

~~SECRET~~

*First Period*

[ 34 slides used in modified presentation on 26 April 1960 ]

~~SECRET~~

SLIDES FOR FIRST PERIOD(Total 34 used 26 Apr 60  
Talk USMC)

<u>PAGE</u>	<u>SLIDE NO.</u>	<u>TITLE</u>
	✓ 1	Bible
6	✓ 2	Scytale
	✓ 4.10	Alphabet of 1401
7	✓ 245.2	Trithemius (put in 2 <sup>nd</sup> period)
	✓ 151	Trithemius Oath
	✓ 242	Sect. 798 of Espionage Law
	✓ 5	Vigenere Square
8	✓ 5.2	Cipher of Phillip II
9	✓ 6.21	Jefferson decode
	✓ 6.31	Jefferson encode
	✓ 6.4	Benedict Arnold
10	6.5	Benedict Arnold
	6.6	Benedict Arnold
12	✓ 7	Confederate cipher device
13	✓ 8	Lincoln Message
	× 152	W. Wilson message
	× 152.1	W. Wilson message encoded by Mrs. Wilson
	× 152.2	W. Wilson message as sent
	✓ 9	Route Cipher - Federal Army
14	✓ 10	Grant cipher
	✓ 214	Gregory Code 1885
15	✓ 215	Gregory Code
	× Roosevelt 1	
	× " 2	
	× " 3	
16	✓ 212	Hitt's manual
17	✓ 28	Zimmermann Telegram (code)
18	× 28.1	Nigel De Grey
	✓ 29	Zimmermann Telegram plain text
19	✓ 33	Hindu
20	✓ 34	Hindu
	✓ 82	Riverbank Class - Knowledge is Power
21	✓ 11	Russian Cipher 1916, WW I
	✓ 12	French Cipher WW I
	✓ 13	Italian Cipher
	✓ 14	German ADFGVX
22	✓ 15	T/A WW I
	✓ 14.1	Special Code Section Report
23	✓ 23	PLAYFAIR CIPHER
	✓ 213	Mauborgne's paper on PLAYFAIR
	× 16	W. U. Code
24	× 18	Specialized Code
25	✓ 21	Baseball code
26	219	Navy NCB

In inviting me to address the staff and students of the Senior School of the Marine Corps on the subject of "Communications Intelligence and Communication Security" I assume that the objective is to make you aware of the roles that these two branches of the science of cryptology have played as vital military weapons in the past and may in the future again play.

Soon after the close of World War II, service schools began to ask for lecturers to tell their student officers something about our cryptologic activities during the war. There was at first serious question as to the advisability of lifting the security veil sufficiently to permit discussion of the subject, but in time an affirmative decision was made. The official views of the Naval War College on the matter were stated in a letter dated 5 February 1946, and because the letter admirably states those views I shall read two paragraphs of it.<sup>1</sup> In commenting upon the fine presentation made by a certain

---

<sup>1</sup> From the then President of the College, Admiral R. A. Spruance, to the Chief of Naval Communications, Admiral E. E. Stone.

---

speaker, the letter said:

*Quote* "His treatment of the subject matter emphasized the value of communication intelligence to naval commanders, the vital importance of maintaining the security of our own communication intelligence activities, and the necessity for observing the principles of communication security in defense against enemy communication intelligence. I consider that the value to be derived from the indoctrination of senior officers of the Navy in these principles far outweighs any possible loss of security resulting from a partial revelation of our activities in the past war, particularly in view of the disclosures which have been made in the press.



~~SECRET~~

contended that the truth could no longer be hushed up or held back because of

an alleged continuing need for military secrecy, <sup>They called for a real investigation,</sup> because ~~the war was over.~~

<sup>saying that although</sup>

there had been investigations--a half dozen or more of them--<sup>they wanted, as</sup> and now there was

<sup>as</sup> a grand finale, <sup>a</sup> Joint Congressional Investigation, <sup>They finally got what they demanded,</sup> which ~~not only would~~

<sup>The hearings disclosed many secret and top secret facts, and they also disclosed</sup> ~~itself bring into the open every detail and exhibit uncovered by its own~~

~~lengthy hearings but would also disclose to America and to the whole world~~

everything that had been said and shown at all the previous Army and Navy

investigations. <sup>Congressional</sup> The hearings made headline copy for all our newspapers.

There came a day in <sup>those</sup> the Congressional Hearings when the Chief of Staff of

the U.S. Army at the time of the Pearl Harbor Attack, 5-star General George C.

Marshall, was called to the witness stand. He testified for <sup>many hours spread over many</sup> several long, long

days. Toward the end of his ordeal <sup>General Marshall</sup> he was questioned about a letter ~~it had been~~

~~rumored~~ he'd written to Governor Dewey ~~in the Autumn of 1944~~, during the <sup>heat of the</sup> 1944

Presidential Campaign. General Marshall ~~talked.~~ He pleaded long and most

earnestly with the Committee not to force him to disclose the letter or its

contents, because <sup>he said, there was still a</sup> necessity for continued secrecy about code matters, but his <sup>pleas were</sup>

<sup>of</sup> no avail. He had to bow to the will of the majority of the Committee. I

now read from TIME:

Quote "U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which cryptographers painstakingly constructed in a hidden room, at Fort Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers had duplicated the decoding devices used in Tokyo. Testimony

~~SECRET~~

~~SECRET~~

before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it ~~(TIME--Dec--10)~~. Now General Marshall continued the story of 'Magic's' magic. It had:

1. "Enabled a relatively small U.S. force to intercept a Jap invasion fleet, win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand.
  2. "Given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled the Navy to concentrate ships which otherwise might have been 3,000 miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.
  3. "Directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.
  4. "By decoding messages from Japan's Ambassador Oshima in Berlin, often reporting interviews with Hitler, it had given our forces invaluable information on German war plans." ! ! . . .
- ~~TIME goes on to give more details of that story, to which we shall return.~~

It is hardly necessary to tell you how carefully Magic was guarded before, during, and after the war. It is still very carefully guarded. Even the fact of its existence was known to only a very few persons at the time of Pearl Harbor--<sup>and that fact</sup> that is an important element in any attempt to explain why we were caught by surprise.

~~TIME says, in connection with this phase of the story of Magic during~~

~~World War II:~~

"So priceless a possession was Magic that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, (and) force U.S. cryptographers to start all over again."

*Unquote*

~~SECRET~~

Now I don't want to ~~seem to~~ over-emphasize the importance of COMINT in the disaster but as for its importance during World War II I do want Pearl Harbor ~~affair but I must not fail~~ to tell you ~~what~~ General Chamberlin,

<sup>General</sup> who was MacArthur's G-3 throughout the war in the Pacific, has written: <sup>about it. Quote</sup> "The

information G-2 gave G-3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." <sup>Unquote</sup> We can't put a

dollar-and-cents value on what our possession of COMINT meant in the way of saving lives; but we can make a dollar-and-cents estimate of what COMINT meant

by shortening the war by two years. <sup>A rough calculation tells us that each dollar</sup> ~~I made a calculation and found that \$1.00~~

spent for COMINT <sup>was</sup> ~~is~~ worth \$1,000 spent for other military activities, ~~and [materials]~~

In short, when our commanders had COMINT in World War II they were able to put what small forces they had at the right place, <sup>and</sup> at the right time. But when they didn't have it--and this happened, too,--their forces often took a beating.

I hope I've not tried your patience by such a lengthy preface to the real substance of my talk, so let's <sup>begin with a bit of background on</sup> ~~get down to brass tacks, and since a bit~~ of history is always useful in introducing a subject belonging to a special and not so well-known field, I'll begin by giving you some historical information about cryptology, which comprises two related sciences, namely cryptography, and cryptanalysis. They are but opposite faces of the same very valuable coin, <sup>because</sup> ~~for~~ progress in one inevitably leads to progress in the other.

~~If time permitted~~ we could go far back into history to see the earliest beginnings of secret communications and this might take us to the very dawn of the art of writing because there is room to wonder which came first, ~~ordinary,~~

~~SECRET~~

intelligible writing or unintelligible, <sup>that is,</sup> secret writing. Instances of cipher  
 are found in the Bible, <sup>as this slide shows.</sup> ~~but we must pass over the history of the~~

~~early days of cryptology with the foregoing single mention.~~ There is, however,

And here's one historical item that

~~one item in that history which~~ is worthy of special notice, the scytale, which

<sup>It's</sup> the earliest cipher device history records, ~~and which~~ <sup>It</sup> was used by the ancient

- (2) ~~Phoenicians~~ or Greeks for military secrecy. They had a wooden cylinder of specific dimensions, around which they wrapped spirally a piece of parchment; they then wrote the message across the edges of the parchment, unwound it, and sent it to its destination by courier, where the recipient would wind the parchment around an identically-dimensioned cylinder, and thus bring together properly the bits of letters <sup>of</sup> representing the message. <sup>It is interesting to note that the</sup> ~~And, by the way,~~ the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.

It is well known that Julius Caesar used cryptography--a very simple method--because all he did was to replace each letter by the one that was fourth from it in the alphabet.

The beginnings of modern cryptology can be traced back to the <sup>early</sup> days of the princes and chanceries of the Papal states, beginning even before the year

- (4.10) 1300. <sup>Here's</sup> ~~I show next~~ an alphabet of that period. It is interesting because it shows that even in those early days <sup>there already was</sup> ~~they already had~~ a recognition of the basic weakness of what we call single or monoalphabetic substitution. Solution of this type of cipher, as you all know, is accomplished by taking advantage of the fact

~~SECRET~~

~~SECRET~~

that the letters, <sup>in alphabetic</sup> ~~of the alphabet in~~ languages are used with greatly differing

(4.10) frequencies. This slide shows that the early Italian cryptographers understood this fact and introduced stumbling blocks to solution by having the high-frequency letters represented by more than a single character. I will add that the earliest

tract that the world possesses on the subject of <sup>cryptology</sup> ~~cryptology~~, or for that matter,

~~cryptanalysis~~, is that ~~which was~~ written in 1474 by a Neapolitan, <sup>named</sup> ~~whose name~~

~~was~~ Sicco Simonetta. He sets forth the principles and methods of solving

ciphers in a very clear and concise form. The first ~~book or~~ extensive treatise

(245.2) on cryptography is that by a German abbot named Trithemius, who wrote his

monumental work in 1531. He planned to write four volumes, but he quit with

the third because he wrote so obscurely and made such fantastic claims that he

~~was~~ <sup>in fact, and his very</sup> ~~got~~ charged with being in league with the Devil. They burned his books, ~~as a~~ <sup>of something from Trithemius</sup>

(151) <sup>life was in jeopardy.</sup> ~~matter of fact.~~ This may be a good place to present a slide, which shows that

<sup>cryptology</sup> the necessity for secrecy in ~~this business~~ was recognized from the very earliest

(242) days of <sup>the science.</sup> ~~cryptology~~. We put teeth <sup>own</sup> in our ~~own~~ somewhat similar oath, and here are the teeth.

(5) The next slide I show is a picture of what cryptographers usually call the

<sup>by means of which polyalphabetic ciphers can be prepared.</sup> The square comprises Vigenere Square, ~~or Vigenere Table~~, a set of twenty-six alphabets successively

displaced one letter per row; <sup>are</sup> ~~with~~ the plain-text letters <sup>at</sup> the top of the

square, the key-letters at the side, and the cipher letters inside. The method

of using the table is to agree upon a key word, which causes the <sup>cipher</sup> ~~the~~ equivalents of

the plain-text letters to change according to the row designated by the key

letters. ~~Now, Vigenere also has an interest to the professional cryptologist~~

~~because although he~~ <sup>Vigenere described his square in 1586 and</sup> ~~is commonly credited with having invented that square~~ <sup>it, but he</sup> ~~he~~

~~SECRET~~

~~SECRET~~

really didn't and, what's more, never said he did. <sup>1586.</sup> It was invented much earlier than

The next cryptographer I wish to mention is <sup>also</sup> a Frenchman, François Vieta, an eminent mathematician, <sup>and</sup> founder of modern algebra. In 1589, <sup>when he was</sup> he became Councillor of Parliament at Tours and then Privy Councillor, ~~while in that job~~ he solved a Spanish cipher system using more than 500 characters, so that all the Spanish dispatches falling into French hands were easily read. <sup>When</sup> Phillip II of Spain, <sup>who was</sup> ~~was so~~ <sup>absolutely</sup> convinced of the safety of his cipher, ~~that when he~~ learned that the French were aware of the contents of his <sup>cipher dispatches</sup> ~~letters~~ to the Netherlands, he complained to

(5.2) the <sup>Pope</sup> ~~people~~ that the French were using sorcery against him. Here's a slide that shows one of the hundreds of ciphers the Court of Spain was then using. Vieta was called on the carpet and made to explain how he'd solved the ciphers.

I want to jump now to the period of the American Revolution, <sup>Believe it or not,</sup> ~~in U.S. history.~~

The ~~cipher~~ systems used by the Americans and by the British, ~~as well as the code systems,~~ were almost identical! In one case, in fact, they used the same dictionary as a code book!

For additional security conventional words were used to represent the names

of persons and places. <sup>Here are some of the code names used by the British:</sup> ~~The British used the following code names:~~

American Generals - Names of the Apostles: Washington - James  
Sullivan - Matthew  
etc.

Names of Cities - Philadelphia - Jerusalem  
Detroit - Alexandria

Names of Bays  
& Rivers - Delaware - Red Sea  
Susquehanna - Jordan

Indians - Pharisees  
Congress - Synagogue

~~SECRET~~

There was an American who seems to have been the Revolution's one-man NSA, for he was the cipher expert to Congress, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages intercepted by the Americans. Of course, the only way in which enemy messages could be obtained in those days was to seize couriers, ~~knock them out or off,~~ and take the messages from them. Rough stuff compared to getting the material by radio intercept.

(6.31) The next <sup>slide</sup> ~~chart~~ shows a picture of a code or "syllabary", as we call it, used by Thomas Jefferson. This syllabary is constructed on the so-called two-part principle. ~~This is a portion of the decoding section.~~ You will note that the

numerical groups are <sup>not</sup> in consecutive order, but ~~their meanings are in no~~ alphabetical order at all, which means that you have to have <sup>a decoding</sup> ~~another~~ section,

(6.21) ~~the encoding section,~~ in which the <sup>code numbers are in numerical order, their</sup> ~~words are in alphabetical order, and their~~ meanings ~~equivalents~~ are in random order. This sort of system, even today, is in extensive ~~use,~~ but with larger vocabularies.

~~use,~~ Jefferson was an all-round genius, and I shall have something to say about him and cryptography a little bit later.

~~sure~~ You've <sup>all</sup> learned as school children ~~all~~ about Benedict Arnold <sup>and what he tried to do</sup> when

he was ~~the~~ Commanding General of ~~the American Forces~~ at West Point; but you probably don't know that ~~practically all~~ his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were in cipher, or in invisible inks. Here's an interesting slide showing one of Arnold's cipher

<sup>And here's the plain text,</sup> messages, <sup>in</sup> which he offers to give up West

6.5 Point for £20,000. Here's another one in which he gave the British information  
6.6 which might have led to the capture of ~~his commander-in-chief~~, General  
Washington--but Washington was too smart to be ambushed--he went by a route  
other than the one he said he'd take.

I think you'll be interested to hear a bit more about that one-man NSA  
I mentioned a couple of moments ago. His name was James Lovell, and besides  
being a self-trained cryptologist <sup>he</sup> ~~was~~ was also a member of the Continental  
Congress. There's on record a very interesting letter which he wrote to  
General Nathaniel Greene, with a copy to General Washington. *I'll read it to you.*  
*Here it is.*

Philadelphia, Sept. 21, 1780

Sir:

You once sent some papers to Congress which no one about you could  
decipher. 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 Enemy make only such changes in their Cypher when  
they meet with misfortune, ~~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

~~In telling you about Lovell I should add to my account of that interesting~~  
~~era in cryptologic history, an episode I learned about only recently. When a~~  
~~certain message of the revolutionists came into Clinton's possession he sent~~

~~SECRET~~

it off post haste to London for solution. ~~But~~ Of course, Clinton knew it was going to take a lot of time for the message to get to London, he solved and returned to America--and he couldn't afford to wait that long. Now it happened that in his command there were a couple of officers who fancied themselves cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry, <sup>who</sup> ~~their solution~~ and he acted upon it, <sup>with disastrous results to his forces,</sup> ~~the operation~~ turned out to be a dismal failure, because the solution Clinton acted upon was all wrong! The record doesn't say what Clinton did to the two amateur cryptologists when the correct solution arrived from London weeks later. By the way, you may be interested in learning that the British have operated a cryptanalytic bureau ever since the year 1540, save for a few years about 1850 to 1914.

There's ~~also~~ <sup>which</sup> an episode I learned about only very recently, <sup>and</sup> which is so amusing I ~~ought~~ <sup>must</sup> to share it with you. It seems that a certain British secret agent in America was sent a <sup>letter</sup> ~~message~~ in plain English, giving him <sup>certain</sup> instructions. But the poor fellow was illiterate and had to call upon the good offices of a friend to read it to him. What he didn't know, however, was that his friend was one of General Washington's <sup>own</sup> secret agents!

*Omit*  
 If interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe. Books on the subject were written and studied. Here's a picture of the frontispiece to a book in French published in 1790, dealing with espionage and counter-espionage; it has a section dealing with cryptology.

*Perhaps*  
~~I had intended to say~~ a few words about the decipherment of Egyptian hieroglyphic writing <sup>will be of interest</sup> because it is supposed to represent the next and a great landmark in the history of cryptology. Professor Norbert Wiener, of M.I.T., in his famous book entitled Cybernetics calls that decipherment the greatest feat in the history of cryptology, but <sup>good</sup> the professor is wrong. The cryptanalysis was rather simple; the difficult part was the reconstruction of the language and its grammar. I'm sorry we can't go into that now, but I do want to add that it was very fortunate that the early students of Egyptology didn't even suspect that the Egyptians also used cryptography, <sup>because, as I mentioned a few moments ago,</sup> there were cryptographic hieroglyphics, ~~if you can imagine such things.~~

~~There is one person I should mention before coming to the period of our~~  
 I must mention <sup>who</sup> Edgar Allan Poe, in 1842 or thereabouts, kindled an interest in cryptography by his famous story of "The Gold Bug", and by some articles on cryptography in newspapers and journals of the period. For his day he was <sup>perhaps</sup> the best informed person in the U.S. on cryptologic matters, <sup>though most of his source material came out of an encyclopedia.</sup>

The period of the Civil War or the "War Between the States", in U.S. history was, as a result of the invention and development of telegraphy, a <sup>in which</sup> period ~~that~~ <sup>was very important.</sup> saw the use of cryptology in a large way. Here is a picture of a Confederate cipher device, captured at Vicksburg. The device is a cylinder ~~of wood, covered with a sheet of paper bearing alphabets, the alphabets of the Vigenere table, in other words, Here is a~~ <sup>of wood, covered with a sheet of paper bearing alphabets, the alphabets of the Vigenere table, in other words, Here is a</sup> ~~knob~~ <sup>knob</sup> pointer that you could slide, and a ~~with which~~ <sup>with which</sup> you could turn the cylinder according to the key letters. You might like to know two of the keys

they used with this ~~system and~~ device: COMPLETE VICTORY was the first; <sup>the second was</sup> ~~and~~ <sup>the second was</sup>

COME RETRIBUTION, ~~the second.~~

Here is a <sup>message</sup> ~~picture of a~~ message, authentic without question, which was

8 sent by President Lincoln to General Burnside. <sup>If you read it as we normally do</sup> ~~It is very simple. It reads this~~

way, of course, <sup>it</sup> ~~and~~ makes no sense; but if you read it backwards it makes

excellent sense: "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." I think the President was kidding a bit,

but he may have lacked confidence in the official cryptosystems in the same

<sup>during World War I</sup> way that <sup>in</sup> President Wilson lacked confidence in <sup>the</sup> codes of the State Depart-

ment, ~~as can be seen in the slides which I now show.~~

152/  
152/1  
152/2  
-----  
-----  
-----

9

This is a photograph of a page or two from the code book and cipher system

used by the Federal Army. They had what we call "route ciphers", that is, they

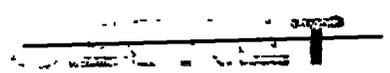
used <sup>diagrams of various dimensions and there were</sup> ~~a matrix with~~ indications of the route to be followed in inscribing and

transcribing the words of the message. Here's how you write the message in:

the first word, second, third, fourth, fifth, sixth and so forth; then you

take them out according to another route. And here the thing is complicated

by the use of arbitrary equivalents for the names of important people.



~~SECRET~~

"President of the U.S." is represented by "Adam" or "Asia". It had two equivalents, you see. Here are some of the names of famous or well-known officers of that period. I have with me today the complete set of cipher books used by the Federal Army during that period. The next slide is a picture of a message sent to General Grant in one of those route ciphers. I shall not take time to read it.

After the Civil War, ~~or War Between the States~~, the use of cryptography in United States military affairs went into a decline, because there was a long period of peace, broken only briefly by the Spanish-American War. In 1885 the War Department published a code called "Code to Insure Secrecy of Telegrams". It is a cryptographic curiosity and ~~no tribute to the imagination of~~ <sup>because</sup> the officer who was responsible for its production, ~~because he~~ copied almost word for word the title page, the instructions for use, and the arrangement of contents from

~~SECRET~~

~~SECRET~~

Here's a

a commercial code. ~~a picture of which I show in this slide~~ in which pages of

215 both codes are placed side by side for your inspection. But good old Lieut.

Colonel Gregory did have a little spark of imagination. See what he changed

(here point out the minor differences). ~~But believe it or not~~ This was the

code that <sup>our</sup> ~~the~~ Army used during the Spanish-American War and in the copy ~~we~~

*I've brought with me there appears,*

~~my collection,~~ on the inside of the front cover, ~~there appears~~ the additive

that was used: 777. ~~I have that copy among my exhibits here.~~ ~~██████████~~

~~There was little use for sound cryptosystems then because radio was just in~~

~~its infancy during that war and there wasn't much danger from interception of~~

~~messages.~~

~~(The Navy Code in the Spanish American war. If there's time.)~~

In 1899 the Chief Signal Officer undertook the preparation of a suitable

<sup>for the Army</sup> code. Economy was stressed--the Chief Signal Officer personally did all the

work--and in 1902 the "Cipher of the War Department" was published by the

Adjutant General. In 1906 a revision of that book was published, and in 1915

a completely new code, the War Department Telegraph Code, was published. But,

believe it or not, that code was printed by a commercial ~~house~~ <sup>printer</sup> in Cleveland!

At least that is what my predecessor in the Office of the Chief Signal Officer

told me when I took over from him ~~in January~~ 1921, after my World War I service.

~~in France.~~

*During*

~~When~~ World War I ~~came in August 1914~~ cryptology entered upon a new and

rapid expansion in invention and development, ~~and we must now turn our attention~~

~~to the principal events in that expansion and development.~~ With Hertz's

~~SECRET~~

discovery of the so-called Hertzian waves, and Marconi's practical demonstration of signalling by wireless, a new era in military communications <sup>began</sup> ~~was ushered in,~~

and this, of course, was what brought about renewed interest and a new era in

<sup>military</sup> cryptology. The first ~~use~~ <sup>usage</sup> of wireless, or radio, as it soon came to be

~~referred to as radio cryptology~~ called in American terminology, was made in Europe before 1914 but wide usage

<sup>began only.</sup> ~~of it~~ <sup>This brought new</sup> developments in cryptography, ~~logged a bit,~~ <sup>as we shall</sup>

Before coming to these developments a few words should be said about the

U.S. position vis a vis the Allies and the Central Powers. ~~Some of you will remember~~

how President Wilson ~~strove and~~ promised to keep the U.S. out of the war, how

at one time during a period of strained relations with both sides he'd declared

<sup>, never, never</sup> that he'd never send our boys to war, <sup>He also said</sup> and that there was such a thing as being

<sup>a thesis I'll not try to defend.</sup> too proud to fight, <sup>U.S. sympathies for the most part were with the Allies,</sup>

especially the British, but there were in the U.S. <sup>millions of people who were against</sup> ~~hundreds of thousands of~~

~~German-Americans and German sympathizers, and all these Americans exercised~~

~~an important role in helping to prevent our entry into the war on either side,~~ <sup>for</sup>

~~at least of all on the side of the Allies.~~ The British tried their best not

~~to provoke or irritate the U.S. but even so~~ there were times when British high-

<sup>on the side of Germany.</sup> handed action almost precipitated us into the war <sup>against them.</sup> There were

<sup>minor</sup> some activities toward preparedness and national defense in case circumstances

~~made our entry into the war unavoidable, but these activities weren't of much~~

<sup>but.</sup> ~~account.~~ In the cryptologic field, <sup>nothing little</sup> ~~for example,~~ was being done by

<sup>officially.</sup> either the Army or the Navy, <sup>American</sup> Two Army officers became interested in the subject

and I show you the title page of the first manual on military ciphers, by the

~~SECRET~~

~~Book~~ then Captain Parker Hitt, ~~and the title page of a small brochure by the then~~

~~VAN~~ Lieut. J. O. Mauborgne. <sup>this was a</sup> But ~~these~~ were almost private ventures. Officially,

as regards cryptographic preparations, no new codes were in preparation in

either Service; no new ciphers were being dreamed up; no cipher devices or

cipher machines were being investigated or invented. As for cryptanalytic

operations--well, there just were none whatever in either Service, and, for that

matter, in the whole government. <sup>At</sup> a private research institution near Chicago,

the Riverbank Laboratories, of which I happened to be a member, working in a

totally different field of science, <sup>certain of us</sup> began studying cryptology and soon <sup>we began</sup> ~~obtain~~

~~members of the staff were~~ working on messages which were <sup>sent</sup> ~~furnished~~ us by various

government departments and agencies in Washington. Most of these were solved

and returned to Washington, and <sup>my</sup> ~~the~~ staff became more and more adept. But,

mind you, this was not even a quasi-governmental agency. It was operated as a

patriotic gesture and at his own expense by the man who, in 1915-16, as an

<sup>[Kentucky variety]</sup> astute and wealthy business-man, Colonel George Fabyan, foresaw the inevitable

<sup>and he saw that the U.S. was</sup> entry of the U.S. into the war, wholly unprepared for any cryptologic work.

The Colonel was right. ~~on~~ On 6 April 1917 the U.S., almost suddenly it seemed,

declared war on Germany. How did this come about? It came about when it did

as a result of a nice piece of cryptanalytic work by British cryptanalytic

experts in London on a message now world-famous as the Zimmermann Telegram.

The message ~~first~~ came from the German Foreign Minister in Berlin, <sup>[Arthur</sup>

~~Zimmermann]~~ <sup>who</sup> to the German Ambassador in Washington, <sup>Count von Bernstorff]</sup> ~~it was~~

28 then sent on to the German Minister in Mexico City. Here's the message in the

~~SECRET~~

SECRET

form in which it was transmitted to Mexico. I won't go into the story about how

(29)

*but here's a translation of it. As you can see,*  
 the British solved it, ~~for this was dramatic and complex, because it involved~~

~~the reconstruction of two rather large codes. The solution represented a~~

~~first class piece of work. But I do want to add a few words about the political~~

~~effects of the solution, and about British cleverness in the handling of the~~

~~case because it gives a good illustration of how astute, diplomatically, they are.~~

~~As I have already said, ~~it~~ resulted in bringing us into the war on their side.~~

*See* Here is the translation of the Z. T. It was important because ~~the message said~~

the Germans were going to resume unrestricted submarine warfare and ~~this~~ *but* part,

here, dealing with a proposal to be made to Mexico, was the straw that broke the

Far and the camel's back. People in the Middle West had been very lukewarm toward the idea

*largely because it was a war that was thousands of miles away.*  
 of our getting into the War--on either side--~~But~~ when the Germans began talking

about returning Texas, New Mexico and Arizona to Mexico, that was something else

again. So, we got into the war within a couple of weeks after the British gave

*the Zimmermann Telegram*

us, and we had established ~~the~~ *its* authenticity of ~~the translation of the Zimmermann~~

~~Telegram.~~ *the whole* A year or so ago the telegram and episode was the subject of one of

*books* most dramatic episodes in

the ~~series of~~ Walter Cronkite's "You Are There" television programs. And a book

of almost 250 pages, dealing only with that telegram and episode, was published

*a year in our country and just a few months ago in England.*  
 just about ~~six weeks ago. I brought a copy with me.~~

Well, ~~as I said a few minutes ago,~~ on 6 April 1917 we were in the war as

*all over the U.S., including*  
 belligerents and things began popping, ~~especially~~ in my own little world at

Riverbank Laboratories. We began training more people and doing more solution

*solved many*  
 work--all paid for by Colonel Fabyan. We had ~~to solve~~ messages ~~to solve~~ that dealt with

~~SECRET~~*our then not very friendly*

~~our~~ neighbor on our southern border, as well as messages that dealt with the activities of enemy agents.

*omit if not kind*

There was one rather interesting case, in which I happened to play a minor role. In 1916 ~~the~~ the Germans financed a large number of Hindus ~~in their~~ ~~attempts~~ to stir up a rebellion in India, the idea being to cause so much trouble ~~in India~~ that the British would be forced to withdraw troops from the Western Front to quell disturbances in India. These Hindus were <sup>to</sup> negotiating ~~for the~~ purchase of arms and ammunition in the United States, with the idea of sending them over to India. Since the U.S. was neutral, it was against our own laws to permit such undertakings ~~against a friendly nation~~. <sup>naturally</sup> The business had to be conducted secretly, and that is how cryptograms entered into the picture.

33

Here is one page of a long, ~~seven or eight page~~ letter that was intercepted <sup>passing</sup> between the top Hindu agent in the United States and his chief in Switzerland. The letter consisted of groups of figures, in which were interspersed some plain-text words. We recognized pretty quickly that the letters of the secret text had been replaced by numbers which indicated specific letters in some ordinary book <sup>that</sup> ~~which~~ could be carried by an agent without arousing suspicion. Each group of numbers represented the page number, the line number, and the position number in the line of that key book. All we needed was the book, but unfortunately the Hindu failed to tell in his letter what the book was, so we had to go ahead and try to solve the message without it. It was solved, but there isn't time to tell you how it was done except to say that by working back and forth between the message and the hypothetical keybook, building up the various words on various

~~SECRET~~

~~SECRET~~

~~might be: by working back and forth, building up the various words on various~~

pages of the book, then building up the words of the message--one helped the

34

other--I finally got certain clues as to the sort of book involved--that it

was a book dealing with the history of German political philosophy, economy,

or history. I hunted and hunted ~~and hunted~~ and finally found it,

all right. It was Price Collier's Germany and the Germans. This message

figured in a long-drawn out trial in San Francisco, where there were about a

hundred ~~of the~~ Hindus on trial simultaneously. ~~Some of the Hindus turned~~

~~State's evidence and got himself involved with the others~~ They were searched

every day before they came into court, but one day, the day after I testified,

one Hindu managed to secrete a gun in his clothes and in the midst of the court

proceedings shot <sup>a</sup> ~~the~~ Hindu who had turned State's evidence, whereupon the

United States marshall, a great big fellow, six feet four, standing in the

back of the court, drew his weapon and shot the first Hindu dead. They were

both dead right there, within <sup>ten</sup> ~~two or three~~ seconds. ~~That's the way that~~

trial ended up / rather dramatically, I'd say.

To go back to the work at the Riverbank Laboratories, ~~and then~~ the Adjutant General began sending us officers for training.

82

Here's a picture of one class, the biggest and the last one I directed before

being commissioned and going directly to France, for service at GHQ, <sup>to</sup> working.

That picture spells out a message in cipher: KNOWLEDGE IS POWER. on German codes and ciphers. / And now for a quick-look at the sort of things

~~found there and was assigned to work at~~  
I found at GHQ when I got there and was assigned to work.

Let's first take a look at <sup>some of the military cryptosystems used by the</sup> ~~and discuss the use of cipher systems by the~~

~~SECRET~~

various belligerents, ~~because these were used for tactical purposes in preference~~

11 ~~to codes and code systems, which came as a later development.~~ Here's a picture

of the cipher system used <sup>or rather</sup> ~~and~~ misused by the Russians. ~~You will note that~~ It

was based upon the old Vigenere principle, using numbers instead of letters. ~~It~~

~~represents a case involving only a set of 7 or 8 alphabets used repetitively, by~~

~~a key number, for substitution. This was the deciphering table. Russian ineptitude~~

~~in communications, and especially in cryptography, cost them dearly, because of~~

~~for they lost the Battle of Tannenberg, <sup>in which they lost</sup> which greatly contributed to their being~~

12 knocked out of the war. The next slide <sup>shows</sup> ~~is a picture of~~ a tactical cipher system

used by the French. It was a transposition system, the columns being here

transcribed according to the columnar key; in addition, certain disturbing

elements came into the method by taking off the letters in diagonals. And here

13 is a picture of the system used by the Italian Army in World War I. Again, it

is only a variation of the old Vigenere system. Here is a system used by the

Germans, beginning in the latter part of 1917. It was invented by them, or, I

should say, they invented a clever combination of two methods. We called it the

14 ADFGVX cipher because the cipher text consisted exclusively of those letters. An

<sup>of 25 letters was written in this 5 by 5 square,</sup>  
~~alphabet, in here, arranged~~ according to some pre-arranged plan, with the coordinates

ADFGVX; the letters of the message were replaced by pairs of coordinates; for

example, the letter R is represented by AG, and so forth. The whole message is

written out in the letters ADFGVX in a transposition diagram at the top of which

is a key, developed from a key word; the letters are then taken out of the diagram

in columnar fashion, according to the key order. That system was a brand new thing in military cryptography and caused no end of headaches for the Allied cryptanalysts until it was discovered just how a solution could be achieved. The solution was not a general one but depended upon special cases; however, these happened so often that we could bank on them occurring practically every day. The ADFGVX system was used by the German high command and it wasn't long before it was discovered that if you made a study of <sup>only</sup> ~~just~~ the number and direction of ADFGVX messages you could infer certain things about the tactical situation and, more important, you could, with some degree of assurance, predict what might happen

15

in three or four days at a certain sector of the front. Here is an example of a chart based upon the ADFGVX intercepts. This, gentlemen, <sup>represents an early, if not</sup> ~~is~~ the first illustration ~~that I know of~~ in history of one of the basic principles of what we call traffic

14.1

analysis and traffic intelligence. (Explain chart.) The next slide gives a picture of the sort of "Bulletins", as we called them, that we put out when the ADFGVX messages were read.

For tactical messages the British and Americans <sup>employed a</sup> ~~in World War I used a~~ method known as the Playfair Cipher, <sup>which also uses a 5 by 5 square by</sup> ~~allegedly invented by Lord Playfair, but he~~ means of which, <sup>not single letters, but pairs of letters are enciphered.</sup> ~~didn't invent it. Sir Charles Wheatstone invented it.~~

~~SECRET~~

23

~~method of Playfair encipherment is to have a square 5 x 5, or 25 cells in~~

~~all, in which you start in with a key word, then follow with the rest of the~~

~~unused letters of the alphabet. (I and J are treated as the same letter). If~~

*For example,*

*if* you want to encipher "AT" the equivalent is "VR", by diagonals, and so on.

Here is an example of how a message is enciphered. In those days <sup>*the Playfair Cipher*</sup> ~~1914~~ <sup>*that*</sup>

was regarded as pretty hot stuff. In fact, an officer of the American Army, <sup>*then*</sup>

Lieut. Mauborgne, <sup>*who*</sup> ~~whom I've already mentioned and who~~  
~~later became Chief Signal Officer, ~~Major General~~ wrote a little~~

213

treatise, published in 1914, <sup>*it under the title*</sup> in which he dealt with ~~this Playfair cipher system.~~

~~The title of his work is~~ "An Advanced Problem in Cryptography". Today, our

most elementary students are given things of that sort to solve after <sup>*only*</sup> a few

lessons.

The British Army developed a cipher device in World War I, They had

manufactured a great many of them, thousands in fact, and they proposed to

the French and the Americans that all the Allies should use it for tactical

communications; but <sup>*for reasons that I'll tell you in the last period the device*</sup> ~~to the chagrin of the British~~ it was never put to use. ~~For~~

~~None of the belligerents in World War I used a cipher device or machine.~~ <sup>*reasons that I will tell you later.*</sup>

~~reasons that I will tell you later.~~

So much for the <sup>*military*</sup> ~~cipher~~ cipher systems ~~used~~ in World War I. Now,

I'd like to say a few words about the codes and code systems. A code is

simply a sort of dictionary in which the words, phrases and sentences are <sup>*replaced*</sup>

~~represented~~ by arbitrary groups of letters or figures. <sup>*Codebooks are merely*</sup> Here is a page from

~~elaborations of the sort of syllabary that Jefferson used.~~

~~a commercial communication company's codebook, which they offer to their~~

~~customers for economy.~~ You'll notice that each of these code groups differs

~~from every other code group by at least two letters.~~ We call that "the

~~SECRET~~

~~SECRET~~

two-letter differential." ~~The reason for having such a differential is that errors are sometimes made in transmission, but the likelihood of making two~~

~~errors in the same group is not nearly as great as making a single error. The~~

~~The~~ 2-letter differential affords methods of readily correcting a group if it has a single error in it; with a bit more trouble 2-letter errors can also be

corrected. Now, code books <sup>usually</sup> ~~are~~ <sup>for general sorts of business</sup> ~~compiled to be suited to general~~

~~specific kinds of business. If generalized, as in a general trade or shipping~~

~~code, or a code for the automotive industry, and so on, they get wide distribution~~

~~by purchase. But codes may also be highly specialized in character, as in the case~~

~~of the one I show in the next slide. specialized~~ You know, there are certain people who believe firmly and

implicitly in the power of healing by suggestion, and here is a picture of a

~~practitioner~~ code book put out by a ~~practitioner~~ in that field, a

code that is <sup>both</sup> in English and <sup>in</sup> French. ~~It is clear that~~ The purpose of it is

~~to be able to receive treatment~~ <sup>from or</sup> by your ~~practitioner~~

no matter where you/or he ~~is~~. Thus, if you should go away on a trip and want

to consult your practitioner, you can send him a message and tell him what

rather you are suffering from, or, ~~what you think you are suffering from.~~

You would simply represent your illness, or alleged illness, by the code

group corresponding to your malaise. Now, note that the <sup>professional</sup> ~~practitioner~~ who got up

this code was pretty well versed in the intricacies of code ~~and~~ communication.

difficulties, because these code groups differ by at least three letters. ~~more~~

The reason for this extra precaution is, of course, clear: It would be a

~~SECRET~~

pretty serious thing if you sent a message telling him that you think you are suffering from ~~coma~~ <sup>dysentery</sup> because ~~with the code group having been garbled in transmission~~ and he unfortunately gives you the treatment for ~~convulsions~~ <sup>constipation</sup>. That would be pretty tough!

Prior to World War I the use of code books for tactical purposes was thought to be impracticable, largely because of the <sup>danger of capture and the</sup> difficulties of compiling, reproducing, <sup>and</sup> distributing ~~and protecting the~~ <sup>new books constantly, especially in combat.</sup> books. I don't think they

thought too much about the possibilities of solving code. Early in 1916 the Germans began to use small field codes, and the Allies soon followed suit.

I had some slides to show you pictures of pages of the code books of the various belligerents, but I will omit them and say that I also have brought exhibits of such books as were actually used for the purpose. ~~Those who would like to see what they were like~~ are welcome to come up after this talk and

Code

21 ~~examine them.~~ The only slide that I will show is one that will give you a

picture of the American Army's <sup>unpreparedness</sup> ~~inadequacy~~ in World War I for <sup>secret</sup> code communications.

This is authentic--I didn't make it up--because I found it in the records when I closed our office in the AEF in April 1919. It's a code gotten out by the 52nd Infantry Brigade, dated 17 April 1918, and it is what we may call "the baseball code". If you wanted to say "killed", you said "struck out"; "wounded" was represented by "hit by pitched ball", and so forth--very elementary.

~~xxxxxxkxkx message xxxkxkx probably the most famous message of~~

~~xxxxxxkxkx message xxxkxkx probably the most famous message of~~

~~SECRET~~

In all I've said thus far about our World War I crypto-communications there's been little or nothing said about our high-command ones, messages

between General Pershing and Washington, for instance. *For this the Army had only*  
~~I did mention the War~~

Department Telegraph Code of 1915, ~~which we had when we entered the war as~~

~~a heliograph.~~ (It is with some sadness but also some amusement that I tell

you that soon after we joined the British they told us, with as much delicacy

as you may imagine the situation required, that ~~that~~ <sup>our</sup> code wasn't at all safe.

You don't have to wonder very much ~~what~~ <sup>about</sup> the implications of such ~~a notice~~ <sup>advice, but</sup>

~~meant, and it was our authorities manifested a great astonishment at the~~

~~time. You'll remember what I said about the British success in solving the~~

~~Zimmerman telegram which brought us into the war on their side.~~

~~With~~ steps were taken right quickly to produce ~~a new and much safer code~~  
 for the War Department and high command use, ~~also a new one for military~~

~~intelligence and secret agent communications.~~ It was also about this time

that our Navy <sup>also</sup> began to improve its communication <sup>security</sup> ~~secrecy~~ by adopting a cipher device

which went under the curious and almost movie-like title of the NCB--the

219

Navy Cipher Box. It was <sup>basically a modification of a very old device about</sup>  
~~a sort of strip cipher system, and I have a picture~~

~~of it.~~ *which I'll tell you something later.*

I don't know what our State Department communication security was like

in those days but I have my suspicions. The <sup>very old European</sup> ~~long~~ tradition of secrecy and

secret diplomacy wasn't our tradition--this was distinctly a European piece

of skullduggery and we ~~had and wanted to have~~ no part in it. Maybe <sup>our diplomats</sup> ~~we~~ were

~~SECRET~~

~~SECRET~~

not for us today but  
 taken for a cryptologic ride--I don't know. That would be something for some  
 cryptologically-minded historian <sup>to investigate in the voluminous records of our National Archives.</sup> He  
~~to look into it. He would have to search the~~  
 might find some interesting things there.  
~~records which is very doubtful.~~

And here is a good point at which to bring to a close this first period.

~~We'll continue with a bit more history in the next period but it will be devoted~~  
~~to watching the developments in a direction opened up by inventions made about~~  
~~the time of World War I.~~

~~SECRET~~