#3 27 Cards

LECTURE NOTE FOR SLIDE 6.8

"The Benedict Arnold indecipherable Treasonable Cow Letter"

Here's an interesting slide showing a picture of a letter which was written by Benedict Arnold, of early Colonial infamy. He even was willing to see that his commander-in-chief, Washington, was captured by giving the British information like this

LECTURE NOTE FOR SLIDE 160

REF ID:A62872

Renaissance of interest in U.S.A.

Colonel Parker Hitt

But despite his knowledge - omit here
WDTC 1915

LECTURE REF ID:A62872 For SLIDE 4.11

Example of a rebus

/No doubt this first slide will carry all of you back to the days of your childhood or at least to your earliest schooldays. I show it only because it has a rather close connection with cryptography. The question as to which came first -- the invention of writing or the invention of cryptography is like the question as to which came first --the hen or the egg. The answer to both is quite difficult to give. But it is quite clear at least that some phases of cryptography came before the

art of writing had undergone any or very much development. The rebus contains features of both -- you have to "decrypt", so to speak, the significance of some of the symbols before you can read the writing as a whole and learn its meaning.

LECTURE NOTE REF ID:A62872 FOR SLIDE 3.2

An example of a hoax involving what appears to be "runic" secret writing.

BIL STUMP - his mark -- from Dickens' Pickwick Papers

SLIDE 217

REF ID:A62872

Cipher used by Mary Stuart, Queen of Scots, with Babington.

(From "The Babington Plot" by Smith, 1936)

She reigned from 1542-1567; beheaded 1587

LECTURE NOTE REF ID:A62872 FOR SLIDE 218

"The Forged Postscript, with Phillips's endorsement"

(Frontispiece of "The Babington Plot" by Smith, 1936)

SLIDE 5.2

REF ID:A62872

A cipher system used by Philip II of Spain
(1555-1598)

LECTURE NOTE REF ID:A62872 FOR SLIDE 3.7

Sliding-card Cipher. A facsimile of one used in the later years of Queen Elizabeth's reign (about 1600).

A sliding card, which could be shifted up and down, was used for changing the key, or as a means of changing the key.

LECTURE NOTE

3.8.

REF- ID:A62872

The Two-Word Square Cipher. A facsimile of a State Cipher used in Charles the First's time (1627) for communicating with France and Flanders. I. The Key. " This cypher is made doble (double) going twise over the alphabet only for varietie to make it harder to be deciphered. When in writing aine thing (anything) in this cypher you are to make use ~~of~~ the letter itself, but in place thereof to set down two letters, one such letter of the word OPTIMUS, as is set directly over the letter you meane: and the other such (word)

use of letters to express your words, your agents

letter p&u the woord DOMINUS as is directly opposite to the said letter you meane to write."

LECTURE NOTE REF ID:A62872 FOR SLIDE 6.1

Cipher table in an early Elizabethan state cipher used in communicating with the Ambassador in Spain.

(Proof that Porta was not inventor?)

(Usually inserted before

REF ID:A62872 SLIDE 5.1

VIETA, FRANCISCUS - French mathematician and founder of modern algebra.

In 1589 became councillor of parliament of Tours - then royal privy councillor. While there discovered key to Spanish cipher - more than 500 characters - then all Spanish dispatches falling into French hands were easily read.

Philip II of Spain was so convinced of safety of his ciphers that when he found French were aware of contents of his letters to Netherlands he complained to the Pope that French were using sorcery against him. Vieta called on carpet to explain.

LECTURE - REF ID:A62872 SLIDE 27.4

Decipherment of a cryptogram in a map:-

Message written in Morse along tram lines on a plan of Amsterdam - addressed to Mr. M.J. Nauk, Rotterdam postmark -S. Newington, 20 Dec 1915

"OEL ANGEKOMMEN ALLES FERTIG
GUSTAV FREI FUR BESTIMMTEN TAG FERTIG"

LECTURE NOTE REF ID:A62872 FOR SLIDE 30

German sabotage message of World War I

"Here is another message solved in World War I by the British and made available to our authorities in Washington; a sabotage message talking about who were reliable saboteurs and what they should do. That message figured in a long,long trial before the German-American Mixed Claims Commission, in which the Germans were charged with certain acts of sabotage, notably the Kingland fire and the Black Tom explosion in New Jersy. Most of you are too young to remember those incidents. The trial resulted in a decision in favor of the United States claimants, who were awarded some 40 million dollars."

LECTURE NOTE REF ID:A62872 FOR SLIDE 127

Example of secret ink writing (1917)

Black Tom and Kingsland Fire --Lackawanna RR et al.
$40,000,000
G-A Mixed Claims Commission

LECTURE NOTE REF ID:A6287 FOR SLIDE 128

Example of micro-writing (1870)

Micro-writing is not so new as we might think. See Galland - under Mendelsohn. Not re Mendelsohn's decoding Gambetta code letter dated Oct 24, 1870 and microphotograph. Could this be same as my micro?

p. 123 of Galland

REF ID:A62872

World War I breaks out August 1914

Renaissance of interest in U. S.

Mauborgne

Hitt

LECTURE NOTE REF ID:A62872

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

LECTURE NOTE REF ID:A62872 FOR SLIDE 155

Herbert O. Yardley as First Lieutenant, 1919.

(Effect of disclosures)

LECTURE NOTE REF ID:A628772 SLIDE 38

The Oil Scandal investigation.

(Where $68,000 gets transformed into 6 or 8 cows)

SLIDE 36

REF ID:A62872

Illustrating one of the cardinal sins in cryptography - repeating a message in another system, without some changes.

Hand-operated "Purple" analogue

Page 232:

"The success achieved in reading the Japanese diplomatic codes merits the highest commendation and 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."

It would be nice if it were permissible to raise the curtain fully and tell you all about the fascinating secrets there are [redacted] now as well as I do that I can't lift the curtain entirely -- I can only let you have a peek. The necessity for secrecy in the field I'm going to talk about is so great that in May 1950 Congress enacted special legislation to give us the protection we need. The law is known as Public Law 513 and if I should violate it by telling you too much, even though my talk has been officially authorized and everybody here is present by proper authority, I could be separated from $10,000 if I had that much, or could be given the dubious pleasure of spending my next 10 years as a guest of one of Uncle Sam's institutions for the re-education of criminals, or I could be given both treatments, neither of which I am anxious to try. So please don't hold on to your seats in the expectation of hearing any real hot stuff. (THE END)

messages and doing the job correctly as regards the requirements of secrecy. Perhaps you will also sometime be responsible for seeing to it that the communications of your own command or of commands under your cognizance are secure, that is, that they won't be easily read by unauthorized persons or, in time of war, by the enemy. Some of you may even find yourselves in positions where it will be your job to supervise the making of our own cryptosystems, or of breaking the enemy's. Hence, an appreciation of some of the pitfalls and achievements of cryptology will be useful to all or most of you, at least some time or other in your military careers.

It would be nice if I were permitted to raise the

(OVER)

LECTURE NOTE

REF ID:A62872

SLIDE 150

Magic Machine

In his recently published memoirs, Winston Churchill tersely appraises the contribution of communication intelligence in these guarded comments on the battle of Midway, which I quote:

"It is difficult to exaggerate the importance of this memorable American victory, not only to the United States, but to the whole allied cause. The American intelligence system was successful in penetrating the enemy's most closely guarded secrets well in advance of events. Thus Admiral Nimitz, albeit the weaker, was twice able to concentrate all the forces he had in sufficient strength at the right time and place. When the hour struck this proved decisive. The importance of secrecy and the dire consequences of leakage of information in war are here proclaimed."

SLIDE 15

REF ID:A62872

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