#7

100 Cards ✓

95 80

REF ID:A62878

West Point lecture
(many cards not here — were used for other lectures)

FRONT

The following cards represent the sequence and content of my lecture "The influence of cryptologic power on history," given before the cadets of the Third Class, U.S. Military Academy, West Point, N.Y. on 28/29 May 1952. [The class was divided into two sections to accomodate seating capacity of lecture room, about 350.] The lecture took 80 minutes, with a 5-minute break about midway.

THE INFLUENCE OF CRYPTOLOGIC POWER ON HISTORY. CARD 1

Colonel Bessell, other members of the Faculty, and Cadets of the Third Class:

This morning I'm going to talk about cryptology, that is, the subjects of cryptography, cryptanalysis, and a type of military intelligence now called communications intelligence, or COMINT, for short. /Define/ In a way, we are making cadet history to-day, for so far as I am aware this is the very first time when a lecture on these subjects has ever been given at the Academy.

When the official request that I give this talk was made, it was stated that:

"The purpose of this lecture is to supplement the

(OVER)

cadet course in Mathëmatical Statistics, by letting the cadets hear an [illegible] discourse related to an important military application of statistics. It is also intended, as a by-product, to enhance the cadets' appreciation of security precautions in military communications."

Cryptology is, in the final analysis, indeed an application of statistics, and, when used for military purposes, it can be important indeed! But the idea that it is a subject of importance was not always evident or generally accepted, and to illustrate I will tell you a story I read some years ago in an old book on cryptography. The story may be apocryphal, but I tell it for what it is worth. /Semiramis/

I'm now going to read you a paragraph or two from TIME MAGAZINE, the issue of 17 December 1945. /Read 1st 2-3 para./

(CONTINUED ON CARD 2)

CARD 2

The account goes on to tell in some detail what the "story" is. I hope I'll have time to return to it a bit later.

With this introduction, I think we're ready to begin. But relax, gentlemen, relax! I do not intend to bother you with any mathematical demonstrations of the statistical methods or principles employed in cryptology, for I suppose you've had enough of that in the course in Probability and Statistics to do you for some time to come. Anyhow, that would be too dry a talk for me as well as for you. I prefer to talk to you about something which I think is far more interesting -- the background of cryptology, especially that part of it which will give you some idea of how cryptography and

(OVER)

cryptanalysis have been used and mis-used in modern warfare and diplomacy, as REF ID:A62878 realize that the often startling results which were obtained were derived by the application of some of the very principles you were taught and have studied in your course you've just completed. It may be that if I show you only a very few of the outstanding and authentic examples of such incidents in cryptologic history you will come to have a sufficient respect for what cryptologic science can do for or against you to remember for a long time after you enter upon your active military career the lessons taught by those incidents. You should remember them because throughout your active career as officers in various positions in the military service, whether those positions are tactical or administrative in character, you will have the responsibility of writing

(CONTINUED ON CARD 3)

CARD 3

REF ID:A62878

messages and doing the correct thing as regards the requirements of secrecy. Perhaps you will also some time be responsible for seeing to it that the communications of your own command or of commands under your cognizance are <u>secure</u>, 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 curtain

(OVER)

~~It would be nice if I were able to raise the curtain~~ fully and tell you all about the fascinating secrets there are behind it. But you know 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 P ublic 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 be given both treatments, neither of which I am'

(SEE ATTACHED CARD)

anxious to try. So please don't hold on to your seats in the expectation of hearing any real hot stuff.

([redacted])

The title of my talk is "From biology to cryptology: a few episodes in the Saga of the Seduction of a Cornellian and its Aftermath."

No doubt you want to know who seduced me to do what and what the aftermath of the seduction was, or is.

First, let me say that the seduction has to do with a situation in which it came about that a graduate student in the AG College at Cornell who had chosen genetics as his area of interest in the biological field and whose studies therein embraced such unmilitary enterprises as marrying pairs of Drosophila Ampelophila (fruit flies, to most of us), setting up the married couple in a pleasant housekeeping situation and watching the types and numbers of the

I will begin by reading an extract from the 17 Dec 1945 issue of TIME--an extract which was at the time not only dramatic in its impact but also devastating to our national security because it told of disclosures about a hitherto extremely well-kept U.S. secret weapon of World War II, a weapon which in the opinion of top-level Congressional personages "contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

Read from TIME, p. 20.

In a few minutes I'll come back to this story, for it is one in which I had the good fortune to play a directing role.

resultant progeny-how it came about, in short, that such a student got mixed up in a military activity of such secrecy that during World War II he was practically directed to have no dealings with his wife who was in an analogous military activity in the Navy--in fact, he was inferentially directed to sleep in a separate room for fear he would talk in his sleep and thus disclose Army secrets to a Navy character--which wouldn't do at all, for at that juncture the military philosophy dictated that Army secrets were Army secrets, and Navy secrets were Navy secrets, and never the twain shall meet at all.

But let's get right down to the story now. It begins in May 1915. I'd received my B.S. in February 1914 and stayed on to pursue work in the Graduate

School, looking toward my doctorate degree in genetics. But a certain Co-ed Prudence Risley?--had set her sights on me and I'd decided that an exodus would be wise before it was too late.

Now by rare good fortune the Dean of the Ag College had just received a request from a wealthy Chicagoan for a young qualified geneticist who might be interested in starting a genetics laboratory on his farm or estate (called Riverbank or the Riverbank Laboratories), about 35 miles west of Chicago. Dean Mann, I think it was, nominated me for the job and that's how I came to work for Colonel (Kentucky variety) George Fabyan, who born a Boston Bralinin became the black sheep of his family. My first talk with him about the job, when I asked about his agricultural activities at Riverbank and wanted to know what he raised out on the farm, Colonel Fabyan replied "I raise hell!" I then asked what part I was to play in these activities and his reply was characteristic: "Well, I want you to help me raise it!" I promised to do my best. I don't think I did too badly.

I left Ithaca, and doubtless a broken-hearted Co-ed--and went directly to Riverbank after a couple months' tour of genetics laboratories in the East (at the Colonel's expense). There at Riverbank I found a couple of other activities of a scientific or quasi-scientific nature. Among these was a division devoted--of all weird things, so I thought at the time--to attempting to prove by means of cryptography that Francis Bacon was the real author of the great plays attributed to William Shakespeare.

Colonel Fabyan provided me with laboratory facilities, greenhouse space, land for the pursuit of my studies in genetics--and batchelor quarters in a wind mill. He gave me an absolutely free hand in respect to the problems I might want to study--that is, except in the case of one episode which may be of some interest if not amusement to tell. (Sowing wild oats by moonlight.)

Now in the year 1915 not many young men just out of college were affluent enough to own automobiles, and I was no exception in this regard. Riverbank was 35 miles from the big city, Chicago, and several miles from the nearest town. So I stayed pretty close to home. Col. Fabyan saw to it, though, that time would not hand too heavily on my hands, by getting me interested in the cipher work of his very old but still very able protoge, Mrs. Elizabeth Wells Gallup, who was in charge of the Bacon-REF ID:A62878 Getting me interested in cryptography was the first step in my seduction. I fell hard for the subject and began studying it in my leisure hours. I even began helping Colonel Fabyan and Mrs. Gallup by making certain drawings and exhibits which later on plagued me no end. These were extended to illustrate points about the cipher system which Francis Bacon had invented and described in his acknowledged works and which Col. Fabyan and Mrs. Gallup firmly believed was imbedded in the plays in the form of secret messages telling tall stories that were completely at variance with history as recorded in the history books.

We'll now leave this phase of my talk for a few minutes while I devote some time to telling you a bit about what I learned of the history of cryptography. The subject is very very old, I can illustrate its age by a story which may be a bit apocryphal.

Semiramis

I daresay, in regard to the point about when cryptography was first used, as in the case of the hen and the egg, that nobody really knows which came first, intelligible writing or secret writing, that is writing to communicate something to somebody or writing to hide everything from everybody except a few cognoscenti, as was true in the case of Egyptian hieroglyphic writing.

So let's now go in for a bit of the history of cryptology, which is the single term that embraces both cryptography (define) and cryptanalysis (define).

SLIDE 1

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

/Incidentally -- Daniel was early psychoanalyst (Nebuchadnezzar's dreams) and first cryptanalyst. (Belshazzar and the handwriting on the banquet-hall wall)7

- - - - - - -

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 want to call 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

17

SLIDES 3, & 246

Examples of cipher alphabets and very brief 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

246 ends here

These on #3

7. Sir Thos. Smith, Paris, 1563
8. Sir Thos. Chaloner, Madrid, 1561
9. Sir Edw. Stafford, Madrid, 1586

[# 246 is the better slide]

19

SLIDE #

SLIDE 4.10

An early Italian cipher alphabet (1401) from Mantau.

[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 245] and [SLIDE 151 oath]

245-TRITHEMIUS - Earliest book, 1516 on cryptography (STEGANOGRAPHIA)

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. (Idea of secrecy curtain goes back to the earliest days of the science!)

SLIDE 6

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.-WWF]

21

The Vigenère Table as it usually appears in the literature

(22)

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

/Vigenere 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.)

23

[redacted]

REF ID:A62878

REVOLUTIONARY WAR PERIOD - Systems used by Americans and by British:

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

(OVER)

(items & code names
(e.g. books such as
(Blackstone - page
(line, no. of words
(in line.

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

American Generals - Apostles (Washington ≡ James
(Sullivan ≡ Matthew

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

SLIDES 6.4 [& 6.5]
omit

See next card ~~for text~~.

Benedict Arnold - "James Moore, Edward Fox, Gustavus"
Major Andre - "Joseph Andrews, John Anderson"

- - - - - - -

Arnold, disgruntled with injustices of Congress, starts off anonymous correspondence, giving information showing he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary; word cipher with words out of Blackstone and songbooks; grilles; slips of paper enclosed in specially constructed hollow bullets. André captured Sep 1780, writes out full confession and was hanged. Arnold barely escaped to British lines (peculiar part of Arnold's treason).

241

SLIDE 6.4

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 (Sir) H(enry) (Clinton) shall possess himself of West Point, the garrison, etc. etc., twenty thousand pounds of 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)

24 2 (

SLIDE 6.6

Treason against Washington

Arnold lays a trap for Washington.

25

LOVELL, James

SLIDE 231

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

- - - - - -

Philada. 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 bben in the attempt. For it appears to me that the

(OVER)

Enemy make only such changes in their Cypher when they meet with misfortune, /_the makes a difference in position only to the same alphabet_7 and therefore if no talk of Discovery if 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

Extract from encoding section, Jefferson syllabary.

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.[

SLIDE 6.10

Dlandol frontispiece (a cryptographer at work)(1793

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

30

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-/

Egyptian Hieroglyphs - Solution of

Champollion - 1821

LECTURE

FOR SLIDE 411

REF ID:A62878

The Rosetta Stone

/_Norbert Weiner in Cybernetics calls decipherment of Egyptian hieroglyphics the greatest achievement in cryptanalytics. Champollion's first decipherments in 1821._7

32

LECTURE

For SLIDE 4.2

Cartouches from the Rosetta Stone and the Obelish from Philae.

[The two top ones thought to represent PTOLEMY. The bottom one was suspected to represent CLEOPATRA. Note the repeated symbol (bird) for the two A's in 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 ????

952

~~Ellis, [FNU]~~

~~The secret office in the Post Office and the Office of Decipherer. [Photostatic copy of a typescript of 160 pages of text and 52 pages of references.]~~

Cryptology - History

The Friedman
Collecti

PTOLEMY and CLEOPATRA

PTOLEMY and ALEXANDER

931

Stein, Gertrude:
Brewsie and Willie. New York: Random House, 1946, pp. 114

Modern Literature
Joyce, James
Stein, Gertrude
Unintelligibility, The cult of

LECTURE

For SLIDE 4.6

Cryptographic hieroglyphics from Drioton

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

The Michigan Cryptographic Papyrus

922

Foner, Philip S. [Editor]

Basic writings of Thomas Jefferson. New York: Willey Book Co., 1944, pp. 816.

American revolutionary period,
cryptology of
Revolution, American
British cryptology in
American Revolution

The Friedman
Collection

AFTER SLIDE 4

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

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 <u>deciphered</u> by Federals, who had a few skilled operators. Ads in Richmond papers for persons skilled in deciphering shows the Confederates lacking.]

SLIDE 9

FEderal Army Route Cipher

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

SLIDE 10

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

42

SLIDE 8

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

Period of decline after Civil War

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

This code was used in the Spanish-American War - 1885 code with simple additive — "777."

We come now to 1914 -- and the outbreak of World War I, in Europe in August. Although for most Americans that war was 3,000 miles across the ocean, there were a very few Americans who were astute enough to try to take a glimpse of that which could or might happen in the not too distant future. One such American was Colonel George Fabyan, my employer.

LECTURE NOTE **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 1914. U. S. position. Fabyan's foresignt - U.S. had no cryptologic bureau. He foresaw it would be necessary to have people trained for cryptologic work on foreign communications and he established contact with Government Departments. (1) for cryptanalytic operations. (Army, Navy, State, Justice, Treasury) (2) School for officer training -- Army and Navy, but mostly Army.

Colonel Fabyan makes contact with Captain J. O. Mauborgne, then an instructor at the Signal Corps School at Ft. Leavenworth. Here's a picture of Mauborgne taken almost 30 years later--when he was Major General, Chief Signal Officer of the Army.

LECTURE 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 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./

Mauborgne's pamphlet on solution of Playfair cipher system.

It was to Mauborgne that Colonel Fabyan went for guidance and assistance in his desire to establish a laboratory or bureau for the study of military cryptology.

Another American Army Officer whose interest in cryptology exercised a very important effect upon us at Riverbank was

Captain Parker Hitt, INF.

We begin serious study of military cryptology using as our principal text Hitt's Manual for the Solution of Military Ciphers.

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

50a

This was the second act in the story of my seduction. I began putting in 1/4 time on studying ciphers--3/4 time in my genetics laboratory.

The third act was when close study together and daily--most of the time, soon hourly--contact brought me to see the virtues and beauteous characteristics of the young lady who was at the head of the group studying Bacon-Shakespeare cryptograms. (She'd arrived at Riverbank exactly one year after me; we were married exactly one year thereafter! The title of my talk had a subtitle in which there is mention of an aftermath of my seduction from biology to cryptology; one of the most important "aftermaths" is here with us tonight--our son John (whose middle name is Ramsay, after the name of his godfather, Ramsay Spillman), also a Cornellian, class of 1950. Stand up, John, and take a bow.

John is a member of the Bell Telephone Laboratories and is doing some interesting things in the way of making documentary films of a scientific character.

There is another "aftermath" -- a very nice young woman, our daughter Barbara, Radcliffe Graduate and wife of a graduate electronics engineer and graduate research physician at the National Institutes of Mental Health, who combines both sciences in his studies of the electronics of the brain and the nervous system.

We assist the British Intelligence in the case of the Hindu Conspiracy, 1916-17.

SLIDE 33

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

SLIDE 34

Solution of the Hindu letter.

SLIDE 28

The Zimmerman telegram

[The telegram which brought American 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!]

WALTER CRONKHITE'S "YOU ARE THERE!" program on the ZIMMERMANN TELEGRAM.

SLIDE 29

The Zimmerman tlegram 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, there was something else agains. So we got into the war within a couple of weeks af;ter the British

(OVER

gave us and established the authenticity of the "The Zimmermann Telegram".

- - - - - -

(How the Zimmerman 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 FOR 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 Washingtonm MI-8, as it was called.

Text on next card

LECTURE NOTE

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!"

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

Original Wheatstone cipher device (invented in 1869 and described in 1879).

[First improvement on the Alberti disk.]

Modified Wheatstone

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

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

I was naturally quite inquisitive about the various codes and ciphers used by our own Army and by our allies, as well as in those used by our adversaries, principally, of course, the Germans. I found that we Americans were woefully unprepared.

The principal code used for Army communications, including highest command, was the War Department Telegraph Code of 1915.

Title page of War Department Telegraph Code of 1915.

The British warn us against its insecurity--even when super-enciphered--and hence there is a clear implication that they had been reading our messages, Army at least for sure. Maybe State and Navy, too!

LECTURE NOTE 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.

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.

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 Playfair, 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

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

Cipher system used by the Russians in World War I (from a book by the Austrain cryptologist, Andreas Figl)

[Misuse of this cryptographic system (or failure to use) cost the Russians defeat at Tannenberg!]

Importance of that defeat

Russo-Finnish War 1940

LECTURE FOR SLIDE 16

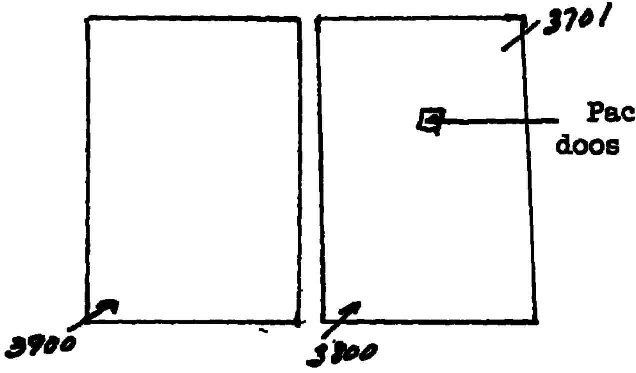
Come now to codes - function (1) Raw code

An example of a commercial code (2) Superenciphered

[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



Pack of running doos - "destruction"

68

FOR SLIDE 18

A highly specialized "commercial code"

[Call attention to 3-letter difference:

YGATA	-	COMA
YGKRO	-	Delirium TREMENS
YGCIB	-	CONSTIPATION
YGMAN	-	DIARRHEA

SLIDES 19-22

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 todgy.

20-Field codes in WW I - will show only one example in slides -- the German type of KRUSA code. Exhibits can be examined later.

SLIDE 20

One of th e 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.]

T^{W}o-part tactical code used by French Army in World War I. The code groups were then enciphered!

British Army Field Code, World War I

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

SLIDE 21

REF ID:A62878

An early AEF Code in World War I

[An indication of hów poorly prepared we were for COMSEC.]

74

LECTURE FOR SLIDE 24

One of the American field codes, World War I

/River series for the First Army; Lake Series for the Second Army/

SLIDE 14.1

"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.]

f76

LECTURE 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.]

77

[illegible]

Yardley and <u>THE AMERICAN BLACK CHAMBER.</u>

The demise of the ABC in 1929.

I take over from Yardley and establish SIS.

A complicated cryptographic system used by rum runners during Prohibition days.

[Mrs. Friedman's work in the Treasury and Coast Guard. Story re "Advise Andrew&s wife send Andrew spare glass eye." "You must have found that rummy all by yourself. Let me smell your breath". Next day - apology and explanantion.]

ESF and The Gordon Lim Case.

FOR SLIDE 149

The S.I.S. staff in 1935.

1. (Call attention to the vault door - when we worked in great secrecy.)

2. We study all kinds of cipher machines and I invent some.

A cipher machine of the 1920-30's period -

THE KRYHA.

The treatise on the KRYHA showing how many permutations and combinations it afford.

German Armed Forces cipher machine of World War II - A modification of THE ENIGMA

A printing model of the ENIGMA - never satisfactory.

German teleprinter ciphering machine.

The HAGELIN CX-52 machine.

But modern machines are electrical, high-speed, printing -- to suit the needs of modern high-speed electricl communications on a world-wide basis.

STOP

Read next card before showing next slide.

It would be nice if it were permissible for me to raise the secrecy curtain more fully than I already have, and tell you all about certain of the fascinating cryptologic exploits and episodes of WW I and WW II, with those of the intervening years, too. But you are certainly well aware of the limitations and restrictions which all governments, and ours included most certainly impose on work and activities and results obtained in this field.

Soon after V-J Day President Truman issued a memorandum which had the effect of an Executive Order. Here it is

The Truman Executive

Memorandum of 28 August 1945

The immediate or short-term purpose of this memorandum was to stave off, if possible, disclosures of a cryptologic import which were being called for by certain vociferous members of Congress who wanted to look into the Pearl Harbor disaster and try to find what skullduggery had been buried by the Democratic Administration--even by the President, the Chiefs of the Army, Navy, etc. But I'm sorry to say it didn't work at all well, as intended.

There were if you will recall a number of investigations into the Attack on Pearl Harbor, culminating in a long and expensive Joint Congressional Investigation which put out a 40-volume report on the subject. I'll read an extract or two from the main report itself.

Read from P.H. Report, various pages.

MARSHALL - DEWEY LETTERS

(Read from)

SLIDE 169

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 FOR SLIDE 131

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

High-speed testing is secret!

~~Earliest cryptanalytic devices at Riverbank Laboratories~~

96

The secrecy ban is great in this field that even our recently published book The Shakespearean Ciphers Examined had to be submitted by me for clearance by the authorities in the Pentagon. And even now I'm waiting--and have been waiting since last November--to have the answer to a question I raised about reprinting in a non-classified journal some things I wrote over 25 years ago, some of them anyhow; and as for writing for scientific journals such as the Scientific American, their request that I do a lengthy piece for them to be published at the end of 1958 or early in 1959 is still under consideration by the authorities. Secrecy is necessary of course, but I wonder if that much is really necessary.

I think it advisable not to say much more here. It is permissible to say that: modern cryptology is important and big business--it costs a great deal! No longer is the picture the average layman has of the cryptanalyst valid.

242

Section 798 of Title 50, USC

Thus far we have dealt with writings which fall in a category that may be described in general terms as writings in which the large majority of people see no secret or hidden messages; only a small minority claim to see or find cryptic texts in them. In these cases we may say that "normal" people don't see or can't find cryptograms in those books; those who say they do see and find such hidden texts are -- well, let's be fair and merely designate them as -- people with certain idiosyncrasies. Let's not say they're "abnormal" or "subnormal." Let's never forget that it was once "normal" to think that the earth is flat, "abnormal" to think it round.

With this prefatory remark I think it will be interesting to take a brief look at another category of writings, a category which has [illegible] we have been discussing. Here I ~~refer to the category~~ of writings of certain authors who claim their work is in plain text and is perfectly intelligible, but many or maybe most people find it unintelligible. Some, indeed, are uncharitable or ignorant, perhaps, and call the writings of these authors sheer nonsense or, worse, plain bunk, as exemplified in a rather well-known piece of doggerel ~~by one William Hines~~, which goes like this:

"There's a wonderful family named Stein,
 There's Gert, and there's Ep, and there's Ein;
  Gert's ~~poems~~ writings are bunk,
  Ep's statues are junk,
 And no one can understand Ein."

I am referring, of course, to what is generally called "modern literature", "modern verse", "modern art", "modern music", etc.

Here is an example from Gertrude Stein's writings (107.1), and here is one from E. E. Cummings ~~(S-52)~~ before, and after what Max Eastman ~~(I think it was)~~ called "an attack of punctuation" ~~(S-53)~~. Here it is in the "before" (S-52), which is almost intelligible on its face; and here it is in the form in which Cummings published the poem. (S-53.

PAUSE! DON'T CALL NEXT SLIDE!

At this point, at the risk of offending some of my listeners who I hope will be patient with me until I return to more serious comments, I want to show a couple of slides which were made from extracts from an anonymous article -- it could have been written, I suspect, only by James Thurber -- published about 25 years ago in the New Yorker. Before showing these two slides I must give a bit of explanation. It was in 1931 that a certain book was published by a very reputable and respectable American publishing house.

So far as I am aware, it is still the only book that cannot be republished or reprinted in this country because an Act of Congress, passed very hurriedly in 1933, forbids doing so. The book was written by one Herbert O. Yardley, who had worked in the government service in a very trusted capacity and had~~, through no fault of his own,~~ lost his job in 1929. This annoyed him excessively, in fact to a degree which caused him to write a book that purports to tell how messages of other governments were intercepted and read by him and his subordinates by cryptanalytic processes, and the book was published with the title The American Black Chamber. It created a sensation but that's all I can say about it here. A couple of years later came the article in the New Yorker with the title The Literary Black Chamber.

I show only two cases of successful treatment in The Literary Black Chamber. The first deals with one of Miss Stein's works and quotes a paragraph from it.

[Then read from slide S-31]

The next case deals with one of Mr. Cummings' poems entitled "Is 5."

[Point out briefly the work done in reducing to plain-code in the ABC Cable Code, Slide S-32.]

Well, that's enough of what may be amusing or unamusing satire on these two devotees of "modern literature." I wish now to return to serious consideration of that sort of literature in the light of what was said a few moments ago about writings in plain language and writings in secret language.

Now I don't exactly feel that the works of the "modernists" are actually cryptic in the sense of that word as it is used in cryptology; nevertheless, because their intelligibility is not patent to the eye or ear one could justify calling them cryptographic in a certain sense.

But first let me show a good example, one taken from the writings of the greatest of them all, James Joyce. Here is a tiny sample of Joyce's last and most important work, Finnegan's Wake (108). I show it in the form in which it was first published, as an installment of the book for which Joyce had as yet selected no title. We won't have the time to point out the meaning or meanings of this fragment even if I know them.

Lights On! ~~80~~ - 84

Let me confess at once that I don't know very much about this sort of cryptography. I've studied some of it casually and find that when the proper keys are used it becomes intelligible--its meaning or significance becomes clear, it has been reduced to plain language. But you generally have to work at the business, just as you do when you solve a cross-word puzzle, or better yet, a cipher. I'd like to read you a brief but interesting commentary by one of America's important literary critics and authors of "non-modern" writings, viz., Edmund B. Wilson, who says the following in regard to James Joyce's Finnegan's Wake:

"Today, when we are getting so many books in which the style is perfectly clear but the meaning non-existent or equivocal, it affords a certain satisfaction to read something that looks like nonsense on the surface but underneath makes perfect sense. Admirers of Balzac and Trollope think nothing of devoting years to reading their favorites through, and why should we grudge time to Joyce? The demands that he makes are considerable but the rewards he provides are astounding...It is an exciting, a unique experience to find pages that have seemed to us meaningless start into vivid life, full of energy, brilliance and passion."

Now I think that what Wilson says here is fair criticism and a succint appraisal of the phenomena involved. The point is, as I've hinted before, that a work of one of the "modernists" requires work on our part to decipher or decode it before its hidden meaning or real significance becomes clear. Some persons are dubious about the value of such work, both the work of the producer of the produce, i.e., the writer, and the work of the decipherer or the "reducer" of the product, i.e., the reader or listener. But let's be fair about this. Just as the mathematician, or the devotee of the game of chess or "go," of bridge or any other complex card game, engages in what is basically (leaving aside psychological factors) a mental activity of a rather high order and just as these persons derive great satisfaction and pleasure from reaching a solution or playing a good game of chess, etc., so does the cryptologist derive great satisfaction and pleasure from solving a cryptogram (leaving aside also in this case other factors such as the possible effect a solution may have on national defense); so also does the devotee derive satisfaction and pleasure from decoding or deciphering words of the "modernists."

In bringing my rather lengthy talk to a close, I may summarize or tie up in one neat bundle about all I've said by closing with these comments: First, we've found no valid ciphers in the Shakespeare Plays which state that Bacon or anybody else wrote them. Second, it takes work and sometimes hard work to solve a complex problem in mathematics, or in cryptography, or in "modern literature." Third, that the pleasure one derives from reaching a valid solution is often in itself sufficient recompense for the work done; but sometimes the pleasure is accompanied also by a sense of unending satisfaction if the solution turns out to be something of great value or importance in any field of endeavor that makes high achievement in our civilization worth while.