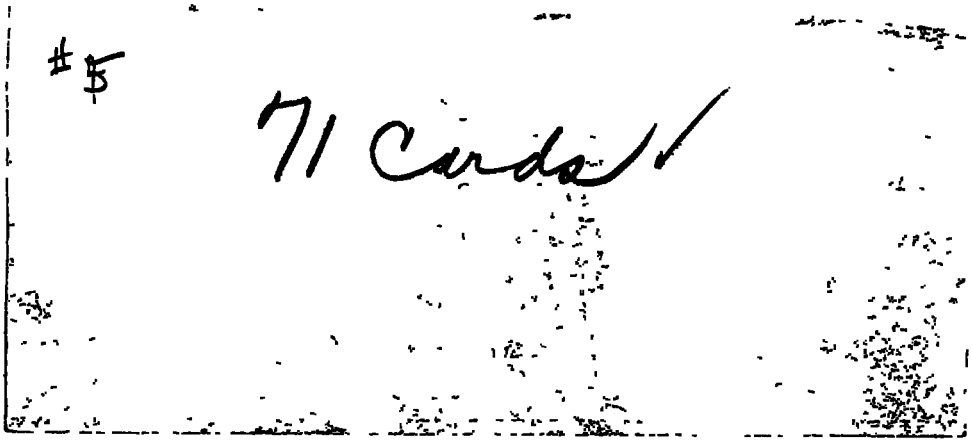


Silde 1

Instances of cipher in the Bible: Jeremiah 25:26 and 51:41 (circa 650 B.C

(Incidentally — Daniel was early psychoanalyst (Nebauchadnezzar's dreams) and first cryptanalyst. (Belshazzar and the handwriting on the banquet-hall wall)

- - - - - -

Mene - God hath numbered thy kingdom and finished it.
Tekel - Thou art weighed in the balances and found wanting.

Upharsin) Thy kingdom shall be divided and given to
Peres) the Medes and Persians.

(OVER)

But I wantto draw your attention to the fact that the use of cryptography goes back much further than 650 B.C. - it was used even by the ancient Egyptians. (Explain)

SLIDE 2

The scytale of the ancient Lacedaemonians - an example of a transposition cipher.

/Origin of European Field Marshal's baton -- one of the insignia of his high office./

Caesar's Cipher

REF ID:A62874 SLIDE 1

Cryptography and cryptanalysis go back to the dawn of the invention of writing, but we won't have time here to go back quite that far, even though the story is very interesting. But I must tell you right off that these two subjects, cryptography and cryptanalysis, are, of course, very closely related - in fact, they may be regarded as the two faces of the same coin. (Explain)

LECTURE NOTE REF ID:A62874 FOR SLIDE 3.1

Example of runes and runic writing (with WFF)

/Rune means "secret". Used by Germanic peoples from 3rd century A.D. and in England through the period of Anglo-Saxons. Used as magical signs, secret writing and especially for inscriptions. Origin obscure but probably from Greek and Latin letters./

SLIDES 3+246

Examples of cipher alphabets and syllabaries used centuries ago:

1. Employed by Charlemagne (768-814 A.D.)
2. Used in England during reign of Alfred (871-899)
3. Ogam writing of ancient Ireland
4. Ogam-like alphabet used by Charles I, 1646 to Marquis of Worcester.
5. Marquis of Worcester's cipher (the so-called "Clock Cipher")
6. Cardinal Wolsey, Vienna, 1524
7. Sir Thos. Smith, Paris, 1563
8. Sir Thos. Chaloner, Madrid, 1561
9. Sir Edw. Stafford, Madrid, 1586

246 goes here

These on #3

[246 is the better one]

SLIDE 4.10

An early Italian cipher alphabet (1429) from Mantua.

/Beginnings of modern cryptography were in Venice, in the Papal States, about 1400. Earliest MSS of Gabriel Lavinde (1380?)/

/Sicco Simonetta - earliest treatise on cryptanalysis - or cryptography in the world (1474)/

/Use of variants indicates also some knowledge of principles of solution by frequency of occurrence./

[2 slides] (Trithemius picture) 245 Oath SLIDE 151

REF ID: A62874

TRITHEMIUS - Earliest book, 1516 on Cryptography
(STEGANOGRAPHIA)

245 MEISTER says T. planned 4 books; T. finished first on March 27, 1500; second on April 20 same year. "Dann war er bekanntlich in den Verdacht der Zauberei geraten, und so hatte er die Arbeit mit dem dritten Buch abgebrochen, das Kein Termin des Abschlusses mehr angibt..."

151 SLIDE SHOWS: The Trithemian Oath.

*

SLIDE 6

REF ID:A62874

Porta's Table, from his book, De furtivis literarum notis, vulgo de ziferis, Naples, 1563.

/Neapolitan mathematician, inventor of camera obscura./

/Earliest solver of keyed multiple-alphabets according to Mendelsohn, but I think Alberti did it first - WFF/

The Vigenère Table as it usually appears in the literature.

SLIDE 5.1

The Vigenère table as it appears in Vigenère's own book, Traicte des chiffres, ou secretes manieres d'escrire", Paris, 1586.

/Vigenère did not invent the square, and never claimed he did -- first one to publish it. Was probably invented by Alberti or some early cryptographers employed by Papal States. Bellaso first suggested key?/

(Will jump directly to C & C of American Revolutionary period.)

REVOLUTIONARY WAR PERIOD Systems used by Americans and by British:

	Americans:-	British:-
Ciphers	(a. Simple momoalph. sub. (b. Monoalph. with variants by use of long key sentence a la Franklin (c. Vigenere with repeating key	(a. Monoalphabetic sub. (b. Vigenere with repeating key (c. Grilles
Codes	(a. Dictionaries (b. Keybook using words (c. Syllabaries	(a. Dictionaries 1) Entick's 2) Bailey's (b. Small alph. 1-part codes of 600-700 items & code names
	(Secret inks (Grilles	

(OVER)

REF ID:A628774

(c.Ord. book such as
(Blackstone - page
(line, no. of words
(in line.

British used code names. In Clinton Papers following are found:

American Generals - Apostles (Named after) (Washington = James)
(Sullivan = Matthew)

" cities:

Philadelphia = Jerusalem
Detroit = Alexandria
Delaware = Red Sea
Susquehanna = Jordan
Indians = Pharisees
Congress = Synagogue

SLIDE 6.4

REF ID:A62874

One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton:- 15 July 1780

"If I point out a plan of cooperation by which S(ir) H(enry) (Clinton) shall possess himself of West Point, the garrison, etc. etc., twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance."

(For full text see typewritten sheet accompanying plate 6.5.)

SLIDE 6.6

REF ID:A62874

Treason against Washington.

Arnold lays a trap for Washington.

LECTURE NOTE - REF ID:A62874 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 FOR SLIDE 6.9

REF ID:A62874

Example of use of a mask or grille by British in American Revolution -- but also used by Americans and particularly by Benedict Arnold.

Text of this example: "You will have heard Dr.Sir I doubt not only before that can have reached you that Sir W. Howe is gone from hence. The rebels imagine that he is gone to the ? , by this time. However he has filled Chesapeake bay with surprize and terror...etc."

SLIDE 231

LOVELL, James REF ID:A62874

Congress' cipher expert who managed to decipher nearly all, if not all, of British code messages intercepted by the Americans."

- - - - - - -

Philad[a]. Sep. 21, 1780

Sir:

You once sent some papers to Congress which no one about you could decypher. Should such be the case with some you have lately forwarded I presume that the result of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has been in the attempt. For it appears to me that the

(OVER)

Enemy make only such progress in their cypher when they meet with misfortune, /as makes a difference in position only to the same alphabet/ and therefore if no talk of Discovery is made by me here or by your Family you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect

Your Friend
James Lovell

(THE END)

SLIDE 6.31

REF ID:A62874

Extract from encoding section, Jefferson syllabary.

SLIDE 6.10

REF ID:A62874

Dlandol frontispiece (a cryptographer at work) [1793]

His assistant -- early model WAF (WAC)(WAVE)

Egyptian Hieroglyphics - Solution of Champollion - 1821.

LECTURE REF ID:A62874 SLIDE 4.0

Champollion, Jean Francois

/"Beside himself (when he had discovered the secret of the cartouches) Champollion left the apartment where he lived,...and ran to the library of the Institute where his brother was working. "I did it" he shouted, throwing some sheets of paper on the table, and fell into an apathy which was to last five long days." --I know how it feels but it never lasted five days with me!-WFF/

LECTURE - - REF ID:A62874 FOR SLIDE 4.1 .

The Rosetta Stone

/Norbert Weiner in Cybernetics calls decipherment of Egyptian hieroglyphics the greatest achievement in cryptanalytics. Champollion's first decipherments in 1821./

Cartouches from the Rosetta Stone and the Obelisk from Philae.

(The bottom one was suspected to represent CLEOPATRA. Note the repeated symbol, the BIRD, for the two A's of CLEOPATRA.)

Top cartouche - which is the middle one of preceding slide --- suspected to represent PTOLEMY.

Middle cartouche - which is the bottom one of preceding slide -- suspected to represent CLEOPATRA.

Bottom cartouche - the letters and unknowns of KL??P????

REF ID:A62874

PTOLEMY and ALEXANDER

REF ID:A62874

LECTURE -- - - For SLIDE 4.6

Cryptogfaphic hieroglyphics from Drioton

/Refer to confirmatory evidence of early invention of cryptography -- with writing itself./

The Michigan Cryptographic Papyrus.

AFTER SLIDE 4

Poe

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.

SLIDE 7

REF ID:A62874

Cipher device used by the Confederate Army, during the Civil War. Captured at Mobile in 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 papers for persons skilled in deciphering shows the Confederates lacking./

SLIDE 9

REF ID:A62874

Federal Army Route Cipher

(Complete set with me - invite ~~cadets~~ to see exhibits.)

SLIDE 10

REF ID:A62874

Example of a message in Federal Army Route Cipher -
a message to Grant from General Halleck in Washington.

SLIDE 8

REF ID:A62874

Cryptographic message supposed to have been sent by President Lincoln to General Burnside.

/Read backwards: "If I should be in a boat off Aquia Creek at dark tomorrow, Wednesday evening, could you without inconvenience meet me and pass an hour or two with me? (Signed) A. Lincoln/

/Possible explanation of Pres. - distrust of Fed. systems since he was getting decrypts./

SLIDES 214 & 215

REF ID:A62874

Period of decline after Civil War

2

War Department Code of 1885 - copied from Slater's Telegraphic Code of 1870. } 214

This code was used in the Spanish-American War - 1885 code with simple additive (717)

LECTURE NOTE REF ID:A62874 FOR SLIDE 157

Colonel George Fabyan

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

World War I in progress since 1915. U. S. position. Fabyan's foresight - U.S. had no cryptologic bureau. Contact with Government Departments. School for training.

LECTURE NOTE REF ID:A62874 FOR SLIDE 160

Renaissance of interest in U. S. A.

Colonel Parker Hitt

But despite his knowledge --
WDTC 1915 -

We begin study of military cryptology after contact established with Captain Parker Hitt, (whose Manual for the solution of Military Ciphers became our text-book).

REF ID:A62874 212

Title page of "Manual for the solution of military ciphers" by Parker Hitt, 1916

LECTURE REF ID:A628874 FOR SLIDE 159

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 cryptographic 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./

LECTURE NOTE REF ID:A62874 FOR SLIDE 213

Mauborgne's pamphlet on solution of PLAYFAIR cipher system.

SLIDE 33

REF ID:A62874

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

REF ID:A62874

SLIDE 34

Solution of the Hindu letter.

SLIDE 28

REF ID:A62874

The Zimmermann telegram

/The telegram which brought America into the war on the Allied side, World War I. Many reasons for thinking we might go in on the side of the Germans and had they been more astute diplomatically, it might have turned out that way!/

SLIDE 29

REF ID:A62874

The Zimmermann telegram as deciphered by the British Room 40 O.B.

"Here is a translation of the thing. It was important because the message said the Germans were going to resume unrestricted submarine warfare and this part, here, dealing with Mexico, was the straw that broke the camel's back. People in the Middle West were very lukewarm toward the idea of our getting into the War - on either side - but when the Germans began talking about returning to Mexico Texas, New Mexico and Arizona, that was something else again. So we got into the war within a couple of weeks after the British gave us and established the

(OVER)

authenticity of the translation of the Zimmermann telegram."

- - - - - - -

(How the Zimmermann telegram was deciphered makes a fascinating story in itself and shows how astute use was made by the British of this telegram. German amazement and embarrassment. Question of spy work etc. in Mexico. British covered up the trail excellently!)

LECTURE NOTE REF ID:A62854 SLIDE 25

The Waberski cryptogram

"Now I am coming to a very interesting example of the use of ciphers by German agents in the World War I period. Here is a cipher message which was found on a German spy in the United States soon after he crossed the Mexican border into Texas. After some weeks it was deciphered by G-2's code-solving organization in Washington, MI-8, as it was called.

Text on next card

LECTURE NOTE REF ID:A628674 FOR 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."

SLIDE 82

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

/Got so immersed in crypt I used it everywhere possible - cipher suppers etc./

LECTURE FOR SLIDE 48

REF ID:A62874

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

(First improvement on the Alberti disk.)

Modified Wheatstone

REF ID:A62874

I go overseas to G-2, A-6, GHQ,

Importance of invention and development of radio in communications, especially military.

LECTURE NOTE FOR SLIDE 12

REF ID:A62874

Transposition cipher system used by the French Army in World War I. Copied from a German book on cryptography (Fig. 1) -- and correct.

LECTURE NOTE REF ID:A62874 FOR SLIDE 13

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

SLIDE 23

REF ID:A62874

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 Playfiar, 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./

SLIDE 14

REF ID:A62874

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./

SLIDE 11

REF ID:A62874

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

SLIDES 19-22

REF ID:A62874

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.

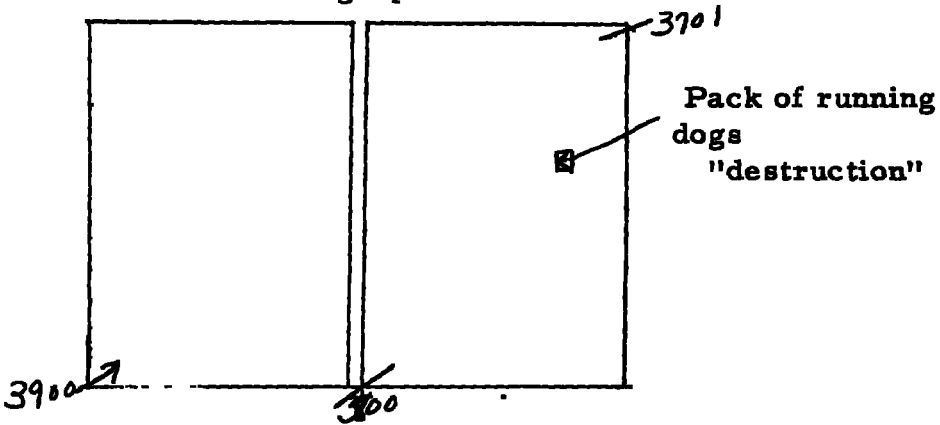
LECTURE REF ID:A62874 FOR SLIDE 16

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 REF ID:A62874 FOR SLIDE 17

Chinese official telegraphic code.



LECTURE REF ID:A62874 FOR SLIDE 18

A highly specialized "commercial code"

Call attention to 3-letter difference:

YGATA - COMA
YGKRO - DELIRIUM TREMENS

YGCIB - CONSTIPATION
YGMAN - DIARRHEA

SLIDE 21

An early AEF Code in World War I

/An indication of how poorly prepared we were for COMSEC./

Title page of War Department Telegraph Code 1915

LECTURE NOTE - REF ID:A62874 FOR SLIDE 19

Two-part tactical code used by French Army in World War I. The code groups were then enciphered!

LECTURE FOR SLIDE 22

REF ID:A62874

British Army Field Code, World War I

/A two-step process. How we got copy -- Relations with British were not close. For that matter, relations with French in these matters were not too close either. How we learned of ground intercept./

SLIDE 20

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./

LECTURE FOR SLIDE 24

REF ID:A62874

One of the American field codes, World War I

[River series for the First Army; Lake Series for the Second Army]

SLIDE 14.1

REF ID:A62874

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

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

SLIDE 15

REF ID:A62874

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

LECTURE REF ID:A628674 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 pool from which to draw trained personnel because there is no civilian occupational specialty of the same nature.)

LECTURE REF ID:A62874 SLIDE 149

The S.I.S. staff in 1935

/Call attention to the vault door -- when we worked in great secrecy./

Marshall - Dewey Letters

LECTURE NOTE SLIDE 150

Magic Machine

SLIDE 169

REF ID:A62874

Collange, Gabriel de

(His photo matches the mental picture the average layman has of a cryptanalyst.)

The veil of secrecy has produced an air of mystery. Before the World War II, it was possible to do much processing merely with pencil and paper. Now cryptanalytic work is a very big business -- complex, expensive, but pays big dividends.

LECTURE NOTE REF ID: A62874 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 important -- the question of testing out multiplicity of assumptions and hypotheses, commonly by statistical methods.

High-speed testing is secret!

- Earliest cryptanalytic devices at Riverbank Laboratories.