SCAMP 1958

LECTURE IV - 30 June

Section 1 & 2

Discussion of the
Zimmermann Telegram

LECTURE NOTE

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

Colonel George Fabyan

Studying cryptology

US had no organisation for cryptanalysis

(26) Navy had a very small group for making
Navy codes + cyphers
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 WD Tel Code 1915
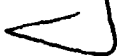
Implications !!

President Wilson's lack of confidence in State Dept Codes.

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

P144 of the book ~~I~~

152.1

Message encoded by Mrs. Woodward Nelson

" as finally sent by
State Dept

1522

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~~

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

Transcription into plain 153,2
on receipt

i

Title page of <u>Manual for the Solution</u> 212
<u>of military ciphers</u> by Parker Hitt, 1916

(Things we studied)

Parker Hitt

213

Title Page of <u>An Advanced Problem in</u>
<u>Cryptography and its solution by</u>
Mauborgne. 1914

— —

J O Mauborgne

Became C.S.O.

We study
We solve msges for State
War
Navy
Justice
We Teach crypt + run classes
We learn Bacon's Biliteral — the
earliest binary code

79

Bacon's "biliterarie alphabet"

Put 231 in proper sequence
Lovell ltr to Wash

81

Example : The Castle

82.1

~~Many~~ years later (15-16) ~~not~~
being ~~desirous~~ of giving a picturesque example of
bilateral ~~Jigsaw~~ in one my ~~texts~~ phoney but thinking
picture of a 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

REF ID:A38404

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 WU or Postal for
    copies of msges of belligerents in Europe
Cyphers of Hindu Conspiracy

———————

Put in here:

79
80 —
81
82. Class of students
82.1 — Modern style in ~~code of any texts~~

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

.

(29)

LECTURE NOTE

Solution of the Hindu letter

(30)

1) Another Hinder 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 1st Lt. Yardley *in summer 1917* + R is cut out for security reas + for schooling of officers ~~Hartly~~

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 : <u>Concealment systems</u> 26.

Secret ink message on ~~music sheet~~

Germany Spy (Courtenay de Rysbach)

sentenced to life

Phoney music   27

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

The message } 26 2

Another exple — every 6th word in lines   27.5

with even number of words — 27.6

"Heavy" letters — passed by German Censor — 27.6

1) Sabotage messages   30-32

2) Spies, _{& secret agents,} Censorship

3) ~~Nalleski~~   25+251

4) ~~Radio censorship~~ next card ~~25,2~~

~~26) German spy sentenced to life~~ ~~26, 262~~ 64

Secret ink writing in the Black
Tom & Kingland fire disasters

127

Waberski

25

25.1

82

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

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

(28)

SCAMP 1958

LECTURE IV — 30 June

Section 2

------

30 June 5-

Enclosure $\underline{IV}$

I am commissioned and go
direitly to France

Col Moorman

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)

French Army

Italian Army

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)

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

Code Systems of WWI

I note

Codes & ciphers in use by
belligerents

Will show only 1 or 2 Russian & German
cipher system

Later something about code systems

An example of a commerical code

$\underline{/}$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.$\underline{/}$

(39)

————— ——— —

<u>LECTURE</u>   <u>FOR SLIDE 18</u>

A highly specialized "commerical code"

/Call attention to 3-letter difference:

      YGATA - COMA
      YGKRO - DELIRIUM TREMENS

      YGCIB - CONSTIPATION
      YGMAN - DIARRHEA

41

17

Chinese Code

German Army High Comd

ADFGVX

14

Codes

LECTURE NOTE

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.

(42)

LECTURE

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 all these with me

(43)

French Army Code

19

British Army Field Code,
World War I

22

Don't click. Read next
card. first.

An early AEF Code in World War I

⟨An indication of how poorly prepared we were for
COMSEC⟩

㊹

American Army Code   24
River Series — First Army
Lake Series — Second "

LECTURE NOTE -- Cryptanaltyic work in World War I

⨍American successes in cryptanaltyic work in the AEF,
World War I, were not remarkable because of circum-
stances. 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 con-
nection with lower echelon 3-number codes, often
tactically useful information was obtained after the
introduction of the 3-number code.

(45)

FOR SLIDE 14.1

"Special Code Section Report" by G-2, A-6, GHQ,AEF
20 Nov 1918.

ΓA crypt "bulletin" from the ADFGVX cipher. This
forms a good example of Special Intelligence in
World War I./

Stop! Don't check!
Tell about cc last, i
next card

46

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

(47)

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 impres-
 sions' which it gives may often be wrong, that it
 must rely heavily on later confirmation from crypt-
 anlysis 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 + am demobilized
Return to Riverbank + write brochure

Trying for Regular Army   at G. Fabyan's insistence
Joining CSO 1921, Jan 1

American & British

Playfair

23

LECTURE NOTE   U.S. COMINT activities in 1920-29

    1. Navy had RPS but small. COMINT just in infan-
cy. 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. HOY 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
  "   " Riverbank
  "   " Gov't Service 1 Jan 1921
                          for six months!
organize Code Compi work
Altho... ... of CAC work
... X ABC = effort of
Studies 1930 - 35

The *First* offered text
WD Tng Pamphlet N° 3

Elements of cryptanalysis

166

Ticom Souvenir

161

Major Owen S. Albright

Reorganization of C+C work

SIS Staff 1935