SCAMP 1958

LECTURE II - 25 June

Section 1 - 1415 - 1510 - 55 min

Typed.

Approved for Release by NSA on 09-19-2013 pursuant to E.O. 13526

No slide

Next great landmark in [cryptanalytic] history of decipherment is the solution of Egyptian Hieroglyphs ~~Solution of~~

~~Champollion — 1821~~

Norbert Wiener's characterization (in Cybernetics, I believe)

Athanasius Kircher delays solution for decades!

Problem not crypt primarily — one of linguistics, of grammar, & recovery of dead lan

4.1

The Rosetta Stone

Found in 1799 at Rashîd or, as the Europeans call it, Rosetta, city N Egypt on the west bank of Rosetta branch of the Nile.

Napoleons Army - Colonel Boussard (or Bouchard)
[1769-1821]
Became General + was alive in 1814

British operations in Egypt - Sir Ralph Abercromby, spring 1801 Important antiquities to be dispatched to Britain - Art XVI called for Rosetta Stone + several other large items

Over

Rosetta Stone didn't leave Egypt until 1801

Inscription in two languages:
1) Egyptian and 2) Greek

Egyptian portion in two parts.
1) Hieroglyphic characters - old picture writing used from earliest dynasties in making copies of the Book of the Dead + in nearly all state + ceremonial documents intended for public display
2) Demotic characters - the conventional abbreviated + modified form of the Hieratic character or cursive form of hieroglyphic writing which was in used in the Ptolemaic Period

The Rosetta Stone [+ the Obelisk from Philae] as CRIBS!

7,1

Rosetta Stone

[Norbert Wiener characterized ~~solution~~] decipherment of Egyptian hieroglyphics the greatest achievement of cryptanalysis!

1st translation of Greek text by Rev Stephen Weston + read by him before Society of Antiquaries in London in April 1802

1st studies of the Demotic text by de Sacy + Åkerblad in 1802 Latter succeeded in making out the general meaning of portions of the opening lines + in identifying the equivalents of the names Alexander, Alexandria, Ptolemy, Isis, etc Both de Sacy + Akerblad began by attacking the Demotic equivalents of the cartouches i.e. the ovals containing royal names in the hieroglyphic text.

[over] In 1818 Dr Thomas Young compiled

for the 4th volume of Encycl Brit (pub in 1819) results of his studies & among them was a list of several alphabetic Egyptian characters to which, in most cases, he had assigned correct values. He was the first to grasp the idea of a phonetic principle in the Egyptian hieroglyphs & he was the first to apply it to their decipherment.

But Young's name not associated in public mind with decipherment — that of Champollion.

Explain what C did. Study of Coptic — only another name for Egyptian Coptic never lost.

Champollion [1790-1832]

~~Norbert Wiener's CYBERNETICS~~

"I've got it!" He cries to his brother after running a mile to latter's office.
And falls into a deep & lengthy lassitude
for 5 days

But Champollion wasn't the only one
who deserves credit or largest share.

Cartouches from the Rosetta Stone & 4.2
the Obelisk from Philae ~~The~~

The bottom one was suspected to
represent CLEOPATRA,

+3

Cartouches for Ptolomey (A-the middle one of the preceding slide)
(B-the lowermost one of preceding slide)
and Cleopatra

Ptolomey + Cleopatra

4,5

Ptolemy and Alexander

Budge says (p.7 of Br Mus Brochure)

"By the comparison of texts containing variant forms, and by the skilful use of his knowledge of Coptic, Champollion succeed in formulating the system of decipherment of Egyptian hieroglyphs then, substantially, that in use at the present day."

→ Read list of items praising Ptolemy, p.7

It was a fortunate accident that early work had to deal with plain-language hieroglyphics What if they'd first come across encrypted hieroglyphs ?!!

1) Cryptographic hieroglyphics from Drioton 4.6

~~More of Same~~ ~~4.7~~

~~" " " " 4.8~~

2) " " " " 4.9

Michigan Cryptographic Papyrus , 4

Stop Wait,

Poe

no slide

LECTURE NOTE ; in America [redacted]

Edgar Allan Poe in the 1840's rekindled interest in cryptography, by his story "The Gold Bug" and a couple of essays and stories on ciphers and deciphering.

Story about challenge One and only
One message "~~he~~ couldn't solve, he wrote,
and that one he proved to be a hoax!
Story of Vincent { "I am the Master of the College
ditty in a { What I don't know ain't know
Cambridge Farce { ledge!

(14)

Come now to the period
of The American Civil War or
the War between the States

The Civil War Period in U.S.

Federal Army Ciphers

Confederate Army Cipher

Federal Army cryptanalytics

Confederate " "

Comment on use of telegraph

A couple of pages from one of the Federal Army Cipher Books

REF ID:A38503

1 Have book of Federal Army Ciphers with me.

2.

10

1) Message to General Grant
15 July 1863

10.1
10.2

2) Another message, Same date, but in two sections

LECTURE

[redacted] SLIDE 7

Cipher device used by the Confederate Army, during the Civil War. Captured at Mobile in 1865.

[Nothing but the old Vigenère cipher with repeating key. Many messages intercepted and deciphered by Federals, who had a few skilled operators. Ads in Richmond papers for persons skilled in deciphering shows the Confederates lacking.]

Keywords . COMPLETE VICTORY
COME RETRIBUTION
? MANCHESTER BLUFFS

REF ID:A38503

A cryptographic message from President Lincoln to Major General Burnside. 8

Comments on this episode: 1) Lack of confidence? 2) Save time?

Wilson, too, lacked confidence in 'official' ciphers

Gettysburg incident. See p 10
of Br Manual

After Civil War use of cryptography or cryptology went into decline during a long period of peace broken only briefly by the Spanish-American War.

(Save for the cryptography in the Tilden-Hayes Campaign of 1878)

Title page of "Telegraphic Code to ensure secrecy in the transmission of telegrams, by Robert Slater, 1870. 214

(This was 5th Edition - the 1st Ed. dates from about 1850)

Title page of Same as put out for War Department by Gregory, 1885

Published by GPO in 1886

Slater's Code Example I
Gregory's " " I

Spanish-American War

Code used was 1885 with fixed additive "777" !!

LECTURE NOTE

X 1. After Civil War use of crypt in U.S. military affairs went into decline during long period of peace, broken only briefly by Spanish-American War.

2. W.D. Tel. Code to Insure Secrecy of Telegrams 1885. Pub. GPO 1886. Based on Slater's Code.

X 3. Spanish-American War - "777"

4. 1899 CSO undertakes preparation of suitable code. Economy featured. Work personally done by CSO. As temporary expedient used W.D. Tel. Code of 1885 with new "Preliminary W.D. Tel Code" of 4000 special words and phrases -- late 99 or early 1900.

'5. 1902 - Cipher of the WD - published by TAG and only on

6. 1906 - WD Tel Code 1906 - by Greely

'7. 1915 - WD Tel Code 1915 - published in Cleveland by private printers

9

Title page of War Department
Telegraph Code 1915

Printed in Cleveland by private printer!

Cipher tables later put on

WW I breaks out in Europe
August 1914
Next period devoted to WW I crypt.

Example of micro-writing,
in the siege of Paris 1870

LECTURE NOTE For World War I

"With Hertz's discovery of so-called Hertzian waves and Marconi's practical demonstration of signalling by "wireless", a new era in military communications was ushered in. And also a new era in cryptology. The first wide usage of wireless or radio, as it soon came to be called, was in World War I. But developments in cryptography lagged a bit, as we shall see."

In Europe, cryptology continued in development
but mostly in the direction of larger and larger
codes, plain or enciphered, and in the direction
of certain types of ciphers, such as the Playfair;
(22) no cipher devices or machines worth mention
except two – and these we will talk about later –