SCAMP 1958

LECTURE IV - 30 June

Section 1 & 2

Discussion of the Zimmerman Telegram

LECTURE NOTE

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 cryptanalyses

(R6) Navy had a very small group for making Navy codes + ciphers

Army had nothing, not even what Navy had

Remember WDTC 1915??
When in April 1917 U.S
entered war, British soon
told Mil. Int Br., War Dept
General Staff about insecurity
of WDTel Code 1915
Implications!!
President Wilson's lack of confidence in
State Dept codes.

152

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

P 144 of the book ~~FE~~ 152.1

Message encoded by Mrs. Woodward Wilson

" as finally sent by 1522
State Dept

153

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

~~Encoded message~~

153.1

P 317 of above showing Prsident Wilson's transcription of the above message into code, done on her own typewriter

Transcription into pl. on receipt 153.2

212

Title page of Manual for the Solution of military ciphers by Parker/Hitt, 1916

(Things we studied)

REF ID:A38404

160

Parker Hitt

213

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

— —

159

J O Mauborgne

Became C.S.O.

We study
We solve msgs for State War Navy Justice
We teach crypt + run classes
We learn Bacon's Bilateral - the earliest binary code

79

Bacon's "biliteraré alphabet"

Put 231 in proper sequence
Lovell ltr to Wash

Example : The Castle

82.1

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

1) Building up R. crypt organization 1916-17
2) What sort of messages did Riverbank solve?

Mexican principally - msgs obtained surreptitiously by D/J.
No facilities for intercept of radio
No arrangements with W.U. or Postal for copies of msgs of belligerents in Europe
Ciphers of Hindu Conspiracy

Put in here:

79

80 —

81

82 Class of students

~~82-1 — Modern style in one of my texts~~

LECTURE NOTE FOR SLIDE 33.1

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

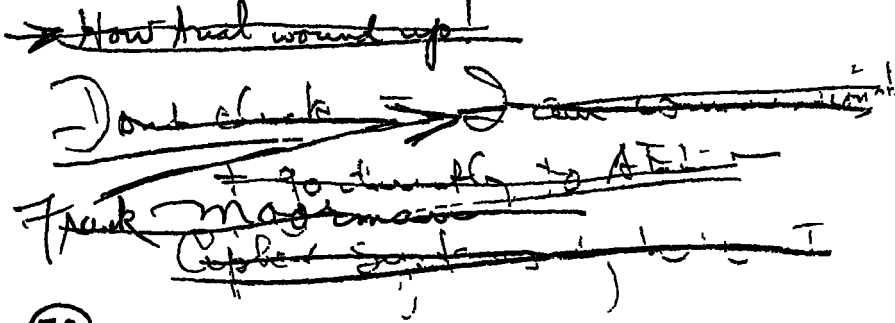
(29)

REF ID:A38404

LECTURE NOTE

FOR SLIDE 34

Solution of the Hindu letter



(30)

1) Another Hunden System 341
2) Trial in Chicago
3) How trial in S.F wound up 1

155

In due course, MID builds an organization in Washington around in summer 1917
1st Lt. Yardley at R is cut out for security ~~Work~~ + for schooling of officers
Will have something to say about HOY later.

The entire officer staff of MI-8

Some of the things MI-8 worked on (with BR help)

Postal censorship: Concealment systems

Secret ink message on music sheet — 26.

Germany spy (Edouard de Rydbeck) sentenced to life

Phoney music — 27

Open code "Concealment (every 4th word) — 26.1

The message — 26.2

Another cypher - every 6th word in lines — 27.5

" with even number of words — 27.6

"Heavy" letters — passed by German censor

1) Sabotage messages 30-32

2) Spies, & secret agents ~~Censorship~~

~~3) Waberski~~ 25 & 251

~~4) Postal Censorship~~ next card ~~252, 250~~

~~(265) German spy sentenced to life~~ ~~(26)~~ 26, 262, 264

127

Secret ink writing in the Black Tom & Kingsland fire disasters

Walerski

25

25.1

82

Riverbank continues to work on Mexican mogea but it tapers off But instructional courses go on.

REF ID:A38404

LECTURE NOTE FOR SLIDE 82

One of the classes of student officers at the Riverbank School of Cryptography, 1917-18.

(28)

SCAMP 1958

LECTURE IV – 30 June

Section 2

REF ID:A38404

30 June 5.

IV

I am commissioned and go
directly to France

156

Col Moorman

LECTURE FOR SLIDE 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

(32)

REF ID:A38404

12

French Army

Italian Army

LECTURE FOR SLIDE 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./

(38)

LECTURE FOR SLIDE 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./

(35)

Double Transposition

REF ID:A38404

Code Systems of WWI

Z note

Codes & ciphers in use by belligerents

Will show also 1 or 2 Russian & German cipher systems

Later something about code systems

LECTURE FOR SLIDE 16

An example of a commerical 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./

LECTURE FOR SLIDE 18

A highly specialized "commerical code"

/Call attention to 3-letter difference:

YGATA - COMA
YGKRO - DELIRIUM TREMENS

YGCIB - CONSTIPATION
YGMAN - DIARRHEA

17

Chinese Code

German Army High Cmd 14

ADFGVX

Codes

LECTURE NOTE FOR SLIDES 19-22

Tactical codes in WW I

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.

LECTURE

FOR SLIDE 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)

Exhibits of old Frame with me

(43)

French Army Code 19

-

British Army Field Code, 22
World War I

Don't click. Read next card first.

LECTURE FOR SLIDE 21

An early AEF Code in World War I

[An indication of how poorly prepared we were for COMSEC]

(44)

24

American Army Code

River Series – First Army

Lake Series – Second "

REF ID:A38404

LECTURE NOTE -- Cryptanaltyic work in World War I

*American successes in cryptanaltyic 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 ciphers 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.

(45)

LECTURE FOR SLIDE 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.]

Stop! Don't click!
Tell about code book, next card

(96)

LECTURE NOTE FOR SLIDE 15

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

LECTURE NOTE 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 cryptanlysis or collateral, and that in particular it is regrettably vulnerable to deception activity by an enemy."

-Travis in letter to Wenger 5 Jan 51

REF ID:A38404

Return to U.S. after
final report + am demobilized
Return to Riverbank + write brochure
Trying for Regular Army at G. Fabyan's assistance
Journey CSO 1921, Jan 1

American & British

23

LECTURE NOTE 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 Jan 1920. - Studies

4. HOT in New York. No relations ABC with OCSig O, AB. AB solved J messages in 1922 Disarmament Conf. 5-5-3 ratio.

5. Albright studies situation.

6. Closing of ABC - STIMSON

→ [OVER]

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 B-2 retained overall responsibility.

8. Publication of Yardley book and effects.

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

~~I return to U.S. & am demobilized~~

~~I " " Riverbank~~

~~I " " Govt Service 1 Jan 1921 for six months!~~

~~I organize Code Comp work~~

~~Albright & reorg. of CAC work~~

~~Yardley & NBC effort of~~

~~Studies 1930-35~~

The First Offered text
WD Trng Pamphlet No 3

166

Elements of cryptanalysis

TICOM Souvenir

161

Major Owen S. Albright
Reorganization of C+C work

--

149

SIS Staff 1935