Legal size triple space 1 carbon copy

LECTURE No 5

For a half century following the close of the Civil War, cryptology in the United States enjoyed a period of hibernation from which it at long last in about 1914, 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, 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 ~~since~~ in time of peace there ~~isn't to be~~ no need for ~~either~~ cryptography or cryptanalysis, and since, it looked as though the U.S. was going to enjoy ~~the duration of the peace appeared to~~ peace for a 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 route ciphers and cipher disks, the Navy Department and the Navy had their desks for producing monoalphabetic ciphers; and the Department of State had a ~~[illegible]~~ more or less code specifically designed for ~~its communications~~ [illegible] Everything on ~~the U.S.~~ international scene, as far as concerned the U.S., was quiet. Let Europe fight — it was none of our way of life or our affair.

The long hibernating 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 popular-vote majority [illegible] 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 convene to do its work. The very same sort of 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 easily the winner. Going to bed on election night, 8 November 1876, Hayes conceded to Tilden and the newspapers next morning in fact reported a Tilden 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 our peculiar system of electing a president, peculiar because it is the electoral, not the popular, vote which determines who is to be president. Two days after the people had voted it became clear that Tilden would have 184 electoral votes, just one vote short of insuring victory, whereas Hayes would have only 163, thus needing 22 more. The Tilden supporters began a frantic campaign to get that one additional vote and they didn't hesitate to try bribery, a rather serious piece of business obviously requiring a good deal of secrecy. Of course, many telegrams had to be exchanged between the Tilden headquarters in New York City and confidential agents sent to certain states where electoral votes could perhaps be purchased; telegrams also had to be exchanged among secret agents in the field. About 400 telegrams were exchanged and about 200 of those were in cryptographic form. Because of communication difficulties two ~~of three separate~~ almost-consummated deals fell through; a third deal failed because the electors were honest Republicans not susceptible to bribery [Insert over]

¶ Those of you who are interested in the political aspects of this ~~campaign~~ intriguing story will find excellent reading material in various book dealing with it. Those of you who are interested only in its cryptologic aspects will find excellent material in the following three documents:

indent single space

(1) "The Cipher Dispatches." The New York Tribune, Extra No. 44, New York, ~~1878~~ (14 January) 1879.

Insert

The existence of these 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 provided against in the Constitution. A crisis arose and the country seemed on the verge of another civil war. By an act of 29 January 1877, Congress created a special electoral commission to settle the disputed electoral 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 which Congress felt it had to look into. Somehow or other copies of the telegrams came into the possession of a Republican newspaper, The New York Tribune, in the summer of 1878, and two members of its staff succeeded in solving those in cryptographic form.

Hassard, John R.G.

single space + indent

(2) "Cryptography in Politics." The North American Review, Vol. CXXVIII, No. 268, March 1879, pp. 315-25.

(3) "U.S. House Miscellaneous Documents, Vol. 5, [redacted] 45th Congress, 3rd Session, 1878-79. [redacted]

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 a Prof. 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 ciphers but only after Mr. John R.G. Hassard, the chief of The Tribune staff, and his colleague, Col. William M. Grosvenor, also of that staff, had reached a solution.

Prof. Holden's testimony is of considerable interest. He presented his solution of the nearly 200 cryptograms entered in evidence. His testimony is summarized in a letter dated 21 February 1879 and it sets forth all the cryptosystems used by both parties, ~~together~~ with their keys and full details of ~~[illegible]~~. In that letter Prof. Holden makes the following statement: "By September 7, 1878, I was in possession

~~tails of these applications~~ * Prof Holden in his letter makes this statement: "By September 1878, I was in possession of a rule by which any key to the most difficult and ingenious of these (the transposition cipher of Democrats) could infallibly be found". Holden worked out the transposition keys but in that he was of course ~~was~~ anticipated by the Tribune cryptanalysts. There were ~~the keys, although Holden independently discovered them~~ in all 10 different keys, two for messages of 10 words, two for messages of 15 words, etc., up to and including ~~to~~ two for messages of 30 words. Here is the complete table of keys:

leave 1/4 page space

[¶ insert over] → ~~I may~~ suspect that the basic or "verse" sequences of numbers were not drawn up at random but were derived from ~~the~~ words or phrases; and I suspect that the odd-numbered ones are the "verse." 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 key word or phrase.

In addition to transposition this system involved the use of code words to represent certain words and ~~the names~~ of certain persons and places, and numerals. There were also a few nulls. Here is the entire vocabulary:

leave 1/4 page space

Footnote ~~* See pp. 315-385 of U.S. House Miscellaneous Documents Vol. 5, 45th Congress, 3d Session, 1878-79. See also article by John R.G. Hassard, Cryptography in politics, in The North American Review, March 1879, pp. 315-325. (Vol. CXXVIII, No. 268)~~

You may be wondering why there are two transposition keys for each length of message from 10 to 30 in multiples of 5. The two keys constitu[illegible] ~~the~~ a pair are ~~correlatives of each other~~ related to [illegible] other; that is, they bear a relationship ~~something~~ which one of the Tribune cryptana[illegible] termed "correlative," but which we now would [illegible] an "encipher-decipher" or "verse-inverse" relationship. Either sequence may be used to encipher, the other, ~~the other can be used~~ to decipher a message. For example, key III consists of the following: 8-4-1-7-13... etc, and the correlative, key IV, is 3-7-12-2-6... etc. A cipher message of 15 words can be deciphered either by (1) numbering ~~the~~ words consecutively and then ~~[illegible]~~ assembling the words in the order 8-4-1-7-13 etc, or by (2) writing the sequence 3-7-12-2-6... above the words of the cipher message and then assembling the thus-numbered words according to the sequence 1-2-3-4-5... . Thus, there were, in reality, not 10 different transposition keys but only five. In the case of ~~each~~ pair of keys one of them must have been the basic sequence, the other the inverse of it. ~~derived sequence~~.

Prof. Holden adds some comments about this system, which are worth presenting:

indent & single space

> The essence of this ingenious and novel system consists in taking apart a sentence written in plain English (dismembering 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~~ the verse-inverse relation in each pair of sequences, or, if he did, he failed to mention it, as Hassard 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 their the most complicated of the cryptosystems involved in this bizarre political episode, became quite clear.

[Insert over] ~~But~~ There were several other ~~[illegible]~~ systems involved, but I am going to have to pass them ~~of which only one or two deserve~~ by because they hardly deserve attention in this brief history. I do, however, want to call your attention to the very close resemblance between the word-transposition ciphers ~~what was~~ characterized by Prof. Holden as "the most difficult and ingenious" of the ciphers he solved, and the USMTC route ciphers ~~of the USMTC which I~~ described in ~~and which, technically considered, were much simpler~~ the preceding lecture. Yet, not only he but also the Tribune amateur cryptanalysts solved those ciphers even though they were technically more complex. without too much difficulty, ~~or delay~~. I think their work confirms my own appraisal of the weakness and futility of the route ciphers used by the USMTC in the Civil War. ~~as ciphers of [illegible]~~

Let us now go on with cryptologic history after this ~~political~~ digression into the realm of what may be called political cryptology. I do not know what the Department of State used

Insert

25
U
100

Another system used by the conspirators used a 2-letter for one letter substitution and was based upon a 10X10 checkboard. Apparently neither Prof. Holden nor the Tribune cryptanalysts recognized the latter principle, nor did they find that the coordinates of the checkerboard employed a key phrase, ~~which, appropriately enough, was "HIS PAYMENT."~~

~~/~~			~~H~~	~~I~~	~~S~~	~~P~~	~~A~~	~~Y~~	~~M~~	~~E~~	~~N~~	~~T~~
			~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~0~~
	~~H~~	~~1~~										
	~~I~~	~~2~~										
	~~S~~	~~3~~										
	~~P~~	~~4~~										
	~~A~~	~~5~~										
	~~Y~~	~~6~~										
	~~M~~	~~7~~										
	[illegible]	~~8~~										
		~~9~~										
		~~0~~										

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 figure cipher:

leave 1/4 page space

They are long enough for solution, if you wish to try to solve them and find the key phrase, which ~~will~~ should 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. LXXXV, No 1, Nov. 1912, a man named John H. Haswell, apparently a code clerk ~~in the Depart-ment~~, referred to "a new code of the department in the following terms:

Single & space indent

> The cipher of the Department of State is the most modern of all in the service of the Government. It embraces the valuable features of its predecessors and the merits of the latest inventions. Being used for every species of diplomatic correspondence, it is necessarily copious and unrestricted in its capabilities, but at the same time it is

single space & indent

economic in its terms of expression. 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 certain telegraph operator and code clerk of the State Department proved how vulnerable the Department's system of enciphered code really was. His name was Herbert O. Yardley and many of you may know a bit about him because he was the author of a famous or infamous "book (depending upon whose side you're on) entitled The American Black Chamber, which was published by The Bobbs-Merrill Co. in 1931. So far as I know it is the only book which cannot legally be reprinted in the United States because a special law ~~but is forbidden by~~ ~~forbids~~ makes it a criminal offense to do so. passed in 1934. That is quite a story in itself but I cannot tell it now." ~~[illegible]~~ So if you happen to own a copy of the first and only American edition ~~it, 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 able to purchase an English edition by a similar sort of deal. But to return to that State Department cryptosystem considered by Haswell "to secure absolute secrecy," here is the cover page of Yardley's 21-page typewritten analysis.

leave 1/4 page space

Yardley was quite wrong in thinking that his was the first successful attempt to solve a problem in enciphered code, for in Europe successful attempts on more complicated cases were often the rule and I ~~haven't the slightest doubt that the British~~ imagine that British cryptanalysts could have and perhaps did read ~~cryptanalysts were quite successful in reading~~ State Department messages as a more or less routine ~~regular~~ matter. For in Europe, cryptanalytic studies were going on apace during the years of American neglect of such studies.

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 very large codebook, 18" long, 12" wide and 2" thick, which had the official title The U.S. Navy Secret Code, and an accompanying but separate cipher book almost as large, and ~~officially~~ designated as a the book of Key Words. In addition to these two books was a third book called "General Geographical Tables. The system was placed into effect on 1 December 1887. About 10 years later a new edition of the third book was placed into effect. Later I will show you a most historic message sent in that clumsy system of secret communication.

In our Army in the middle eighties, too, 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 apparently popular~~ small code first published in 1870 for use by the general public ~~under the title~~: Telegraphic code to ensure secresy in the transmission of telegrams, by Robert Slater, secretary of the French Atlantic Telegraph Co. [Insert next] ¶ Slater's ~~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 (1879), 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 easily see in the picture I show you next. It would appear that Col. Gregory was just a bit deficient

Insert

As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using this work":

Single space & indent

> It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No., [from 6001 to 25000, with exactly 100 words per page], 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 as thus far described is what we now call an additive or subtractor ~~system~~ 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 ~~code~~ words standing alongside the sum (or difference) of the mathematical operation be sent.

in imagination because, not only did he simply borrow the basic idea of Slater's code but also when it came to preparing the rules for and examples of enciphering the code groups the colonel used the identical rules and wording, and even the same type of transformations of those that are found in Slater's original. ~~In the latter,~~ for Let me show Example I of Slater's code side by side with the same example from Gregory:

leave 1/2 page space

All the other methods and examples in the two codes are practically identical. Colonel Gregory gives credit to a civilian aide, in the following terms: "The labor of compiling the new vocabulary has been performed by Mr. W. G. Spottswoode." And Mr. Spottswood's work consisted in casting out such words as ABALIENATE and ABANDONEE from Slater's list and replacing them with such words as ABATEMENT and ABATIS. This sort of work must indeed have been arduous. I'm sorry to appear to be so critical of my predecessors in the construction of codes and code systems for War Department and Army usage, but I feel sure you will agree that more imagination and ingenuity could have been employed than were used by Messrs. Gregory and Spottswood.

Col. Gregory prepared a confidential letter to Lieut. General Sheridan", Commanding Army of the U.S.", to explain the beauties 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 from Col. Gregory to Lieut. General Sheridan is printed in toto in Appendix I, ~~to this letter~~ to which I have added ~~the~~ Col. Gregory's "Introduction" ~~that Col. Gregory proposed~~ 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 additive, because in a copy in my collection the additive is written on the inside of the front cover. It was 777. In pages 41-42 of The American Black Chamber the author throws an interesting sidelight on this code system:

single space & indent

> The compilation of codes and ciphers was, by General Orders [he 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 attache to an Allied country. It was not intended that attaches should actually

encode 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 attache, 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 as children we read in Poe's *The Gold Bug*.

single space + indent

He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard of 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 years just before our entry into World War I are true enough and Yardley's impatience and satires in this regard are ~~fallacious~~ unfortunately fully warranted.

We have noted how inadequately the Army and the War Department were equipped for cryptocommunications in the decades 1890-1910. Let us see how well equipped ~~the~~ Navy and the Navy Department were. For this purpose I have an excellent 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 cryptosystem for the Navy and I told you about the large basic codebook and its ~~accompanying, enciphering~~ almost as large a book for the code groups. For the ~~the afternoon of 25 February 1898, a~~ On Saturday, ~~the Secretary of the Navy,~~ ~~John D. Long,~~ ~~had taken off perhaps~~ for home, ~~for a nap or a game of cards,~~ ~~leaving Theodore Roosevelt, the Assistant Secretary in charge of the store. It was Teddy's opportunity for a bold move unhampered by his superior.~~

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. Teddy 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, and stirred 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, Teddy sat down and wrote out a cablegram to go to Commodore George Dewey. Here it is, with his bold signature at the bottom:

cablegram

leave 1/4 page space

That was the now historic 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 that 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 code cablegram as it was received in Hong Kong.

[Leave 1/2 page space]

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 the~~ consult and use the necessary ~~two~~ books from Navy Security archives. To translate a message three steps are necessary. First, ~~the~~ cable words (the peculiar, outlandish words in line 2 — WASSERREIF PAUSATURA BADANADOS, CENTENNIAL, etc.) are sought in the cipher book, and their accompanying cable-word numbers set down. WASSERREIF yields 99055, PAUSATURA yields 62399, BADANADOS, 11005; CENTENNIAL, 16820. The next step is to append the first digit of the second cable-word number to the last digit of the first cable-word number to make the latter a six-digit number. Thus 99055 becomes 990556. The six-digit code-group 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 straightford, mathematical method of solving the Vigenere cipher was published in Berlin during the mid-period of the Civil War in America. If the book created an add 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 explained quite accurately in the first American text on cryptology, Capt. Parker Hitt'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 in Europe during this period, among which the more important were the following:

leave 1/2 page space

Of the foregoing two deserve special mention. The first, by Commandant Bazeries, 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 cylindrical cipher device, a picture of which I

I now show you. But our own Thomas Jefferson anticipated Bazeries 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 in the foregoing list which is deserving of attention is the one by de Viaris, in which he presents methods for solving cryptograms prepared by the Bazeries cipher cylinder 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, ~~for~~ 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 or departing from telegraph offices or in transit through them. This was true in the case of every country in Europe with one very important exception: Great Britain. The story is highly interesting but I must condense it to a few sentences.

In England from about the year 1540 onward a black chamber was in constant operation. It was one of two collaborating organizations called The Secret Post Office and the Office of Decipherer. ~~Th~~

A famous mathematician, John Wallis, took part in the activities of the Office of Decipherer. But in 1844

In the former, letters were opened, copies of them were made, the letters replaced, the envelopes resealed, and if there were wax 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 completely down, so that from 1844 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 ~~the~~ England's black chamber had to start from scratch, but British brains and ingenuity within a few months built a cryptologic organization, known as "Room 40 O.B.", which contributed very greatly to the Allied victory in 1918.

Perhaps the greatest ~~and most important~~ achievement of Room 40 O.B. was the interception and solution of what is, known as the Zimmermann Telegram, deservedly called the most important single cryptogram in all history. On 8 September 1958 I gave an account of this cryptogram, its interception, its solution

an operation which just in the nick of time brought this country into World War I as an active belligerent on the Allied side. The operation involved under the auspices of the NSA Crypto-mathematics Institute, was recorded and is on file. It

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 plain-text was obtained, least of all that it had been obtained by interception and solution 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 important 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 astutely 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 feat 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

REF ID:A62844 CONFIDENTIAL (23)

~~From~~ the day that Ambassador Page sent his ~~cable~~gram to President Wilson ~~on~~ (24 February 1917) quoting the English translation of the Zimmermann Telegram ~~as it was~~ in the form in which it had 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. Under big black headlines the English text appeared in our newspapers on 1 March. [Indent over] ~~and on 6 April 1917~~ that the United States Congress declared war on Germany and the Central Powers. The date was 6 April 1917.

In the War Department, and in the Navy Department, the pace set for preparing for active war operations quickened. There was at the moment ~~no organization~~ in neither of those departments, nor in the Army or in the Navy ~~— nor in the Army, nor, for that matter, in the Navy Depar tment — in the Navy~~, any organizations whatever, either for intercepting enemy communications or for studying ~~for cryptanalytic operations on them. The~~ them. There was, it is true, since the autumn of 1916 a very small ~~a privately supported small~~ group of self-trained cryptanalysts, supported by a private citizen named Colonel* Fabyan who operated the Riverbank Laboratories at Geneva, Illinois. That organization maintained an unofficial relationship with the authorities in Washington and ~~established a small school for training military~~ ~~which~~ received from time to time copies of cryptographic messages obtained ~~by surreptitious means~~ from telegraph and

Fot note * Honorary title, conferred by the Governor of Illinois for Fabyan's participation as a member of the Peace Commission that negotiated the Treaty of Portsmouth, which followed the Russo-Japanese War in 1906.

Insert

For instance, here is the bold black 8-column 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 subheads that extended halfway down the page, beginning with:

MEXICO AND JAPAN ASKED BY GERMANY
TO ATTACK U.S. IF IT ENERED 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 thes furor that the disclosure of the Zimmermann 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 representatives who disbelieved the story. It was too fantastic; it was a British plot, unproved; Wilson was being taken in, etc., etc. But when Zimmermann himself foolishly acknowledged that he had indeed sent such a telegram, disbelief changed quickly into vehement anger. Surely war would now be declared on Germany!

REF ID: A62844 ourselves for this unusual task, and later, what we used later on for training the student officers sent to Riverbank for cryptologic instruction. As

Begin insert

¶ You may like to know what we ~~regarded~~ our self-instruction training material, ~~Well~~, there wasn't much but among the very sparse ~~literature~~ in English there was a small book entitled Manual for the Solution of Military Ciphers, which had been prepared by a Captain Parker Hitt and printed ~~at~~ by the ~~Leavenworth~~ Press of the Army Service Schools at Fort Leavenworth, in 1916. The Signal Corps School was then a one of those ~~Army Service~~ Schools, ~~at Leavenworth and where~~ and there a few lectures were given by ~~two or three~~ officers who, when World War I broke out in August 1914, took an interest in the subject of military ciphers. ~~Messrs~~ They foresaw that sooner or later there would ~~might~~ be a need for knowledge in military cryptology and training. Capt. Hitt's Manual was then and still is a model of compactness and practicality. Here is its title page.

Fig. DD

It was the ~~succinctness~~ of the Manual that caused us ~~to sweat~~ much work and perspiration in our self-training. I later came to know and ~~very much~~ admire its author, whose photograph I show you.

There was one other item of training literature which we studied avidly too, a very small pamphlet entitled An advanced Problem in Cryptography and its Solution, put out by the same Leavenworth Press in 1914. Here is its title page, and a photograph of its author, then 1st Lieut. J.O. Mauborgne, but later Chief Signal Officer of the Army. The advanced problem dealt with by that pamphlet was the Playfair cipher, about which I shall say something later.

¶ Returning now to what our self-trained cryptanalytic group was able to do in a practical way in the training of others, there should be in NSA archives the ~~notes~~ exercises and problems prepared at Riverbank for this purpose. They are still of much interest historically.

(At that period in our history ~~our~~ diplomatic relations with Mexico were in a sad 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.) ~~Under my direction~~ Riverbank ~~operations of this group, which~~ was successful in solving all or nearly all the Mexican cryptograms it was given, usually returning the solutions to Washington very promptly. It was also successful with certain other cryptograms but I cannot deal with them now because there just isn't time.

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. [Insert over] ~~In~~ Lecture II (Fig. 27) there is a picture of the last of the several classes sent by The Adjutant General of the Army to Riverbank for training. It should be noted that this 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 first lieutenant and ordered immediately to proceed to American General Headquarters in France where I became a member of the German Code and Cipher Solving Section of the General Staff, a designation that was abbreviated as 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~~ Army field ciphers, the other, to working on German Army field codes. There were other very small groups working on other material such as meteorological messages, reports on direction-finding bearings, and what we now call traffic intelligence, that is, the study of enemy messages in order to determine enemy order of battle from an analysis ~~of the bearings~~ of the direction, ebb and flow of enemy radio traffic and other data sent back from our direction-finding operations at or near our own intercept stations.

In connection with the last-mentioned operations you will no doubt be interested to see what is ~~perhaps~~ one of the earliest, if not the very first chart in cryptologic history that shows ~~showing~~ the results of traffic analysis and its utility in deriving intelligence about enemy intentions from a mere study of the ebb and flow of enemy traffic,

Fig 00

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 ~~the~~ a clever cryptosystem devised by German cryptographers and only ~~one~~ used for German High Command communications, principally between and among the headquarters of divisions and army corps. Theoretically it was ~~a very~~ extremely secure ~~cryptosystem~~, because it combined both a good substitution and an excellent transposition principle in one and the same method without being too complicated for cipher clerks. Here is a diagram which, if ~~you will look at~~ ~~it~~ ~~and~~ ~~if you~~ studied carefully, ~~you~~ will give a clear understanding of its method of preparation and usage. If you ~~should~~ wish further details I suggest you consult documents available in the ~~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, a great many messages ~~about 50% of all the~~

*Initially this cipher employed only the letters A,D,F,G, and X, for a matrix 5×5; later, the letter V was added, for a matrix 6×6.

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 in those days three and only 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 A, D, F, G, V and X 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 messages with identical beginnings. You might think that cases of messages with identical beginnings or endings would be rather rare, but the addiction to stereotypic phraseology in the German military mentality was then — and perhaps still is — so confirmed, 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 a very able ~~French~~ cryptanalyst named Capt Georges Painvin 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 50% of all messages sent in that cipher were ~~solved~~ read and a great deal of valuable intelligence was derived. On one occasion solution was so rapid that an important German operation dissolution depended upon the three rather special cases mentioned.

closed by one message was completely frustrated.

Although the ADFGVX 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 13-part message in that key gave the complete plan of the German retreat from Roumania.

During the whole year of the life of the ADFGVX cipher, No general solution for it was devised by the Allies despite a great deal of study. However, members of ~~the~~ our own Signal Intelligence Service, in 1933, and while still students undergoing instruction in cryptanalysis, devised a general solution and proved its efficacy. ~~Their~~ Pride in their achievement was not diminished when, in the course of writing up and describing their method, a similar one was encountered in a book by French General Givierge (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 called "the Wilhelm," which used a cipher square with a set of 30 fairly lengthy keywords. The cipher square is shown in Fig. 00 and the set of keys as originally recovered is shown in Fig. 00. Just why the square contains only 22 rows instead of 26 is unknown. Certainly the rows within the square are not random sequences, for the letters within them manifest permutated arrangements in sets of fives; nor are the keys sequences of random letters. I leave it to you to try 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 disarrangent, something typical of German cryptography.

The other cipher to be mentioned is the double transposition, an example of which is shown in Fig. 00. The process consists in applying the same transposition key twice. Solution of the true double transposition 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 find two messages of identical length. Having demonstrated the weakness of the system, even when properly employed, it probably was withdrawn from usage by the British, but we were not told directly that this was done. I should add that I think the devising of a general solution for the true double transposition cipher 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 could hardly be thought to be safe for modern military secret communications.

We come now to the code systems used by the belligerents in World War I. And first, let us ~~Review quickly what the Am~~ differentiate those used for diplomatic communications from those used for military communications. What sorts did the German Foreign Office use? We have noted how the British Black Chamber, "Room 40 O.B." dealt with stupendous 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 attacks.~~ Excessive pride in German achievements, a wholely unjustified confidence in their cryptosecurity, and a disdain for the ~~cryptanalytic~~ prowess of enemy cryptanalysts laid German diplomatic communications open to solution by the Allies to the point where there came a time when nothing the German Foreign Office was ~~thinking about~~ ~~and~~ telling its representatives abroad by telegraph, cable or radio remained secret from the British. For those of you who would like to learn some details, I refer you to the ~~final~~ following monographs on the subject by my late colleague, Captain Charles J. Mendelsohn: Studies in German Diplomatic Codes Employed During the World War, Government Printing Office, 1937. This monograph is confidential; ~~and~~ copies are available in the Office of Training, NSA.

"At the time of ~~American~~ entrance into the war, German codes were an unexplored field in the United States," says Dr. Mendelsohn. "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 19,200 words and 800 of the possibly 7,600 proper names). This code and its variations or encipherments had been in use between the German Foreign Office and the German Embassy in Washington up to the time of the rupture in relations, and our files contained a considerable number of messages, some of them of historical 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 two columns of 50 each accompanied by numbers from 00 to 99. Here is a copy of a typical page in Code 13040. In each column the groups were in blocks of 10, in the left-hand column, for instance, 00-09, 10-19, etc, to 40-49; then 50-59, etc. The pages in the basic code were numbered at the top from 10 to 239 and from this code several ~~and~~ derivative codes were made ~~based~~ by the use of conversion tables. This ~~upon the basic which~~ enabled ~~a~~ the original single basic code to serve ~~as a basis~~ as the framework for codes for several different communication nets. What the number of the basic code was is unknown, but we do know that from the derived code designated as 13040 came codes 5950, 26040, and others, derived ~~a codes designated as 5950 and 26040 were derived~~ merely by means of ~~a~~ tables for converting the page numbers in the basic code into ~~a~~ different page numbers in the derived code ~~In addition there were tables for converting the line numbers (from 00 to 99) on the page from one code to the other.~~

These conversions were systematic, in blocks of fours: Thus, for example, pages 15-18 in code 13040 became pages 65-68 in code 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~~ code into different ~~line~~ line numbers in another version of the basic code, and this was done in blocks of 10. For example, the fifth block (penultimate figure 4) became the first (penultimate figure 0), and the 1st, 2nd, 3rd, and 4th blocks were moved down one place.

[Continue over]

The other five blocks (right-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 can by no means be considered as ~~represent the equivalents of~~ being different codes; they were all relatively minor ~~are the~~ equivalents of ~~these~~ 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 [etc. continue with p.33]

Some of ~~these~~ besides the ones already mentioned (13040 and 5950), ~~were designated~~ by indicators such as 12444, 1357, 18470, 1777, 2815, 4565, 5717, 44499, 58585, 2310, 98989, 1111, 80574; ~~there were~~ others besides these. [Insert over]

true two-part code, since the same book served for both encoding and decoding. However, the German Foreign Office later on did compile, and use ~~had~~ true two-part, truly randomized codes of 10,000 groups numbered from 0000 to 9999. One such code had as its indicator the number 7500. And that there were several others like it I have no doubt.

When one reviews Dr. Mendelsohn's monograph one becomes ~~is~~ overwhelmed by the ~~[illegible]~~ multiplicity of the codes and variants thereof used by the German Foreign Office. ~~Not~~ Many were basic codes but ~~and how~~ many were derivatives, or superencipherments thereof. It is even hard to ascertain the exact number of different methods. Yet a great deal of the traffic in these codes was read. Considering the rather small number of persons on the cryptanalytic staff of G-2 in Washington and its homologous organization in ~~the~~ London, in the British Black Chamber, one can only be astonished by the great achievements of the ~~collaborative~~ efforts of these two collaborating organizations during World War I.

~~So much for the German diplomatic cryptosystems. What about the German Military Cryptosystems? In this area we must credit the Germans with being the initiators of most of the new ideas and improve- first to decide that the old idea that a code could not be practically or safely employed in the field for tactical communications was not valid.~~

Insert

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 versions of the basic code were not actually printed as separate books ~~so that code 13040 [illegible] was~~ but that the original, page number on each page was altered by hand, ~~the original~~ number being crossed out and ~~entirely different in its appearance~~ the new number written either at the top or the bottom of the page, perhaps in both places. Similarly, the block numbers were probably changed by hand. In both cases the alterations were ~~chosen~~ in accordance with some system, and for the idea of randomicity seems foreign to the German mentality, ~~the Germans never do anything by random~~ I am sure that if randomicity 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 communications. 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 speedy and secure crypto-communications. Numerous complaints were registered by German commanders concerning extensive loss of time occasioned by the far too complicated methods officially authorized for use and the consequent necessity for sending messages in the clear. Not only did this reveal intelligence 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 ~~are~~ became of great importance in cryptanalysis when German cryptosystems improved. For the German Army learned by hard ~~experience~~ something about ~~and learned rapidly because~~ its shortcomings in this area of warfare and began to improve to the point where we must credit the Germans with being the initiators of most of this new and very important developments in field military cryptography. In fact, the developments and improvements began not longer after the ~~outbreak~~ ~~of the war~~ the Battle of the Marne and continued steadily until ~~the~~ end of the war. When on 11 November 1918 the armistice ended active operations, German military cryptography had attained a remarkably high state of efficiency. The astonishing fact, however, 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 save 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 cryptologic 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 principally ~~only~~ concerned with 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 and published in Stockholm in 1931 by a Swedish cryptanalyst, Yves Gyldén, 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 in the World War, Government Printing Office, 1936.

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 communications was wrong. They had two different types of
which the Germans called the SCHLUESSELHEFT or "key ~~but which~~
field codes, one we called the "three-number code";
which the Germans called the SATZBUCH or "Sentence Book" but which we called
the other, the "three-letter code". The former
a small vocabulary of
was standardized code with a frequently-used
digits, letters and syllables totally 1,000 ~~words~~ for
words and expressions, which the code equivalents were 3-digit numbers. A cipher was applied
only first two digits of
to the code numbers and this cipher consisted of a 10 x 10 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
compiled by the end of January 1918 it was
danger zone. Although this code was not put into use until the opening day of the last and greatest German
nature of the
offensive 10 March 1918. The new code was ascertained
and ~~the~~ few 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 new code 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 five-number proved rather easy to solve on a daily basis and much useful intelligence was obtained thereby.

The solution of 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 and what constituted ~~but what became~~ 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 ~~but~~ as to the sector ~~from~~ to 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 ~~in~~ within a quiet sector of the front and trying to solve a few messages in the code was really a painfully slow, very diff~~icult and~~

generally frustrating experience. On my reporting for duty Colonel Frank Moorman, who was chief of the whole unit and whose photograph I show you here, asked me whether I wished to be assigned to the cipher ~~solvers~~ 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~~ to be assigned to the code solving unit. I gained the experience I wanted and needed to broaden ~~I~~ my knowledge and practice in cryptology but little did I realize what ~~I was in~~ 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 experiences in this area, let me refer you to my monograph entitled Field Codes Used by the German Army during the World War, copies of which are on file in the Office of Training, NSA. I will quote a few [insert over]

What sort of cryptosystems did the French Army use? First, as for ciphers, they put

Insert

paragraphs from my "estimate of the three-letter code" ~~taken~~ as it appears on p.65 of that monograph:

p. 65

much trust in transposition methods and here is an example of one type:

Fig. 00

As for codes, like the Germans they used ~~some of~~ a small front-line booklet, called a "Carnet Reduit," or an "Abbreviated Codebook," ~~for~~ various sectors of the front had different editions, and I will show a picture of one of them. Then, in addition, there was a much more extensive ~~two~~ code which was not only a two-part, randomized book of 10,000 four-digit code groups, but a superencipherment was applied to the code messages when transmitted by radio or by "TPS," that is, "telegraphie par sol", or earth telegraphy. Here is one of the tables used for enciphering (and deciphering) the code groups:

Fig. 00

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

Fig. 00

You will notice that the enciphering process breaks up the 4-digit groups in a rather clever manner by enciphering ~~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 digital 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, theoretically at least, 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. ~~[illegible]~~ I venture the opinion that it was not used often, or successfully, with the superenciphering method provided for the basic code.

Now 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 field code. It ~~was~~ 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 even have a copy of their code — only a typewritten transcript which was furnished us quite reluctantly and I will show a typical page thereof.

Fig. 00

~~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 show you a picture of it here:~~

~~Fig. 00~~

~~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 in Italy a far greater 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 makes filing away in dusty archives records of cryptanalytic successes a desideratum but also ~~presents~~ hinders or absolutely prevents those who might have been born with what it takes to ~~[illegible]~~ 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 "cifrario militaire tascabile" or the "pocket military cipher"? It, 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 encipherment 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 same Italian "expert" announced his invention of an absolutely indecipherable cipher system which, Gylden says (p. 23) "still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on his part."

What about Russian cryptologic 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~~ bureau for constructing and compiling diplomatic codes and ciphers, 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 Bolshevik revolution of 1916 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 successes 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 a cryptographic system which proved to be too complicated for the ignorant and poorly trained Russian cipher and radio operators to use when it was placed into effect toward the end of 1914. Here is an example of that cipher, which has an enciphering and a deciphering table:

Fig. 00

In the enciphering table the letters of the Russian alphabet (33 in all) appear in the top line; the 2-digit groups in random order within the 8 rows below are their cipher equivalents and these ~~are in random order in each row, thus~~ rows therefore constitute a set of 8 cipher alphabets ~~each of which~~ is preceded by key numbers from 1 to 8 in random order, also subject to change. Indicators were used to indicate how many letters were enciphered consecutively in each alphabet, the indicator consisting of one of the digits from 1 to 9 repeated five times. The alphabets were then used in key-number sequence, 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 cipher alphabet 8, return is made to cipher alphabet 1, repeating the sequence in this manner until the entire message had been enciphered. In enciphering a long message the cipher operator could change the number of letters enciphered consecutively by inserting another indicator repeated five times and then continuing with the next alphabet in the sequence of alphabets. The cipher text was then sent in 5-digit groups. The use of the deciphering table hardly requires explanation but a ~~comment~~ question may be in order: Why ~~was there any~~ the aversion 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 was 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 communications became known to the German and Austrian High Commands within a few hours after transmission 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 inept that not only were their cipher messages easily solved but also they made so many errors that the intended 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 the Russian. To send out dispositions, impending 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 criminology. 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,

[Continue over]

p. 96 continued

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 first 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 that extensive code for administrative telegraphic correspondence, the 1915 edition of the War Department Telegraph Code about which I've 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 principles 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. 00, and will let you assess its security yourself.

Fig. 00

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 cryptology 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 lecture, so the invention of radio also played a very important role in field communications during World War I. Now, although it can hardly be said that all commanders from the very earliest days of the use of radio in military communications acutely 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 increased use of cryptology that this service 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 cryptocommunications except those three inadequate means I've 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 ~~[illegible]~~ "Trench Code", of which 1000 copies were printed, together with what were called "distortion tables." These were simple monoalphabets for encipering the 2-letter groups of the ~~[illegible]~~ code. I show a picture of a page of this code and of one of the "distortion tables."

Fig. 18 (P13:)

Fig. 00 (P142)

The danger of capture of these codes was recognized as being such that the books were not issued below battalions. Hence, to meet the needs of the front line, a much smaller book was prepared and printed, called the "Front Line Code". Distortion 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 inexperienced personnel in cryptanalysis. Finally, the light broke through: the Code Compilation Service began to see the advantages of the German 3-letter randomized 2-part code known as the Satzbuch. I've 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 "American River Series", appeared on 24 June 1918, in an edition of 2,000 copies. It contained approximately 1,700 words and phrases and, as the official report so 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 commonsense sense:

"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 ciphering 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 Potomac, 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 Suwanee, 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" for the Second Army was issued with the Colorado of the "River Series" for the First Army; these were followed by the Huron and the Osage, the Seneca 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 message among the higher commands in the field and between these and GHQ. This was a task of considerable magnitude and required several months' study of messages, confidential papers concerning organization, replacement, operations, and of 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 a field printing organization and I believe that this was the largest and most comprehensive codebook ever compiled and printed by an 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 superencipherment 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 ~~was~~ 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

Copies are on file in the Office of Training.

in 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 the codes and ciphers produced and used not only by the AEF but also by our allies and enemies during that conflict.