For a half century following the close of the Civil War, cryptology in the United States enjoyed a period of hibernation from which it awoke, not refreshed, as did Rip Van Winkle, but weaker. This is perhaps understandable if we take into account the fact that the United States was able to enjoy a long era of peace, broken only briefly by one short war, the Spanish-American War of 1898. For over three decades there was no need for cryptologic operations except such as were required for the communications of the Department of State. The military and naval services apparently felt that peace means peace. There was no need for their cryptography or cryptanalysis, and peace, the abhorrence of the peace-loving people, peace for as long an indefinitely long time, those services did not think it necessary or desirable to engage in cryptologic studies. Of course, the War Department and the Army still had their routine and cipher desks, the Navy Department and the Navy had their desks for producing monoalphabetic ciphers, and the Department of State had a few codebooks specifically designed for the communications between our embassies and consulates abroad. The U.S. was quiet.

Confidential
The long-furlonging period was briefly broken by one episode that may interest you. I had not planned to bring it to your attention in this brief history, but certain events in the very recent past lead me to tell you about it. I refer here to the very small majority by which Democratic candidate Kennedy won the presidency over Republican candidate Nixon, and the consequent talk about the possibility of an upset when the electoral college would come to do its work. The very same situation occurred in the presidential election of 1876, in which Democratic candidate Samuel J. Tilden was pitted against Republican candidate Rutherford B. Hayes. On the basis of early returns Tilden seemed to be in the lead, but Hayes, wearying of going to bed on election night, 8 November 1876, Hayes conceded to Tilden and the newspapers next morning in fact reported Tilden's victory. But a couple of days after the election it began to appear that perhaps Tilden's victory was not sure, and his supporters began maneuvers to try to make it certain by taking advantage of the peculiar system of electing a president, because it is the electoral, not the popular vote which determines who is to be president. Two days
The problem was solved by developing an efficient system for exchanging messages.

Plots were drawn and materials were exchanged between the two parties. Public key cryptography was used to ensure the confidentiality of the communications. Encryption tools were purchased and used to encrypt the messages. The messages were then exchanged and deciphered using the appropriate keys. This allowed for secure communication between the agents and prevented unauthorized access to the information.
The telegrams remained unknown for months. But the outcome of the election remained in doubt because four states—Florida, South Carolina, Louisiana, and Oregon—each sent two groups of electors, an event not foreseen and prohibited against in the Constitution. A crisis arose and the country seemed on the verge of civil war. By an act of 29 January 1877, Congress created a special electoral commission to settle the disputed votes in the four states. The commission voted in favor of the Hayes electors in each case and Hayes entered the White House. But it was only some months afterward that the telegrams to which I have referred were brought to light and a situation arose within Congress felt it had to look into. Somehow or other copies of the telegrams came into the possession of the Republican newspaper, The New York Tribune, and two members of its staff succeeded in solving those in cryptographic form.
Hassard, John R.G.


The Congressional House Committee designated to conduct the investigation was named "The select committee on alleged frauds in the Presidential Election of 1876." In the course of the investigation, the Committee called Dr. Edward S. Holden, of the United States Naval Observatory in Washington. I think he was a captain in the Navy and specialized in mathematics. The Tribune had brought him into the picture and Prof. Holden solved the equations but only after Dr. John R.G. Hassard, the chief of the Tribune's staff, and his colleague, Dr. William M. Groseclose, also of their staff, had reached a solution.

Prof. Holden's testimony is of considerable interest. He presented his solution of the many 200 cryptograms entered in evidence. His testimony is summarized in a letter dated 21 February 1879 and it sets forth all the cryptograms used by both parties and the dates with their keys and full details. In that letter, Prof. Holden makes the following statement: "By September 7, 1876, I was in possession..."
I

The article by J.T. Hill, "The North American Review," March 18, 1871, pp. 315-325, describes a method by which any key to the most difficult combination of a key to the most difficult decipherable text could be found. Holden worked out the transportation code that was anticipated by the Tribune and its cryptanalysts. There were ten keys, although Holden independently discovered ten more.

In all 10 different keys, two for messages of 10 words, two for messages of 15 words, etc., two for messages of 30 words. Here is the complete table of keys:

| Leave 1/4 page space |

I suspect that the sequences of numbers were drawn up at random but were derived from the words or phrases. I have not had time to try to reconstruct them. Perhaps some of you may like to make the attempt. You will notice that in the odd-numbered keys the positions of adjacent digits reflect an underlying order of names. In addition to transportation, this system involved the use of code words to represent the names of certain persons, places, and numera. There were also a few initials. Here is the entire vocabulary:
The essence of this ingenious and novel system consists in taking apart a sentence written in plain English (disregarding it as it were) and again writing all the words in a new order, in which they make no sense. The problem of deciphering it consists in determining the order according to which the words of the cipher should be written in order to produce the original message.

There is one way, and only one way, in which the general problem can be solved, and that is to take two messages, A and B, of the same number of words, and to number the words in each; then to arrange message A with its words in an order which will make sense, and to arrange the words of message B in the same order. There will be one order—and only one—in which the two messages will simultaneously make sense. This is the key.

It appears that Prof. Holden did not note the inverse-inverse relation in each pair of sequences, or, if he did, he failed to mention it, as Neumann did in his article.
There were enough messages to permit of establishing the meanings of the code words used, so that the plain text of practically all the messages in this the most complicated of the cryptosystems involved in this bizarre political episode, became quite clear. But there were several other systems involved, of which we may not be too precise about because they hardly deserve attention in this brief history. I do, however, want to call your attention to the very close resemblance between what was characterized by Prof. Holden as "the most difficult and ingenious" of the ciphers he solved, and the USMC route ciphers used by the USMC ciphers described in the previous lecture. Yet, not only he but also the Tribune cryptanalyst solved these ciphers without too much difficulty or delay. I think their work confirms my own appraisal of the weakness in the ability of the USMC ciphers to cope with the ciphers used in the USMC during the war. Let us now go on with cryptologic history after this political digression into the realm of what may be called political cryptology.
Another system used by the conspirators used a 2-letter for one substitution and was based upon a 10x10 checkerboard. Apparently, Prof. Holdon nor the Tribune cryptanalysts recognized the letter principle, nor did they find that the coordinates of the checkerboard employed a key phrase, which appropriately enough was "His Patient."

Nor did they realize that the same checkerboard, with numerical coordinates, was used for the 2-digit for one letter substitution. Here are two of the messages exchanged by the conspirators, one in the letter cipher, the other in the

They are long enough for solution, if you wish to try to solve them and find the key phrase, which will amuse you by its appropriateness.
for cryptographic communications in the years following
the Civil War. Probably it was a small code, even
an adaptation of some commercial code. But in an
article entitled "Secret Writing," which appeared in
Century Magazine, Vol. xxx, No. 3, a man named John
H. Nassau, apparently a coder clerk in the Depart-
ment, referred to it as code, in the following terms:

The cipher of the Department of State is the
most modern of all in the service of the Govern-
ment. It embraces the valuable features of its
predecessors and the merits of the latest inventions.
Being used for every species of diplomatic corre-
psondance, it is necessarily complex and unrestricted
in its capabilities, but at the same time it is
economic use in terms of expressiveness. It is simple and speedy in its operation, but so ingenious as to secure absolute secrecy. The construction of this cipher, like many ingenious devices whose operations appear simple to the eye but are difficult to explain in writing, would actually require the key to be furnished for the purpose of an intelligible description of it.

Only four years later a telegraph operator and code clerk of the State Department proved how vulnerable the Department's system of encrypted code really was. His name was Herbert O. Yardley, and many of you may know about him because he was the author of a famous and infamous book: Espionage, published by Bobbs-Merrill in 1931. As far as I know it is the only book which cannot legally be reprinted in the United States because it poses a serious national security threat. That is quite a story in itself, but I cannot tell it now. I'll save it for you if you happen to own a copy. But, protect it carefully, don't let it get away from you, because you can only obtain another copy of it by a more or less "under the table" deal or may only be purchased. An English edition by a similar sort...
Of deck. But to return to that State Department cryptosystem considered by Haswell "to secure absolute secrecy," here is the cover page of Yardley's 24-page typewritten analysis.

Yardley was quite wrong in thinking that this was the first successful attempt to solve a problem in unscrambled code, for in Europe successful attempts on more complicated cases were then the rule and I imagine that British cryptanalysts should have and perhaps did read. Cryptanalysts were quite successful in reading State Department messages only more or less regularly.

In our Navy the monoalphabetic cipher continued in use until the middle of the eighties, when several naval officers were designated to prepare a more suitable system based upon a code particularly for naval communications. The system they worked out involved a large codebook which had the official title Cipher Book, almost as large. In addition to these...
two books was a third book, "General Geographical Tables," the system
was placed into effect on 1 December 1884. About 10 years later, a new
edition of the fourth book was placed into effect, dated 1894

show you a most historic message sent in that Army
system of secret communication.

In our Army a code was also prepared,
and its composition and format hardly shed
laurels upon those responsible for its production
because it was merely a counterfeit of a commercially
available and popular small code for use by the
general public. William T. Thomas, Telegraphic code to
ensure secrecy in the transmission of telegrams, by
Robert Slater, secretary of the French Atlantic Telegraph
Co., the code must have met with popular acclaim
because by 1906, it was in its fifth edition. You may
like to see the title page of the second edition, a
copy of which is in my collection. I wish I had a
copy of the very first edition but not even the
Library of Congress has one; that's how scarce it is.

To get on with the story, in 1885 the War Department
published a code for its use and the use of the Army.
Here is a picture of its title page. The only difference
between it and the title page of the 2nd edition of Slater's
Code is in the spelling of the word secrecy, as you can
readily see in the picture I show you next. It would
appear that Col. Gregory was just a bit deficient
As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using this work":

It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No., and the method of using it is by an interchange of Nos., in accordance with a private understanding between correspondents, that a further No. is to be added to or deducted from the No. in the code, of the word telegraphed or written, to indicate the real-word intended, thus a "Symbolic" or "Dummy Word" is telegraphed, the meaning of which can only be read by those who have the key to the secret of how many should be added to or deducted from the No. in the Code, of the "Dummy Word", to find the word meant.

Here we have a sentence of 116 words with a meaning which is quite murky but I think you will gather its import. The system is what we now call an additive or substractive code method. But in the detailed instructions Slater goes one step further and suggests that instead of telegraphing the code numbers resulting from addition or subtraction, the actual words standing alongside the sum (or difference) of the mathematical operation be sent.
The rules for the exercise were:

- Improve your vocabulary.
- Use the correct tense.
- Use the correct word order.
- Use the correct word form.

Example: I am reading a book.

Example: I was reading a book.

Example: I have read a book.

Example: I had read a book.

Example: I will read a book.

Example: I will have read a book.

Example: I will be reading a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.

Example: I will have been reading a book.

Example: I will have read a book.
to Genl. General Sherman," Commanding Army of the U.S., to explain the betteries of the new code. Again because I'm afraid you won't place too much credence in what I'm telling you, the confidential letter is printed in full in Appendix I, to the letter which I have added: "Introduction" that Col. Gregory's part to the instructions for using the code.

Believe it or not, this was the code that the War Department and the Army used during the Spanish-American War. It was apparently used with simple substitutes in a copy in my collection. The substitute written on the inside of the front cover was 777. The American Black Chamber threw an interesting sidelight on this code system:

The compilation of codes and ciphers was, by General Orders, "The meant Army Regulations", a Signal Corps function, but the war [1917] revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer of the Signal Corps who had just been appointed a military attaché to an Allied Country. It was not intended that attaches should actually

-13-
arcade and decode their own telegrams, but as a part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.

When the new attaché, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communication. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which children we read in Poe's The Gold Bug.

He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it."
Although The American Black Chamber abounds with exaggerations and distortions, what the author tells about the inadequacies of United States codes and ciphers in the year just before our entry into World War I are true enough and Yardley's impatience and satires in this regard are fully and unfortunately fully warranted.

We have noted how inadequately the Army and the War Department were equipped for cryptographic communications in the decades 1890-1910. Let us see how well equipped the Navy and the Navy Department were. For this purpose I have an example and one of great historical significance and interest. You will recall my mention of the appointment of a board of Navy officers to prepare a suitable cryptopgraphy for the Navy and large I told you about the basic codebook and its almost algebraic book for companies, forming the code groups. For the headquarters, the Secretary of the Navy, John T. Morgan, perhaps for a map or a game board. Leaving Theodore Roosevelt, Assistant Secretary in charge of the store. It was Teddy's opportunity for a bold move unhampered by his superior's
story we go back to the time of President McKinley, whose election brought Theodore Roosevelt, a former member of the Civil Service Commission, back to Washington as Assistant Secretary of the Navy. Tally was an ardent advocate of military and naval preparedness and frankly favored a strong foreign policy, looking forward in fact to the ultimate withdrawal of the European powers from the Western Hemisphere. With vigor, he set to work to make the Navy ready. When the Battleship Maine was blown up in Havana Harbor on 15 February 1898, Roosevelt sharpened his efforts. During a temporary absence of his chief, John D. Long, he took it upon himself to instigate the preparations which he had in vain asked the Secretary to make. He ordered great quantities of coal and ammunition, directed the assembling of the fleet, started the arsenals and navy yards to activity. On a Saturday afternoon, ten days after the Maine was blown up, and still in the absence of Secretary Long, Tally sat down and wrote a cablegram to go to Commodore George Dewey. Here it is, with his bold signature at the bottom:

```
[signature]
```
That was the message which alerted Dewey and which resulted in our taking the Philippines from the Spanish in the war which was declared ten days later on Spain.

I don't know when their classification

"Secret and Confidential" was crossed out but it must have been years later, for those three words appear in the plain text of the deciphered and decoded cablegram. Here is a picture of the cablegram as it was received in Hong Kong:

And now I show you the deciphered and decoded text, which I produced myself by courtesy of the Chief of the Navy Security Group, who permitted me to borrow two books from Navy archives. To translate a message three steps are necessary.

First, the cable words (punctuation and English words—WASSERREIF, PAUSAUTURA, BADANADOS, etc.) are sought in the cipher book, and their accompanying numbers set down. WASSERREIF yields 99055; PAUSAUTURA yields 62399, BADANADOS, 11005; CENTENNIAL, 16820.

The next step is to append the first digit of each number to the last digit of the first cable-word number. Thus, 99055 becomes 990556. The six-digit number is then sought in the basic code book and its meaning is found to be "Secret and Confidential." The transfer of
demonstration of a straightforward mathematical method of solving the Vigenere cipher was published in
Paris during the mid-period of the Civil War in
America. If the book created an unspecified impression in
Europe, it was altogether unspectacular; in America
it remained unheard of until after the advent of
the 20th Century. Although Kasiski's method is ex-
plained quite accurately in the first text on cryptology,
Capt. Barker Hitti's *Manual for the Solution of Military
Ciphers* (Fort Leavenworth, Kansas: Army Service Schools
Press, 1916), the name Kasiski doesn't even appear in
it. Other books on cryptologic subjects appeared dur-
ing this period, among which the more important were
the following:

Of the foregoing two deserve special
mention. The first, by Commandant Bajonies, is a
book notable not for its general contents, which
are presented in a rather disorganized, illogical
sequence, but for its presentation of a cipher
device invented by the author, the so-called
cylinrical cipher device, a picture of which is

- 19 -
I now show you. But our own Thomas Jefferson anticipated Bezzerides by a century and here are two slides describing Jefferson's "Wheel Cypher" copied from the original manuscript among the Jefferson Papers in the Library of Congress. The second book devoting attention is the one by de Varios, in which he presents methods for solving cryptograms prepared by the Bezzerides ciphered cylinders or Jefferson's Wheel Cypher.

It was in the period during which books of the foregoing nature were written and published that the chanceries of European Governments operated the so-called Black Chambers, organized for solving the secret communications of one another. Intercept was unnecessary because the governments owned and operated the telegraph systems and traffic could be obtained simply by making copies of messages arriving, departing, or in transit through them. This was true in the case of every country in Europe with one exception: Great Britain. The story is highly interesting, but I must condense it to a few sentences.
In England from about the year 1580 onward, a black chamber was in constant operation. It was one of two organizations called The Secret Post Office and the Office of Decipherer. A famous mathematician, John Wallis, took part in the activities of the Office of Decipherer, but later in the 16th century letters were opened. In the copies of them were made, the letters replaced the envelopes resealed, and if there were no seals, duplicates were made. Copies of letters in cipher were sent to the Office of Decipherer for solution and the results sent to the Foreign Office.

A scandal involving these two secret offices caused Parliament to close them down so that from 1846 until 1914 there was no black chamber at all in Britain. As a consequence, when World War I broke out on the first of August 1914, England's black chamber had to start from scratch, but British brains and ingenuity within a few months built a cryptologic organization which contributed very greatly to Allied victory in 1918.

Perhaps the greatest and most important achievement of Room 40, C.B., was the interception and solution of what is deservedly called the most important single cryptogram in history. On 8 September 1918, I gave an account of this cryptogram, its interception, its solution.
and how the solution was handed over to the United States, bringing America into the war on the British side, without disclosing to the Germans just how the plaintext was obtained. Least of all, that it had been obtained by cryptanalysis—my talk took two and a half hours and I didn't quite succeed in telling the whole story, which you will find in great detail except for some technical data not yet available to the public—in a book entitled _The Zimmermann Telegram_, by Barbara Tuchman (date). Also, you should consult a book entitled _Eyes of the Navy_, by Admiral Sir William James (date). Both books deal at length with the Zimmermann Telegram and tell how astute Sir William Reginald Hall, Director of British Naval Intelligence in World War I, managed the affair so as to get the maximum possible advantage from the fact accomplished by the British Black Chamber. To summarize as I must, this fascinating true tale of cryptanalytic conquest, let me first show you the telegram as it passed from Washington to Mexico City.

Leave 1/2 page space
the day that French Ambassador Page sent his telegram to President Wilson on 24 February 1917. Quoting the English translation of the Zimmerman Telegram in the form in which it has been forwarded by German Ambassador von Bernstorff in Washington to German Minister von Eckhardt in Mexico City, the entrance of the United States into the war as a belligerent on the side of the Allies was assured. The English text appeared in our newspapers on 1 March, and on 6 April 1917 the United States declared war on Germany and the Central Powers. The date was 6 April 1917.

In the War Department, the pace set for preparing for active operations quickened in neither of these departments nor in the Navy Department, which was at the moment organizing Army and Navy, 

- in the Navy Department, there was no organized arms against the interception of communications by the Japanese, and since the autumn of 1916, as a very small organization with the authorities in Washington and official school for cryptographic

- obtained by interception means from telegraph and

- Honorary title conferred on the "Admiralty, Professor Fabyan" for participation as a member of the Peace Commission in negotiations
&colum

For instance, there is the bold black headline in the

New York Times of 1 March:

GERMANY SEEKS ALLIANCE AGAINST U.S.

ASKS JAPAN AND MEXICO TO JOIN HER;

FULL TEXT OF HER PROPOSAL MADE PUBLIC

The New York World had a series of headlines and
subheadings that extended halfway down the page,
beginning with:

MEXICO AND JAPAN ASKED BY GERMANY

TO ATTACK U.S. IF IT ENTERS THE WAR;

BERNSTORFF A LEADING FIGURE IN PLOT

There followed nine full lines of subheads to what
was a most amazing and dramatic story:

Still, notwithstanding all the furor that
the disclosure of the Zimmerman telegram created in America,
President Wilson still hesitated. And it was not until
more than a month later, and after several
American ships were sunk without warning on 18
March, that

There were plenty of senators and representa-
tives who disbelieved the story. It was too fantastic;
it was a British plot, improved; Wilson was being
taken in, etc., etc. But when Zimmerman himself publicly
acknowledged that he had indeed put such a telegram
disbelievingly charges quickly into vehement anger. Surely
war which now of declared on Germany!
REF. For: Training ourselves for this unusual task, and later, what we needed later on for training the student officers sent to Paris before for cryptologic instruction. As

You may like to know what we used to train ourselves—very instruction training material. There was a small book, which had been prepared by a Captain Parker Hitt and printed out by the Army Press. The Signal Corps, at Fort Leavenworth in 1914. The Signal School was there a part of from the beginning, and there a few lectures were given by persons—officers who, when World War I broke out in August 1914, took an interest in the subject of military ciphers. Captain Hitt wrote a book on military cryptology which was a real book for knowledge and training. Hitt's Manual was then and is still is a model of compactness and practicality. Here is the title page.

It was the succinctness of the Manual that work and caused us to spread much perseverance in our self-training. Later, come to know and recognize admittance to the author, whose photograph I show you.

There was one other item of training literature which we studied widely too—very small pamphlet entitled 'Advanced Problems in Cryptography and Its Solution, put out by the same Leavenworth Press in 1914. Here is its title page, and a photograph.
...diplomats,

At that period in our history our relations with Mexico were in a bad state so that U.S. attention was concentrated southward. Therefore, practically all the messages sent to Riverbank were those of the Mexican government. (Cable offices in Washington, Vondermark direction-Riverbank.

operations of this group which was successful in solving all of nearly all Mexico's cryptograms was given, returning the solutions to Washington very promptly. It was also soon after war was declared on Germany. The Riverbank laboratories established, a school for training Army and Navy officers sent there to learn something about cryptology. In Lecture II (Fig. 21) there is a picture of the last of the classes sent by the Adjutant General of the Army to Riverbank for training. It should be noted that the instruction was conducted at Colonel Fabyan's own expense as his patriotic contribution to the U.S. war effort. Upon completion of the last training course I was commissioned a 1st lieutenant and ordered immediately to proceed to France where I became a member of the German Code and Cipher Solving Section of the General Staff, G-2, A-6, GHQ - A.E.F. As the expanded designation implies, the operations were conducted in two principal sections, one devoted to working on German military field ciphers, the other to working on German field codes. There were other very small groups working on cipher materials, such as meteorologic message traffic, on direction finding bearings and what we now call intelligence that is, deciphering messages written to determine enemy order of battle flow of intelligence, an analysis of the bearing of the direction, and flag of enemy traffic and other data sent back from our direction finding stations, etc, or our own intercept stations.
In connection with the last-mentioned operations, you will no doubt be interested to see what is perhaps in cryptography, history, that shows one of the earliest, if not the very first, chart showing the results of traffic analysis, enemy intentions, from a mere study of the ebb and flow of enemy traffic.

This particular chart was drawn up from data based solely upon the ebb and flow of messages in what was called the ADFGVX cipher, which was devised by German cryptographers and often used for German High Command communications. Theoretically, it was very secure because it combined both substitution and transposition principles. There is a diagram which, if you studied it carefully, will give a clear understanding of its method of usage.

If you wished for further details, I suggest you consult documents available in NSA Training Literature Department Division of the NSA Office of Training. In this lecture, there is only time to tell you that although individual or isolated messages in that system appeared at that time to be absolutely impregnable against solution, approximately 50% of all the.

*Initially, this cipher employed only the letters A, D, F, G, and X; for a matrix 5 x 5; later, the letter Y was added, for a matrix 6 x 6.
messages transmitted in the ADFGVX system were read by the Allies. You may be astonished by the foregoing statement and may desire some enlightenment here and now on this point. Well, in brief, there were three different methods of attacking the traffic in that cipher. Under the first method, two or more messages with identical beginnings/plain-text could be used to uncover the transposition as the first step. Once this had been done, the cryptanalyst had then to deal with a simple substitution in which two letter combinations of the letters ADFGVX represented single plain-text letters. The messages were usually of sufficient length for this purpose. Under the second method, two or more messages with identical plain-text endings could be used to uncover the transposition, and this was even easier than in the case of identical beginnings. You might think that cases of messages with identical beginnings or endings would be rather rare, but the stereotypic phraseology in German military mentality was then—and perhaps still is—so conformist that cases were almost invariably found in each
day's traffic. This is astonishing considering that the keys changed daily. This system first came into use on 1 March 1918, three weeks before the last and greatest spring offensive by the German Army. Its appearance was almost coincident with that of other new codes and ciphers. The number of messages in the ADFGVX cipher varied from about 25 a day, when the system first went into use, to as many as about 150 at the end of two months. It took about a month to figure out a method of solution, and this was done by the very able French cryptanalyst named Captain George Parmann of the French Cipher Bureau.

The ADFGVX cipher was used quite extensively during May and June of 1918 but then the number of messages dropped very considerably. How many different keys were solved by the Allies? Not many—10 in all, that is, the keys for only 10 different days were found. Yet, because the traffic on those days was heavy, about 52% of all messages sent in that cipher were solved and a great deal of valuable intelligence derived. On one occasion solution was so rapid that an important German operation di-
closed by one message was completely frustrated. Although the ADFVX cipher came into use first on the Western Front, it later began to be employed on the Eastern Front, with keys that were first changed every two days but later every three days. On 2 November 1918 the key for that and the next day was solved within a period of an hour and a half because two messages with identical endings were found. A third message in that key gave the complete plan of the German retreat from Romania.

During the whole year of the life of the ADFVX cipher, no general solution for it was devised by the Allies despite a great deal of study. However, members of the own Signal Intelligence Service, in 1933, and while still students undergoing instruction in cryptanalysis, devised a general solution and proved its efficacy. Pride in their achievement was not diminished when the course of writing up and describing their method in a book, "French Cifrerie (Cours de Cryptographie), published in 1925."
The ADFGVX cipher was not the only one used by the German Army in World War I, and there will be time to mention only very briefly two others. The first of these was a polyalphabetic substitution cipher, with a set of 36 fairly lengthy keywords. The cipher square is shown in Fig. 00 and the set of keys is shown in Fig. 00. Just why the square contains only 22 rows instead of 36 is unknown. Certainly the rows within the square are not random permutations of the 26 letters, but the manifestly fixed arrangement in sets of five sequences, as now are the key sequences of random letters. To reconstruct the real square and the real keys, the latter problem should be relatively easy; as to the former, I really don't know—I have never tried it myself, but I suspect some systematic disarrangement. The other cipher to be mentioned is the double transposition, solution of which usually depended upon finding two messages of identical length. No general solution was known to the Allies during World War I. Occasionally an operator would apply only the first transposition and when this happened solution was easy. Then the key thus recovered could be used to decipher other messages which had been correctly enciphered.
by the double transposition. Again, students of
the Signal Intelligence Service devised a general
solution for the double transposition cipher and
during World War II were able to prove to our
British allies that such ciphers could be solved
without having to send two messages of identical
length. Having demonstrated a properly employed, it
was withdrawn from usage by the British, but we
were not told directly that this was done. I should
think that the devising of a general solution for the
two double transposition ciphers represents a real
landmark of progress in cryptanalysis without the
aid of high-speed, electronic equipment. I do
not doubt that, with such equipment, this cipher
would hardly be thought to be safe for modern
military communications.

We come now to the code systems used
by the belligerents in World War I. And first let us
recognize that the Anglo-Americans used for diplomatic communications from those
used for military communications. What post did the
German Foreign Office use? We have noted how
the British Black Chamber, "Room 40, B," dealt
with tremendous success on the code used for the transmission of the Zimmermann Telegram. But that's only part of the story—the most important part remains to be told and unfortunately I cannot divulge that part yet. But the version of that telegram as it passed from Washington to Mexico City was in one version of a basic code which had several other versions, all quite similar in basic construction and equally vulnerable to cryptanalytic attack. Excessive pride in German achievements, and a disdain for the cryptanalytic prowess of enemy cryptanalysts, led General diplomatic communications open to solution by the Allies to the point where nothing the German Foreign Office was thinking about, telegraphed abroad, was secret, for those of you who would like to learn some details, I refer you to the final monograph on the subject by Charles J. Mandelkorn: Studies on German Diplomatic Codes Employed During the World War, Government Printing Office, 1937. This monograph is confidential, but copies are available in the Office of Training, NSA.
At the time of the War, German codes were an unexplored field in the United States. The

American code was sent to Britain by Dr. Mandelson. "About a year later we received from the British a copy

of a partial reconstruction of the German Code, 13040 (about half of

the vocabulary of 19,400 words and 800 of the possibly 7,600 proper

names). This code and its variations over several years had been in

use between the German Foreign Office and the German Embassy in

Washington up to the time of the outbreak of war, and our files con-

tained a considerable number of messages, some of them of histori-

cal interest, which were now read with the aid of the code book.

The vocabulary of the German diplomatic codes contained 189 pages,

containing exactly 100 words or expressions to the page,

arranged in four columns of 50 each accompanied by

numbers from 00 to 99. In each column, the groups

were in blocks of 10. The pages in the basic code were

numbered from 23 and from this code several were made

numbered at the top and derivative codes based

for the use of conversion tables. This enabled the basic code to

serve as a basis for several different communications

what the number of the basic code was a known,

code, but we do not know that from the derived code, designated

code 5950, 62040, and others, derived

as 13040, codes dermal 5950, 62040

merely by means of tables for converting the page

numbers in the basic code into two different page numbers

in the derived code. In addition, there were tables for

converting the page numbers from one code to another.

These conversions were systematic, in blocks of five:

Thus, pages 15-18 in 13040 became pages 65-68 in

5950, pages 19-22 in 13030 became pages 192-195 in

5950, etc. Then there were tables for converting line

numbers from one version to another version of the basic

code, and this was done in blocks of 10. For example, the fifth block

(25th figure of 31) became the first (penultimate figure of 31)

and the 1st, 2nd, 3rd, and 4th blocks were moved down one place.
The other five blocks (left hand side of the page) were rearranged in the same manner.

It is obvious that codes derived in such a manner from a basic code by no means represent the equivalents of being different codes, they were all and the equivalents of one another. Also to be mentioned is the fact that in certain cases 3-digit numbers were added to or subtracted from the code numbers of a message and that in practically every case it was not difficult to determine the additive or subtractive.

In none of the cases or codes mentioned thus far was there one that could at least be considered to be a randomized, "hatted", or true two-part code. [To continue on p. 33]
twin two-part code, since the same book served
for both encoding and decoding. However, the
German Foreign Office later took true two-part codes of
10,000 groups, numbered from 0000 to 9999. One such code
indicated the number that several cipher machines were to
use in conjunction with the usual rotors. And there were others besides these. (Ernst
Dietrich, 1943, p. 24)

When one retrieves Dr. Mendelssohn's
monographic one is overwhelmed by the multiplicity of the codes used by the German Foreign
Office. Many were quite similar but many were far
removed from the original. It is therefore hard to ascertain the exact number of
derivatives, i.e., even hard to distinguish them. Yet a
great deal of the traffic in these codes was
read. Considering the rather small number
of persons on the staff of G-2 and its analogous organization in the London
Black Chamber, one can only be astonished by
the achievements of the collaborative effort
of these two organizations during World War I.

So much for the German diplomatic
cryptosystem. What about the German military
cryptosystem? In this area we must credit the Germans
with being first to decide that the old idea
that a code could not be practically or safely employed
in actual communication was not valid.
It is my belief that the conversion tables were not used by the code clerks but by the compiling authorities in Berlin. In other words, the various, not versions of the basic code were actually printed so that the original, page number-verified pages altered as separate books. Instead, code was entered by hand, the original number being crossed out and entirely different numbers appearing. The new number written either at the top or bottom of the page, perhaps in both places. Similarly, the block numbers were probably changed by hand. In both cases the alterations were made in accordance with some system, the idea of randomness seems foreign to the German mentality, and the Germans never do anything by random. I am sure that if randomness were a desideratum, they would figure out a system therefor.
So much for German diplomatic secret communications. What about German military crypto-
communications? In this area it is necessary to mention a situation which is somewhat unique. When World
War I commenced the German Army was very poorly
prepared to meet the requirements for secure communi-
cations. It seems that up until the Battle of the Marne in
1914 several German Army radio stations went into the
field without any provision having been made or even
foreseen for the need for crypto-communications.
Numerous complaints were registered by German com-
manders concerning extensive loss of time occasioned
by the far too complicated methods officially author-
ized for use and the consequent necessity for sending
messages in the clear. Not only did this reveal intelli-
gence of importance to their opponents but what is
equally important the practice permitted the
British and the French to become thoroughly familiar
with the German telegraphic procedures, methods of
expression, terminology, and style, and these items
became

...
field
ments in military cryptography. In fact, the develop-
ments and improvements began not long after the out-
break of the war and continued steadily until the end. When
on 11 November 1918 the armistice ended active opera-
tions, German military cryptography had attained a remark-
ably high state of efficiency. The astonishing fact is that,
although very proficient in cryptographic invention,
they were apparently quite deficient in the science
and practice of cryptanalysis. In all the years since the
end of World War I no books or articles telling of German
success with Allied traffic during that war have appeared.
peace for one very brief article by a not very bright German
cryptanalyst. One could, of course, assume that they
kept their successes very well hidden but the German
archives taken at the end of World War II contain
nothing significant in regard to cryptanalysis during
World War I although a great deal of important
information in this field during World War II was
found. A detailed account of the war between the
Allied and German forces in World War II would
require scores of volumes, but [continue over].

In this lecture, however, we are prin-
cipally

concerned with the German military cryptography
during World War I, and I have already told you
There is one source of information which I can highly recommend to those of you who would like to know more details of the cryptologic warfare between the belligerents in World War I. That source is a book written by a Swedish cryptanalyst, Yves Gylden, under the title *Chifferbyråernas Insatser I Världskriget Till Lands*, a translation of which, with some comments of my own in the form of footnotes, you will find on file in the Office of Training, NSA, under the title *The Contribution of the Cryptographic Bureaus to the World War*. Government Printing Office, 1986.
something about the cipher systems that were used. There remain to be discussed the field codes. It was the German Army which first proved that the old idea that codebooks were impractical for use in the combat zone for tactical communication was wrong. They had two different types of field codes, one we called the "three-number code," while the Germans called it the SATZBUCH or "sentence book" but which we called the other, the "three-letter code." The former was a single vocabulary code with a frequently used word list and expressions, which the code equivalents were 3-digit numbers. A cipher was applied to the code numbers and this cipher consisted of a 10x10 matrix for the numbers from 00 to 99. The last digit of a code group remained unenciphered. Each division compiled and issued its own table, which was in two parts, one for encipherment, the other for decipherment. The three-number code was intended for use in all forms of communication within or to and from a 3-kilometer front-line danger zone. Although this code was not put into use until the opening day of the last and greatest German offensive, 10 March 1918, the new code was specified and the four groups in it were solved the very same day because an operator, who was
Here copy p.3 of
Field Codes used by the
German Army
unable to translate a message in the requested and received a repetition in the old code, the three-letter code, and the latter had been solved to an extent which made it possible to identify homologous code groups in both messages. The three-number proved rather easy to solve on a daily basis and much useful intelligence was obtained thereby.

The three-letter code, however, proved much more difficult. In the first place, it had a much larger vocabulary, with nulls and many variants for frequently-used words and numbers; in the second place, three-letter combinations were an essential part of the solution and the real stumbling block to solution was the fact that it was a true two-part randomized or "hatted" code, and in the third place, each sector of the front used a different edition of the code, so that traffic not only had to be identified as to the sector from which it belonged but also it was not possible to combine all the messages for the purpose of building up frequencies of usage of code groups. Working with the sparse amount of traffic from a quiet sector of the front and trying to solve further codes within the code was really a painfully slow, very difficult task.
generally frustrating experience. On my reporting for duty Colonel Frank Moorman, who was chief of the whistle unit and whose photograph I show you here, asked me whether I wished to be assigned to the cipher stress section or to the code section. Having had considerable experience with the solution of the former types of cryptosystems but none with the latter, and being desirous of gaining such experience, I chose asked for an assignment to the code polishing unit. I gained the experience I wanted and needed to broaden my cryptology knowledge almost immediately, but little did I realize what a painful and frustrating period of learning and training I had undertaken. Still, I have never regretted the choice I made; in fact, it turned out to be a very wise and useful one. If any of you would like to read about my experience in this area, let me refer you to my monograph entitled *Field Codes Used by the German Army during World War II*, copies of which are on file in the Office of Training, N.S.A. I will quote a few [sentences]

What sort of cryptosystems did the French Army use? First, as for ciphers, they put
Paragraphs from my "estimate of the three-letter code table" as it appears on p. 65 of that monograph.
much trust in transposition methods and here is
an example of one type:

As for codes, like the Germans they
called "Carnet Reduit"
used a small front-line booklet by Various sectors
of the front and I will show a picture of one
of them. Then, in addition, there was a much
more extensive code which was not only a
two-part, randomized book but a transposition
method was applied to the code messages when
transmitted by radio or "TPS," that is, "telegraphic par
sole," or earth telegraphy. Here is one of the tables used
for enciphering (and deciphering) the code groups:

And here is the example given in the code in my
collection:

You will notice that the enciphering
process breaks up the 4-digit groups in a rather
clever manner by making the first digit of the
first code group separately; the second and third
digits of the first group are enciphered as a pair, then
the last digit of the first group and the first digit
of the second code group are enciphered as a pair,
and so on. This procedure succeeds in breaking up
the code groups in such a manner as to reduce very
greatly the frequency of repetition of 4-digit groups
representing words, numbers, phrases, etc. of very
common occurrence in military messages. My appraisal
of this French Army cryptosystem is that it certainly
was the most secure of all the systems used by
the belligerents but I don't know how much usage
was made of it. I venture the opinion that
it was not used often, or successfully, with the
superenciphering method provided for the basic code.

How about the cryptosystems used
by the British Army? First they used the Playfair
Cipher, a system of digraphic substitution considered
in those days to be good enough for unimportant messages
in the combat zone. But today, of course, its security
is known to be so low as to be unworthy of placing
any reliance in it. The British also used a fixed
code, this contained many common military
expressions and sentences, grouped under various
headings or categories, and, of course, a very small vocabulary of frequently used words, numbers, punctuation, etc. It was always used with super-
encipherment, the nature of which was not disclosed
even to their Allies, so I unfortunately am not in a position to describe it. I don't have a copy of their code—only a typewritten transcript which was furnished us quite reluctantly and I will show a typical page thereof.

What about the cryptosystems used by the Italian Army? You may find it hard to believe but it was a simple variant of the very old Vigenere cipher and I showed you a picture of it here.

Whether a code book was used in addition, I do not know.
What about the cryptosystems used by the Italian Army in World War I? The general level of cryptologic work during that period was quite low in character, a fact which is all the more remarkable when we consider that the birthplace of modern cryptology was in Italy several centuries before this period. There appears to have been a knowledge of cryptologic techniques in the 15th and 16th centuries than in the 19th paradoxical as this may seem to us today. Perhaps this can be considered as one of the consequences of a policy of secrecy which not only filing away in dusty archives records of cryptanalysis successes a decadent but also prevents those who might have born with what it takes to develop a flair for cryptologic work from profiting from the progress of predecessors who have been successful in such work. Should we be astonished to learn, therefore, that when Italy entered into World War I, the Italian Army put its trust in a very
Simple variation of the ancient Vigenere cipher, a system called the "cifraso militaire tascabile" or the "pocket military cipher"? Or, as well as several others devised by the same Italian "expert," were solved very easily by the Austrian cryptanalysts during the war. The Italian Army also used codes, no doubt, but since decipherment of such codes consisted in adding or subtracting a number from the page number on which a given code number group appeared, the security of such systems was quite illusory. As late as in 1927 the Italian "expert" announced his invention of an absolutely indescribable cipher system which, Giedion says (p. 23) "still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on this part."

What about Russian cryptographic work in World War I? So far as Russian cryptographic work is concerned, we know that there was during Czaristic days an apparently well-organized and effective black bursam for diplomatic codes and cipher, organized by a Russian named Savinsky.
formerly Russian minister to Stockholm. He had
all codes and ciphers in use up to then improved,
introduced strict regulations for their use, and
kept close watch over the service. He also was
head of a cryptanalytic activity, and it is
known that Turkish, British, Austrian and
Swedish diplomatic messages were solved. After
the Bolshevist revolution of 1917 some of the
Russian cryptanalysts managed to escape
from their homeland and I had the pleasure
of meeting and talking with one of the best of
them during his service in the black chamber of one of our allies in World
War II. He wore with great pride on the
index finger of his right hand a ring in
which was mounted a beautiful large ruby,
the ring having been presented him by the
last Czar in recognition of his cryptanalytic
proeess while in his service.

But the story is altogether different
as regards cryptology in the Russian Army.
The military cryptographic service was
poorly organized and, besides, it had adopted
Enciphering the first set of letters (5, 7, etc.) according to the indicator by alphabet 1. The next set by alphabet 2, and so on. After the 8th set of letters, which was enciphered by alphabet 2, return to alphabet 1, repeating the sequence until the entire message has been enciphered.

Consecutively, by redrawing and then continuing with the next alphabet, the indicator suggesting how many letters were enciphered would precede a set of figures indicating how many letters were enciphered. Indicators were sometimes repeated. Therefore, it can be seen below are the figures and letters of the alphabet. In the top line, the 2-digit group consists of 1 to 8. Randomly, the 3rd group appears in the sequence as well. Notice 3 is repeated twice.

Fig. 00

A table was enciphered alphabet by alphabet in pairs, with the 2-digit groups written down. Now, an example of how to use the table is shown next.
It was then sent in 5-digit groups. The use of the
deciphering table hardly requires explanation but
questioned may be in order: Why to the use of zero and to the use of double digits
such as 11, 22, 33, etc? This remains a puzzle to me.

I have told you that this cipher system
proved too difficult to use, so difficult that
messages had to be repeated over and over, with
great loss of time. It is well known that
the Russians lost the Battle of Tannenberg in
the autumn of 1914 largely because of faulty
communications. Poor cryptography or failure to
use even simple ciphers properly on the field
of battle, and not brilliant strategy on the part of
the enemy, was the cause of Russia's defeat in that
and in subsequent battles. The contents of Russian communi-
cations became known to the German and Austrian
high commands within a few hours after transmis-
sion by radio. The dispositions and movements of Russian
troops and Russian strategic plans were no secrets
to the enemy. The detailed and absolutely reliable
information obtained by intercepting and reading the
Russian communications made it very easy for the
German and Austrian commanders, not only to take
proper counter-measures to prevent the execution of
Russian plans, but also to launch attacks on
the weakest parts of the Russian front. Although the Russian
ciphers were really not complicated their cipher clerks
and radio operators found themselves unable to exchange
messages with accuracy and speed. As a matter of fact they
were so unwise that not only were their cipher messages easily solved but also they made so many errors that the recipients themselves had considerable difficulty in deciphering the messages even with the correct keys. In some cases this led to the use of plain language so that the German and Austrian forces did not even have to do anything but intercept the messages and translate them. To send out dispositions, movements, immediate and long-range plans in plain language was, of course, one cardinal error. Another was to encipher only words and phrases deemed the important ones, leaving the rest in clear. Another cardinal error, made when a cipher was superseded, was to send a message to a unit that had not yet received the new key and then repeat the identical message in the old one. I suppose the Russians committed every error in the catalog of cryptographic crimes.

No wonder they lost the Battle of Tannenberg, which one military critic said was not a battle but a massacre, because the Russians lost 100,000 men in the 3-day engagement, on the last day of which the Russian commander-in-chief committed suicide. Three weeks later another high Russian commander followed suit.
and the Russian Army began to fall apart, completely disorganized, without leadership or plans. Russia itself began to go down in ruins when its Army, Navy, and Government failed so completely, and this made way for the birth of the October revolution, ushering in a regime that was too weak to put things together again and to hold them together. The remnants, picked up by a small band of fanatics with military and administrative ability, with treachery, violence, and cunning, welded together what has now become a mighty adversary of the Western World, the USSR.
I have left to be treated last in this lecture the cryptosystems used by the American Expeditionary Forces in Europe during our participation in World War I.

When the contingents of the AEF arrived in France in the summer of 1917, there were available for secret communication within the AEF but three authorized means. The first was the extensive code for administrative telegraphic correspondence, the 1915 edition of the War Department Telegraph Code, about which I already told you something. Although it was fairly well adapted for that type of communication, it was not at all suitable for rapid and efficient strategic or tactical communications in the field, nor was it safe to use without a clumsy superencipherment. The second cryptosystem available was that known as the repeating-key cipher, which used the Signal Corps Cipher Disk, the basic principle of which were described as far back as about the year 1500. The third system available was the Playfair Cipher, which had been frankly copied from the British who had used it as a field cipher for many years before World War I and continued to use it. In addition to these authorized means there were from time to time current in the AEF apparently several — how many,
no one knows—unauthorized, locally—improvised "codes" of varying degrees of security, mostly nil. I show one of these in Fig. 60, and will let you assess its security yourself.

Fig. 60

Seen in retrospect, when the AEF was first organized, it was certainly unprepared for handling secret communications in the field, but it is certain that it was no more unprepared in this respect than was any of the other belligerents upon their respective entries into World War I, as I've indicated previously in this lecture. This is rather strange, because never before in the history of warfare had cryptography played so important a role. When measured by today's standards it must be said that not only was the AEF unprepared as to secret communication means and methods and as to cryptanalysis, but for a limited time it seemed almost hopeless that the AEF could catch up with the times, because their British and French allies were at first most reluctant to disclose much of their hard-earned information about these vital matters.

Nevertheless, and despite so inauspicious a commencement, by the time of the Armistice, in
November 1918, not only had the AEF caught up with their allies but they had surpassed them in the preparation of sound codes, as may be gathered from the fact that their allies had by then decided to adopt the AEF system of field codes and methods for their preparation, printing, distribution, and usage.

Just as the invention of Morse wire telegraphy had a remarkable effect upon military communications during the American Civil War, as related in the preceding lectures, so the invention of radio also played a very important role in field communications during World War II. Now, although it can hardly be said that all commanders from the very earliest days of the use of radio in military communications recognized one of the most important disadvantages of radio—namely, the fact that radio signals may be more or less easily intercepted by the enemy—it was not long before the consequences of a complete disregard of this obvious fact impressed themselves upon most commanders, with the result that the transmission of plain language became the exception rather than the rule. This gave the most momentous stimulus to the development and increase of use of cryptology that this science had ever experienced.
Let us review some of the accomplishments of the Code Compilation Service under the Signal Corps, AEF. It was organized in January 1918 and consisted of one captain, three lieutenants and one enlisted man. Until this service was organized, that is from the summer of 1917 until the end of that year the AEF had nothing for cryptography except those three inadequate means. They mentioned when it had been determined that field codes were needed little time was lost in getting on with the job that had to be done. Since I had no part in this effort I can say without danger of being misunderstood as to motives, that the Code Compilation Service executed the most remarkable job in the history of military cryptography up to the time of World War II.

The first work entrusted to it was the compilation of a freestream "Trench Code", by which 10,000 copies were printed, together with what were called "distortion tables." These were simple monosyllables for enciphering the 2-letter groups of the code. I show a picture of a page of this code and one of the "distortion tables."
The danger of capture of these codes was recognized as being such that the books were not issued below battalion. Hence, to meet the needs of the front line, a much smaller book was prepared and printed, called the "Front Line Code." Distraction tables, 30 of them in all, were issued to accompany this code, of which an edition of 3,000 copies was printed—but not distributed, because a study of its security showed defects. AEF cryptographers were groping in the dark, with little or no help from allies and with inexperience in cryptanalysis. Finally, the light broke through: the Code Compilation Service began to see the advantages of the German 3-letter randomized 2-post code known as the Satzbrush. She told you about this code and what the AEF learned about its advantages. Here, then, was the origin of the AEF real Trench Codes—copying from the experience of German code compilation and then going them one better. The first code of the new series, known as the "Potomac Code," the first of the so-called "River Series," appeared on 24 June 1918, in an edition of 2,000 copies, and contained approximately 1,700 words and phrases, and as the official report...
as succinctly states, "was made up with a coding and decoding section in order to reduce the work of the operators at the front." The designation "two-part" or "randomized," or even "hatted" code was still unknown—but the principle was there, nonetheless. Let us see what the official report goes on to say on this point; let us listen to some sound communique pause: 

"The main point of difference from other Army codes lay in the principle of reprinting these books at frequent intervals and depending largely upon the rapidity of the reissuance for the secrecy of the codes. This method did away with the double work at the front of deciphering and deciphering [sic!], and put the burden of work upon General Headquarters, where it properly belonged. Under this system one issue of codes could be distributed down to regiments; another issue held at Army Headquarters; and a third issue held at General Headquarters. As a matter of record this first book, the Patomac, was captured by the enemy on July 20, just one month after issuance, but within two days, it had been replaced throughout the entire Army in the field."
The replacement code was the Seneca, the next in the River Series, followed by the Wabash, Allegheny, and the Hudson, all for the American First Army. In October 1918 a departure in plan was made and different codes were issued simultaneously to the First and Second Armies. This was done in order not to jeopardize unnecessarily the life of the codes by putting in the field at one time 5,000 and 6,000 copies of any one issue. Thus the Champlain, the first of what came to be called the "Lake Series," was issued with the Colorado of the "River Series" for the First Army; these were followed by the Huron and the Osage, the Senaca and the Niagara, in editions of 2,500 each.

In addition to the foregoing series of codes were certain others that should be mentioned, as for example, a short code of 2-letter code groups to be used by front line troops as an emergency code; a short code list for reporting casualties; a telephone code for disguising the names of commanding officers and their units, and so on. But there was in addition to all the foregoing one large code that must be mentioned, a code to meet the requirements for secure transmission of messages among the higher commands.
in the field and between there and SPA. This was a task of considerable magnitude and required several months' study of messages, confidential papers concerning organization, replacement, operations, and military documents of all sorts. The code was to be known as the AEF Staff Code. In May 1918 the manuscript of this code was sent to press and the printing job was done in one month by the printing facilities of the AEF Adjutant General. Considering that the code contained approximately 30,000 words and phrases, accompanied by code groups consisting of 5-figure groups and 4-letter groups, the task completed represents a remarkable achievement by field printing organization and I believe that this was the largest and most comprehensive codebook ever printed by any army in the field. More than 50,000 telegraphic combinations were sent in tests in order to cast out combinations liable to error in transmission. One thousand copies of this code were printed and bound. With this code as a super-enormous system there were issued from time to time "distortion tables". There remain only to be said that the war was over before this
code could be given a good work-out, but I have no doubt that during the few months it was in effect it served a very useful purpose. Moreover, the excellent vocabulary was later used as a skeleton for a new War Department Telegraph Code to replace the edition of 1915.

One more code remains to be mentioned: a "Radio Service Code", the first of its kind in the American Army. This was prepared in October, to be used instead of a French code of similar nature. Finally, anticipating the possible requirement for codes for use by the Army of Occupation, a series of three small codes, identical in format with the war-time trench codes of the river and lake series, was prepared and printed. They were named simply Field Codes No. 1, 2, and 3, but were never issued because there turned out to be no need for them in the quietude in Germany after the Army of Occupation marched into former enemy territory but now very friendly territory.

I will bring this lecture to a close now by referring those of you who might wish to learn more about the successes and exploits of the cryptographic organization of the AEF.
World War I to my monograph entitled "American Army Field Codes in the American Expeditionary Forces during the First World War." Government Printing Office, 1942. In that monograph you will find many details of interest which I have had to omit in this talk, together with many photographs of codes and ciphers produced and used not only by the AEF but also by our allies and enemies during that conflict.