LECTURE II - SECTION I

Next great landmark in (cryptanalytic) history of decipherment is the solution of Egyptian Hieroglyphs

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

Athanasius Kircher delays solution for decades

Problem not crypt primarily one of linguistics, grammar and recovery of dead language

41
The Rosetta Stone.

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

Napoleon's Army - Colonel Boussard (or Bouchard) Became General and was alive in 1814. (1769-1821)

British operations in Egypt - Sir Ralph Abercomby, Spring 1801 Important antiquities to be despatched to Britain - Art XVI called for Rosetta Stone and several other large items

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 and nearly all state and ceremonial documents intended for public display.

2. Demotic characters - the conventional abbreviated and modified form of the Hieratic character or cursive form of hieroglyphic writing which was in use in the Ptolemaic Period.

The Rosetta Stone (and the Obelisk from Philae) as CRIBS!

First translation of Greek text by Rev Stephen Weston and read by him before Society of Antiquaries in London in April 1802

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

In 1818 Dr. Thomas Young compiled for the 4th volume of Encycl Brit. (pub. in 1819) results of his studies and among them 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 and 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.

4.0
Champollion (1790-1832)

"I've got it!" He cries to his brother after running a mile to latter's office And falls into a deep and lengthy lasitude for five days

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

4 2
Cartouches from the Rosetta Stone and the Obelisk from Philae.

The bottom one was suspected to represent CLEOPATRA.

4 3
Cartouches for Ptolemy (A-the middle one of the preceding slide)
(B-the lower most one of preceding slide)
and Cleopatra

4.4
Ptolomey and 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 skillful use of his knowledge of Coptic, Champollion succeeded in formulating the system of decipherment of Egyptian hieroglyps this, 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?!'!

4.6
Cryptographic hieroglyphics from Drioton

4 9
More of the same.

4.
Michigan Cryptographic Papyrus

POE

Edgar Allan Poe in the 184Ø's rekindled interest in cryptography in America 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 ditty in a Cambridge Farce:

"I am the Master of the College What I don't know ain't knowledge!

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

The Civil War Period in the U.S

Federal Army Ciphers.

Confederate Army Cipher.

Federal Army cryptanalytics.

Conferedate Army cryptanalytics

Comments on use of telegraph.

9 A couple of pages from one of the Federal Army Cipher Books (Have book of Federal Army Ciphers with me)

10 Message to General Grant, 15 July 1863

10 1 and 10 2 Another message, same date, but in two sections.

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

(Nothing but the old Vigenere cipher with repeating key Many messages intercepted and deciphered by Federals, who had a few skilled operators Ads

in Richmond paper for persons skilled in deciphering shows the Confederates lacking.)

KEYWORDS: COMPLETE VICTORY
COME RETRIBUTION
MANCHESTER BLUFFS

8

A cryptographic message from President Lincoln to Major General Burnside.

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

Wilson, too, lacked confidence in official ciphers.

Gettysburg incident. See p 10 of British 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)

214

Title page of "Telegraphic Code to ensure secrecy in the transmission of Telegrams," by Robert Slater, 1870. (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 in GPO in 1886

215

Slater's Code Example I.
Gregory's Code Example I

Spanish-American War.

Code used in 1885 was fixed additive "777"''

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

1902 - Cipher of the WD - published by TAG and only one.

1906 - WD Tel Code 1906 - Greely

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

216

Title page of War Department Telegraph Code 1915

Printed in Cleveland by private printer'

Cipher tables later put on

WWI breaks out in Europe, August 1914.

Next period devoted to WWI crypt.

128

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

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 No cipher devices or machines worth mention except two--and these will be talked about later