#6
✓ 64 cards ✓

63

① Extras

REF ID:A62875

Sequence for DC-E Dir talks Air Univ

PART I

(30 slides)

SLIDES

151✓
242✓
~~3~~
6.21✓
243✓
244✓
232✓
232.1✓

6.4✓
6.5✓
6.6✓
231✓
~~8~~
7✓
9✓
28✓
29✓

82✓
33✓
34✓
11✓
23✓
14✓
16✓
18✓
19✓
20✓
21✓
22✓

14.1✓
233✓
155✓

(1)

REF ID: A62875

Part I
Section 1

SLIDES

4.5 ✓
45.4 ✓
47 ✓
48 ✓
49 ✓
49.1 ✓
49.4 ✓
50.4 ✓
50.2 ✓
50 ✓
50.12 ✓
54 ✓
55 ✓
58.1 ✓
59 ✓
65 ✓
54 ✓

Sequence of Slides for C-E Dir Air University talks

(2)

REF ID:A62875

PART II

Section 2

SLIDES

172 — 71 ✓
71.1 ✓
72 ✓
172.10 ✓
170 ✓
170.9 ✓
173 ✓
174 ✓
56 ✓

258 ✓
60 ✓
180 ✓
171 ✓
164 ✓
70.1 ✓
70.3 ✓
74.2 ✓
230 ✓

PART III

Cryptanalysis
Traffic Analysis

REF ID:A62875

PART III

SLIDES

245 ✓
Plumb 6.10 ✓
15 ✓
238 ✓
254 ✓
255 ✓
256 ✓
131 ✓
134 ✓
141 ✓
145 ✓
139 ✓
138 ✓
143 ✓
250 ✓
251 ✓
150 ✓
150.1 ✓

Cards applicable to the lectures given before the (fully crypto-cleared) [redacted] on the Communications-Electronics Division of the U.S. Air Force Air University at Maxwell Air Force Base, Montgomery, Alabama on (1) 4 Sept 1952 (2) 11 March 1953, (3) 26 August 1953, and 31 March 1954. The lectures were in a series of three periods of 50 minutes each. I had students which were of much interest to the audience after the talks.

J

"The Influence of Cryptologic Power on History."

REE ID: A62875

I have in mind a subtitle, too. It is "Or, on the one hand, how to win campaigns and go down in history as a great strategist and leader of men; or, on the other hand, how to lose campaigns and go down in history as a numbskull and incompetent commander."

For my talk this morning I've chosen from my series one entitled "How to make the most of a cryptologic opportunity."

My talk today is one of a series with the overall title REF ID:A62875 of C-Power on History."

Now before my many Navy friends here jump up to yell "Yeah! Mahan!" I hasten to explain that the "C-Power" I'm going to to talk about is not the same sort of power Admiral Mahan wrote about in his famous book The Influence of Sea Power on History. The C in my title stands for the word CRYPTOLOGIC, so that the real title of the series I'm preparing is

—over.

P.79 of Majority Report 20 July 46:

Intelligence available in Washington "Magic"

"With the exercise of the greatest ingenuity and utmost resourcefulness, regarded by the committee as meriting the highest commendation, the War and Navy Departments collaborated in breaking the Japanese diplomatic codes. Through the exploitation of intercepted and decoded messages between Japan and her diplomatic establishment the so-called Magic, a wealth of intelligence concerning the purposes of the Japanese was available in Washington."

and again, on p. 232: Communications intelligence

..."all witnesses familiar with ~~Magic~~ material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

(2) General Chamberlin's statement (over)

Chamberlin was [redacted] throughout war. He said:
"The information G-2 gave G-3 in the Pacific Theater alone saved so many thousands of lives and shortened the war by no less than two years".
Hardly need say what Ultra alone was worth in billions of dollars. Cost in comparison is negligible. $1 m into COMINT = $1000 m of defense.

5. What is this "Magic"? Origin of term. We didn't call the machine that. TIME was wrong in that respect.
The British first used. Our "Magic Summary"
"Magic" -cover name for product of COMINT operations
6. Handbook for magicians: 1st gives "The Effect" 2nd: How produced -the method. I won't be able to give much re methods today but can give background and some effects.
7. Before proceeding, must say few words of caution required by security considerations. Hardly need stress necessity for secrecy re CI work and results. Hope of future success depends to very great degree on maintaining secrecy with respect to past achievements. Changes easy to make and hard for COMINT

(3)

(over)

people to follow. Effects of compromise or leakage widespread because of wide or world-wide use of cryptosystems. During WW II continuance of success often hung by very slender thread. OSS in Lisbon
Examples: J red, MIDWAY* (next card) (and P.H. investigation. Yardley's A B C. Read Time p.21
Public #513 - Everybody must be careful. As for me, haven't ever been in jug and don't think would like it.

8. Also hardly need give definition of COMINT but make sure we all understand: COMINT is information produced by an agency engaged in studying radio transmissions and other communications of a foreign country. Divided into:

1) Special intelligence
2) T/I
3) Special Weather "

* Most disastrous one of war. Early June 42 right after battle. Winchell & Chicago Tribune. Japs change everything.

These are naturally [illegible] producing complete answers.

School instructors have no doubt given adequate definitions so will simply cite three main objectives of COMINT:

A. Provide authentic information for planners and policy makers to apprise them of the realities of the international situation, of the war-making capabilities and vulnerabilities of foreign countries, and of the intentions of those countries with respect to war.

Read Bradley

B. To eliminate the element of surprise from an act of aggression by another country.

C. To provide unique information essential to the successful prosecution of war and vital to a shortening of the period of hostilities.

(4)

Chamberlain's statement: (It was for MacArthur):

"The information [-2 gave [-] in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years."

Hardly need to say what latter alone was worth in billions of dollars. Cost negligible in comparison.

9. Background of SI which is based upon science of cryptanalysis forms very interesting history -- inextricably bound up with history of cryptography. The two are but opposite faces of the same coin. Progress in one inevitably leads to progress in the other -- and so, too, in re retrogression.

LECTURE REF ID:A62875 FOR SLIDE 6.21

The syllabary used by Thomas Jefferson (Extract from decoding section)

/That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -- as will be discussed later./

LECTURE NOTE REF ID:A62875 9

10
10.1
10.2

Federal Army Route Cipher

Don't click — tell content of next 3 cards

(17)

214

LECTURE NOTE

REF ID:A62875

War Department Code in Spanish-American War --
the code of 1885 plus additive -777

(21)

LECTURE NOTE REF ID:A6287 FOR SLIDE 157

Colonel George Fabyan

How I came to be a cryptologist -- Riverbank Laboratori
Departments of Genetics, Ciphers, Acoustics

World War I in progress since 1914. U.S. position.
Fabyan's foresight - U.S. had no cryptologic bureau.
Contact with Government Departments. School for
training.

(27)

LECTURE NOTE

REF ID:A62875

I am commissioned and go directly to AEF

(31)

LECTURE NOTE REF ID:A62875 FOR SLIDE 12

Transposition cipher system used by the French Army in World War I. Copied from a German book on cryptography (Figl)-and correct.

(33)

REF ID:A62875

LECTURE NOTE FOR SLIDE 13

Cipher system used by the Italian Army in World War I. A simple numerical equivalent of the Vigenere table and system.

(34)

LECTURE FOR SLIDE 159

REF ID:A62875

Major General J.O. Mauborgne

1. As Major in 1920 head of Research and Engineering Division of OCSigO, gave real impetus to R&D in crypto graphic field.
2. His contact with Riverbank brings knowledge of Hitt's device and he got some ideas as to alphabets and form.
3. He has some test messages set up in his alphabets

(36)

LECTURE NOTE REF ID:A62875 SLIDE ~~213~~

[Renaissance of U. S. A. interest.] omit

Mauborgne's pamphlet on solution of Playfair cipher system.

(37)

LECTURE REF ID:A62875 FOR SLIDE 16

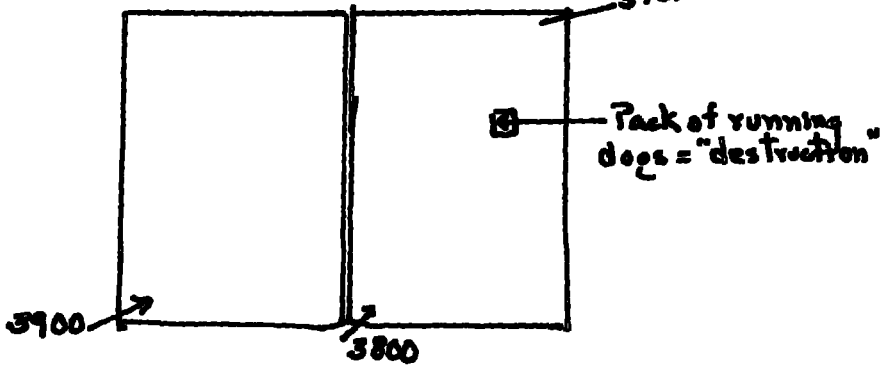
An example of a commercial code

/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./

LECTURE

FOR SLIDE 17

Chinese official telegraphic code



LECTURE REF ID:A628705 SLIDE 18

A highly specialized "commercial code"

Call attention to 3-letter difference:

YGATA - COMA
YGKRO - DELIRIUM TREMENS

YGCIB - CONSTIPATION
YGMAN - DIARRHEA

LECTURE REF ID:A628675 FOR SLIDE 133

Back in Washington - MI-8 was working.

Officers of M.I.-8 in World War I

/Point out Manly who solved the Waberski telegram. Practically all professors at universities-- shows that ideas as to caliber of intellect required were good and recognition of fact that no poot from which to draw trained personnel because there is no civilian occupational specialty of the same nature./

(48)

LECTURE NOTE REF ID:A62875 FOR SLIDE 155

Herbert O. Yardley as First Lieutenant, 1919

[Effect of disclosures?]

49

LECTURE NOTE REF ID:A62875 SLIDE 25.1

The Waberski message.

Here is the deciphered German text, and this is what it said: "To the Imperial Consular officials of the Republic of Mexico. Strictly secret! The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German agent." And so forth. The Court sentenced him to be shot; President Wilson commuted the sentence to life imprisonment; and he was out of the pokey after only one year!"

(50)

LECTURE NOTE FOR SLIDE 38

The Oil Scandal investigation.

Where $68,000 got.s tr. anaformed w'u 60v8 cows

53

LECTURE REF ID:A62875 FOR SLIDE 44.1

A cryptogram sent to President Roosevelt

"NDOIMDEYLOAUEETVIEBR?

Or else you die!!"

Did you ever bite a lemon?

LECTURE REF ID:A62875 FOR SLIDE 45

The earliest picture of a cipher disk, from Alberti Trattati in cifra, Rome, c. 1470.

"Oldest tract on cryptography the world now possesses"

(57)

LECTURE NOTE REF ID:A62875 FOR SLIDE 45.4

The Alberti Disk reincarnated in the U.S. Army Cipher Disk of 1914-18.

58

LECTURE REF ID:A62825 SLIDE 47

The cipher disk as again patented in 1924 -- Huntington Patent

/Shows that the Patent Office does not have general information on cryptography because of the secrecy involved./

59

LECTURE REF ID:A62875 FOR SLIDE 48

Original Wheatstone cipher device (invented and described in 1879).

/First improvement on the Alberti disk./

(60)

LECTURE REF ID:A62875 FOR SLIDE 49.1

The Decius Wadsworth cipher device (invented and built in 1817 when Colonel Decius Wadsworth was Chief of Ordnance.)

(62)

LECTURE REF ID:A62875 SLIDE 49.4

The Bazeries cryptographe cylindrique (1901) as shown in his book "Les chiffres secrets devoiles"

/But he may have described this in his article "Cryptograph a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891./

(63)

LECTURE NOTE REF ID:A628675 FOR SLIDE 50

Second page of Jefferson's description of "The 'Wheel Cipher"

64

LECTURE NOTE REF ID:A628763 FOR SLIDE 160

Renaissance of interest in U.S.A.

Colonel Parker Hitt

But despite his knowledge —
WDTC 1915 —

65

LECTURE NOTE REF ID:A62875 FOR SLIDE 50.8

U.S. Army Strip Cipher Device M-138.

(69)

LECTURE REF ID:A628[illegible] FOR SLIDE 50.12

U.S. Army cipher device, Type M-138-A (with Russian legends)

/Story of Russian legends and how they came to be there./

(79)

The Kryha cipher machine

(72)

REF ID:A62875 59

Swedish machine connected to electric typewriter

(76)

LECTURE , REF ID:A62877 FOR SLIDE 65

The keyboard electrically-operated B-211 Swedish machine

/Self-contained, instead of separate typewriter./

(44)

LECTURE REF ID:A62875 FOR SLIDE 71.1

The first Hebern machine

/Manufactured for use by the Ku Klux Klan/

(79)

LECTURE REF ID:A62875 FOR SLIDE 72

The 5-rotor Hebern machine

/Story of solution/

(80)

W.F.F.'s "work-sheet" solution of Navy challenge messages.

(81)

LECTURE NOTE REF ID:A62875 SLIDE 172.10

One of Hebern's developments for the Navy, after his release.

/This is the one that wouldn't work - but Hebern said the contract didn't specifically state that it had to work. He insisted on being paid -- and was!/

(One Navy file insisted that Navy had an admiral in Navy District HQ in S. F. just to keep Hebern out of jail so he could finish Navy contract!)

(82)

REF ID:A62875 170

U. S. Army Converter M-134-T1

Basic principle - external keying element

84

REF ID:A62875 170.4

U.S. Army Converter M-134-T2 (1936)

(85)

The SIGABA/ECM
(Converter M-134-C)

A+N get together. Benefits thereof
Withheld from all Allies

87

LECTURE NOTE REF ID:A62875 FOR SLIDE 56

With growth of teletype communications the need for and practicability of automatic encipherment became obvious.

-- The first attempt -- the machine developed by the AT&T Co. (1918) in collaboration with the Signal Corps.

(88)

REF ID:A62875 64

The IT&T Co. Teletype cipher attachment

(Internal mechanism exposed)

Solution story

Effects of lack of contact with work

Lesson re flying pay

(91)

LECTURE NOTE

FOR SLIDE 178

In 1942 the need for automatic teletype encipherment was met on the basis of expediency: the old AT&T Co. double-tape system was adopted and installed on a "crash" program at the few signal centers, while a large program for the production and procurement of Converter M-228 (SIGCUM) was being executed.

LECTURE REF ID:A62875 FOR SLIDE 171

M-161: Signal Corps model made at Fort Monmouth

(Efforts to develop field machine)

REF ID:A62875 70.1

Converter M-209

(94)

LECTURE NOTE REF ID:A62875 70.2

Converter M-209 with keying mechanism exposed.

(98)

LECTURE NOTE REF ID:A62875 FOR SLIDE 131

Cryptanalysis of modern systems has been facilitated by the invention, development, and application of special cryptanalytic aids by way of machines. The nature of the problem - not merely the number of permutations and combinations but the type is more improtant -- question of testing out multiplicity of assumptions and hypotheses, commonly by statistical methods.

High-speed testing is secret!

Earliest cryptanalytic devices at Riverbank Laboratories.

(106)

LECTURE REF ID:A628[illegible] SLIDE 131

The Riverbank "Polyalphabet" -- the first cryptanalytic aid.

My use of AT&T machines to compile DFC's (1921-22)

(107)

REF ID:A62875 SLIDE 134

My memo begging for one set of IBM, dated 30 Oct 1934.

(108)

The IBM contract, dated 12 Nov 1934!

Just one half month later - a remarkable record.
The memo must have been pretty potent medicine!

One wing of IBM installation in WW II

(110)

An analog.

(This was for JAS system (Jap MilAtt)

The Analog for Jap "Green"

(113)

A "brute force" machine

(114)

Machine for matching messages.

(115)

LECTURE NOTE REF ID:A62875 140

The "Camel"

(116)

The "Auto-scritcher"

/Rodin - the "Thinker"/

(118)