization for cryptanalysis

Navy had a very small group for making Navy codes and ciphers.

Army had nothing, not even what the Navy had.

Remember W.D. T.C. 1915???

When in April 1917 U.S. entered war, British soon told Military Intelligence Branch, War Department General Staff about insecurity of WD Telegraph Code. 1915 Implications!'

President Wilson's lack of confidence in State Department codes.

152 P. 143 of The Life and Letters of Woodrow Wilson, Vol. 6, Showing plain text of message from Wilson to House, in Wilson's handwriting

152.1 P. 144 of the book. Message encoded by Mrs. Woodrow Wilson.

152.2 Message as finally sent by the State Department.

153
P. 316 of Woodrow Wilson's "Life and Letters", Vol 5, showing shorthand notes made by Wilson for a telegram to Colonel House.

153.1
P. 317 of above showing President Wilson's transcription of the above message into code, done on his own typewriter.

153 2
Transcription into plain language on receipt.

212
Title page of Manual for the Solution of Military Ciphers by Parker Hitt, 1916 (Things we studied.)

160
Parker Hitt.

213.
Title page of An Advanced Problem in Cryptography and its Solution by Mauborgne. 1914.

159.
J. O. Mauborgne. Became Chief Signal Officer.

We study. We solve messages for State, War, Navy and Justice. We teach crypt and run classes. We learn Bacon's Biliteral--the earliest binary code.

79
Bacon's "biliterarie alphabet"

81
Example: The Castle.

Many years later (15-16), being desirous of giving a picturesque example of bilateral cipher in one of my texts but thinking the picture of a phoney castle would not be acceptable to the authorities in the OCSigO, I put in an example and challenge students to solve it.

1. Building up Riverbank crypt organization, 1916-1917.

2. What sort of messages did Riverbank solve? Mexican principally -- messages obtained surreptitiously by D/J.

No facilities for intercept of radio.

No arrangements with Western Union or Postal for copies of messages of belligerents in Europe.

Ciphers of Hindu conspiracy.

33.1 One of the ciphers used by the Hindu conspirators - 1916-17.

34 Solution of the Hindu letter.

34.1 Another Hindu system.

Trial in Chicago.

How trial in San Francisco wound up!

In due course, MID builds an organization in Washington around 1st Lt. Yardley. In summer 1917 Riverbank is cut out for security reasons and for schooling of officers.

Will have something to say about H.O.Y. later.

133
The entire officer staff of MI-8.

Some of the things MI-8 worked on (with British help): Postal censorship, 26
concealment systems, secret ink message on music sheet, German spy (Courteney de Rysbach) sentenced to life.

27
Phoney music.

26.1
Open code "Concealment" (every 4th word)
26.2
The message.

27.5
Another example - every 6th word in lines with even number of words.
27.6
Heavy letters --passed by German censor.

3Ø-32
Sabotage messages.

Spies and secret agents.

127
Secret ink writing in the Black Tom and Kingsland Fire disasters.

25 and 25.1
Waberski.

82
Riverbank continues to work on Mexican messages but it tapers off. But instructional courses go on. One of the classes of student officers at the Riverbank School of Cryptography, 1917-18.

Section 2 begins

I am commissioned and go directly to France.

156
Colonel Moorman.

11
Cipher system used by the Russians in World War I (from a book by the Austrian cryptologist, Andreas Figl). (Misuse of this cryptographic system (or failure to use) cost the Russians the defeat at Tannenberg! Importance of that defeat.

Russo-Finnish War 1940.

12
French Army.

13
Italian Army.

14
The German ADFGVX cipher system, used by the German High Command during World War I. (First new system used by them. Invented by putting together two well-known steps.)

23

The PLAYFAIR Cipher. This cipher was used by the British and Americans, and was thought to be 'hot stuff' in 1914. Solution was described in Mauborgne's "An advanced problem in cryptography".

Cipher allegedly invented by Playfair, but he did not do it -- rather Wheatstone. Wheatstone is credited with having invented the electrical bridge, but he did not do it -- rather Christy.

Double transposition.

Code systems of WWI.

16

An example of a commercial code. Call attention to 2-letter difference. All kinds, suited and specially constructed for general or specific businesses and industries, such as leather, steel, automotive, shipping, etc.

18

A highly specialized "commercial code" Call attention to 3-letter difference:

YGATA -	COMA
YGKRO -	DELIRIUM TREMENS
YGCIB -	CONSTIPATION
YGMAN -	DIARRHEA

17

Chinese code.

19-22

Tactical codes in WWI. Prior to World War I and, in fact, for the first two years of World War I code was thought to be impractical for military field or

tactical use. But the Germans began to use code late in 1916, and the Allies followed suit Question of reproduction then as it is today.

Field codes in WW I - will show only one example in slides --the German type of KRUSA code Exhibits can be examined later.

20

One of the German Army Field Codes, World War I.

KRU	676 x 3	1928	(1)
KRUS		676	
KRUSA		2604	(2)
		676	
		3280	(3)

19

French Army Code.

22

British Army Field Code, World War I.

21

An early AEF Code in World War I. An indication of how poorly prepared we were for COMSEC.

24

American Army Code. River series - First Army, Lake series - Second Army.

Cryptanalytic work in World War I. American successes in cryptanalytic work in the AEF, World War I, were not remarkable because of circumstances. We were working on traffic from "quiet sectors" -- hence had little but practice,

and that was largely in 2-part codes. Fair success with cipher because traffic from all sources and collaboration with French and British. Best results were in connection with lower echelon 3-number codes, often tactically useful information was obtained after the introduction of the 3-number code.

14.1 "Special Code Section Report" by G-2, A-6, GHQ, AEF 20 Nov 1918. A crypt "bulletin" from the ADFGVX cipher. This forms a good example of Special Intelligence in World War I.

15. One of the earliest examples of traffic analysis and traffic intelligence - based on study of traffic in ADFGVX messages.

On traffic analysis. "The problem of the extent to which traffic analysis can be regarded as a reliable source of intelligence is an extremely tricky one. I feel that it will always have its limitations, that the 'first impressions' which it gives may often be wrong, that it must rely heavily on later confirmation from cryptanalysis or collateral, and that in particular it is regrettably vulnerable to deception activity by an enemy." - Travis in letter to Wenger 5 Jan 51

Return to U.S. after final report and am demobilized. Return to Riverbank and write brochure. Trying for Regular Army at G. Fabyan's insistence. Joining CSO, 1921, January 1.

U S. COMINT activities in 1920-29.

1. Navy had RPS but small. COMINT just in infancy. All work under Naval Communications. No official relations between Army and Navy.

2. Army -- cryptologic work under much divided authority:

Signal Corps, G-2, and AG with MI having over-all responsibility for security.

3 WFF came to OCSigO on 1 January 1920

4. H.O.Y. in New York. No relations ABC with OCSigO, AB AB solved J messages in 1922 Disarmamant Conference 5-5-3 ration.

5. Albright studies situation.

6 Closing of ABC - STIMSON.

7 SIS formally established on paper in April 1929 by transfer of solution activity to OCSigO and little later transfer of AG duties to OCSigO also - thus integrating all work under one head. But G-2 retained over-all responsibility.

8. Publication of Yardley book and effects.

I begin compilation, revision of codes and ciphers. Study cryptanalysis. Put out some brochures.

166
The first official text. W D. Training Pamphlet No. 3. Elements of Cryptanalysis. TICOM souvenir.

161
Major Owen S. Albright. Reorganization of C & C work.

149
SIS Staff - 1935.