

## 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 awoke at long last, about 1914, 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 the short war with Spain, in 1898. For over three decades there was little or no need for cryptography in the United States Government, except for the communications of the Department of State. The military and naval services apparently felt that in time of peace there was no need for either cryptography or cryptanalysis, and since it looked as though the US was going to enjoy peace for a long, an indefinitely long time, those services did not think it necessary or desirable even to engage in theoretical cryptologic studies. Of course, the War Department and the Army still had those route ciphers and cipher disks/ described in the preceding lecture; the Navy Department and the Navy had cipher disks for producing simple monoalphabetic ciphers; and the Department of State had a code more or less specifically designed for its communications. Separated from Europe by the broad Atlantic, and mindful of General Washington's policy of non-involvement in the problems of European diplomacy, America followed the traditional and easy course of isolationism. The quarrels among the countries in Europe were none of our business and America stood aside for a half century, not even interested in those disputes.

There was, however, in this long hibernating period in U. S. cryptology one episode of particular interest. It concerned a Presidential election in which the circumstances paralleled the election of 1960, when the very small popular-vote majority of the Democratic candidate suggested a possible upset in the electoral college voting. The episode to which I refer here occurred nearly a century ago, 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 evening election returns Tilden seemed to be easily the winner. Indeed, just before going to bed on election night, 8 November 1876, Hayes conceded the election to Tilden, and, in fact the newspapers next morning reported a Tilden victory. But when final tallies began coming in they showed that the closeness of the popular vote made Tilden's victory not so sure as his supporters had calculated, and they

therefore began to become apprehensive about their candidate's victory. Their apprehensions were valid because of our peculiar system of electing a president, peculiar because it is the electoral and not the popular vote which determines who is to be the next occupant of the White House as 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 they needed and they didn't hesitate to try every possible ruse to obtain it, including bribery, a rather serious piece of business and one obviously requiring a good deal of secrecy, especially in communications. Of course, many telegrams had to be exchanged between the Tilden headquarters in New York City and confidential agents who had to be sent to certain states where one or more electoral votes could perhaps be purchased; telegrams also had to be exchanged among those secret agents in the field. About 400 telegrams were exchanged and some 200 of these <sup>were</sup> <sub>in</sub> cryptographic form. I feel sure that you will be interested to learn that because of communication difficulties two almost-consummated bribery deals fell through; a third deal failed because the electors proved to be honest Republicans not susceptible to monetary temptation. The existence of these telegrams, however, remained unknown to the public for months and we shall come to them later. Despite the efforts of the Tilden supporters, 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 for in the Constitution. A crisis arose and the country seemed to be on the verge of another civil war. By an Act of 29 January 1877, Congress created a special electoral commission to investigate and decide upon the matter of the disputed electoral votes in the four states. Recounts of votes in certain election precincts were made, sometimes aided by soldiers of the Federal Army. The commission voted in favor of the Hayes electors in each case, and, having obtained the needed 22 electoral votes, Hayes entered the White House. 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, in the summer of 1878, copies of those telegrams had come into the possession of a Republican newspaper in New York City, The Tribune. Interested only in ascertaining the truth, the editor put two members of his staff on the job and they succeeded in solving those telegrams which were in cipher.

Various books dealing with the political aspects of this intriguing story are available in public libraries, but those of you who are interested only in its cryptologic aspects will find excellent material in the following three documents:

- (1) "The Cipher Dispatches", The New York Tribune, Extra No. 44, New York, (14 January) 1879.
- (2) Hassard, John R. G., "Cryptography in Politics", The North American Review, Vol CXKVIII, No. 268, March 1879, pp 315-325.
- (3) Holden, Edward S., The Cipher Dispatches, New York, 1879.
- (4) U. S. House Miscellaneous Documents, Vol 5, 45th Congress, 3rd Session, 1878-79.

The last-mentioned item, that put out by the Congressional House Committee which had been designated to conduct the investigation and which was named "The select Committee on alleged frauds in the Presidential Election of 1876," is of special interest. In the course of the investigation, the Committee solicited the technical assistance of Professor Edward S. Holden, of the United States Naval Observatory in Washington, the author of the third item listed above, <sup>who</sup> I believe ~~he~~ was a captain in the Navy and had specialized in mathematics. The Tribune had brought him into the picture by asking his help when solution seemed hopeless but it turned out that Mr. John R. G. Hassard, the chief of The Tribune staff, and his colleague, Colonel William M. Grosvenor, also of that staff, solved the ciphers independently ~~of~~ and, in fact, shortly before Prof. Holden solved them, although it was the latter that the Congressional Committee called upon to explain matters, as would only be natural under the circumstances.

Professor Holden's testimony, in which he set forth his solution of the nearly 200 cryptograms entered in evidence, is presented in the form of letter to the Committee, dated 21 February 1879. In it ~~he~~ described and explained all the crytosystems used, together with their keys and full details of their application. In that letter, Professor Holden makes the following statement: "By September 7, 1878, I was in possession of a rule by which any key to the most difficult and ingenious of these [ciphers] could infallibly be found." Holden worked out the transposition keys but in this he had been anticipated by the Tribune cryptanalysts. There were in all 10 different keys, two for messages of 10 words, two for messages of 15 words, etc., up to and including two for messages of 30 words. Here is the complete "Table of Keys":

TABLE OF KEYS

10 Words		15 Words		20 Words		25 Words		30 Words	
I	II	III	IV	V	VI	VII	VIII	IX	X
9	4	8	3	6	12	6	18	17	4
3	7	4	7	9	18	12	12	30	26
6	2	1	12	3	3	23	6	26	23
1	9	7	2	5	5	18	25	1	15
10	6	13	6	4	4	10	14	11	8
5	3	5	8	13	1	3	1	20	27
2	8	2	4	14	20	17	16	25	16
7	10	6	1	20	16	20	11	5	30
4	1	11	11	19	2	15	21	10	24
8	5	14	15	12	19	19	5	29	9
		9	9	17	13	8	15	27	5
		3	14	1	10	2	2	19	19
		15	5	11	6	24	17	28	17
		12	10	15	7	5	24	24	25
		10	13	18	14	11	9	4	22
				8	17	7	22	7	28
				16	11	13	7	13	1
				2	15	1	4	18	18
				10	9	25	10	12	12
				7	8	22	8	22	6
						9	23	21	21
						16	20	15	20
						21	3	3	29
						14	13	9	14
						4	19	14	7
								2	3
								6	11
								16	13
								23	10
								8	2

Fig. 1

You may be wondering why there are two transposition keys for each length of message from 10 to 30 words, in multiples of 5. The two keys constituting a pair are related to each other, that is, they bear a relationship which Mr. Hassard, one of the Tribune cryptanalysts, termed "correlative", but which we now would call an "encipher-decipher" or a "verse-inverse" relationship. Either sequence of a correlative pair of sequences may be used to encipher a message; the other, ~~the inverse of the pair~~ can then be used to decipher the message. For example, key III consists of the following series of numbers: 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 its words consecutively and then assembling the words in the order 8-4-1-7-13, or by (2) writing the sequence 3-7-12-2-6-. . .above the words of the cipher message and then assembling the numbered words according to the sequence 1-2-3-4-5. . . Thus, there were, in reality, not ten 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, or at least some derivative thereof.

I suspect that the basic or "verse" sequences of numbers were not drawn up at random but were derived from words or phrases; and I think that the odd-numbered ones are the "verse", because, as you will notice, it is in the odd-numbered keys that the positions of sequent digits reflect the presence of an underlying key word or phrase; this is not true in the even-numbered keys. I have not seriously attempted to reconstruct the key words but perhaps some of you may like to try and ~~perhaps~~ will succeed in doing so.

In addition to transposition, this system involved the use of "arbitrariness" to represent certain words, the names of important persons and places, numerals, etc. There were also a few nulls.

Professor Holden adds some comments about this system which are worth quoting:

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.

Here, in a nutshell, we find the basic theory of solving transposition ciphers by anagramming messages of the same length, explained in a most succinct manner.

It appears that Professor Holden, clever as he undoubtedly was, did not note the verse-inverse relation in each pair of sequences, or, if he did, he failed to mention it in his testimony. However, Hassard in his article (reference No. 2 above) specifically points this out.

There were enough messages in this system to make it possible to solve <sup>code</sup> words used, as well as to recognize a few nulls which were occasionally added to complicate matters. Hence, <sup>the</sup> most complicated of the cryptosystems involved in this bizarre political episode, were solved.

Another system used by the conspirators employed a bilateral substitution, that is, one in which a pair of cipher letters represents a single letter. This substitution was based upon a 10 x 10 checkerboard. Apparently neither Professor Holden nor the Tribune cryptanalysts recognized the latter principle, nor did they find that the coordinates of the checkerboard employed a key phrase, nor did they realize that the same checkerboard, with numerical coordinates, was used for a numerical substitution alphabet in which pairs of digits represent letters of the alphabet

Here are two of the messages exchanged by the conspirators, one in the letter cipher, the other in the figure cipher. The messages are long enough for solution. Try to solve them, reconstruct the matrix and find the key phrase from which the coordinates of the matrix were derived. It should amuse you by its appropriateness.

The message in letter cipher is as follows:

Jacksonville, Nov. 16 (1876)

Geo. R. Raney, Tallahassee:

PP YY EM NS HY YY PI MA SH NS YY SS IT EP AA EN SH NS SE US SH NS MM PI YY SW  
 PP YE AA PI EI SS YE SH AI NS SS PE EI YY SH NY NS SS YE PI AA NY IT NS SH YY  
 SP YY PI NS YY SS IT EM EI PI MM EI SS EI YY EI SS IT EI EP YY PE EI AA SS IM  
 AA YE SP NS YY IA NS SS EI SS MM PP NS PI NS SN PI NS IM IM YY IT EM YY SS PE  
 YY MN NS YY SS IT SP YY PE EP PP MA AA YY PI IT L'Engle goes up tomorrow.

(Signed) Daniel

The example in figure cipher is as follows:

Jacksonville, Nov. 17 (1876)

S. Pasco and E. M. L'Engle:

84 55 84 25 93 34 82 31  
 31 75 93 82 77 33 55 52  
 93 20 90 66 77 65 33 84  
 63 31 31 93 20 82 33 66  
 52 48 44 55 42 82 48 89  
 42 93 31 82 66 75 31 93

(Signed) Daniel

There were several other systems involved in this episode of political skulduggery but I am going to have to pass them 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 characterized by Professor Holden as the "most difficult and ingenious" of the ciphers he solved, and the USMTC route ciphers described in the preceding lecture. Yet, not only he but also the Tribune amateur cryptanalysts solved those ciphers without too much difficulty, even though they were technically more complex. I think their work on the Tilden ciphers clearly confirms my own appraisal of the weakness and of the route ciphers used by the USMTC in the Civil War.

After this digression into the realm of what may be called political cryptology, let us now go on with our <sup>military</sup> cryptologic history. I have already told you that the Department of State used a code for cryptographic communications in the years following the Civil War, but I do not know what it was like. It may even have been an adaptation of some commercial code. But in an article entitled "secret writing", which appeared in Century Magazine, Vol LXXXV, November 1912, No. 1, a man named John H. Haswell, apparently at that time a code clerk in the Department, referred to a new code of the department in the following terms:

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 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 as the author of a famous or infamous book (depending upon whose side you're on) entitled The American Black Chamber, published in Indianapolis 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 passed in 1934 makes it a criminal offense to do so. That is quite a story in itself but I cannot tell it now. If you happen to own a copy of the first and only American edition, 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; but you may be able to purchase a British edition, or a translation in French, in Japanese, or in other languages, for the book was sensational. But to return to that State Department cryptosystem, which was considered by Haswell as giving absolute secrecy and which was readily solved by Yardley, here is what appears on the cover page of Yardley's 21-page typewritten analysis and solution of the system:

**"THEORY AND PRACTICE OF ENCIPHERED CODE**

**State Department Problems**

**I, II, and III**

NOTE: The following was written in March 1916 and, so far as I can learn, is the first successful attempt to solve a problem in enciphered code.

(Signed) H. O. Yardley'

Yardley was quite wrong in thinking that his was the first successful attempt to solve a problem in enciphered code, for in Europe more complicated cases were often solved and I imagine that <sup>European</sup> British cryptanalysts could have read, ~~and~~ ~~possibly did read~~, State Department messages as a more or less routine matter. I think I am warranted in assuming that what I have just said is true because, in Europe, cryptanalytic studies were going on apace during the years of American neglect of such studies. The turning point from neglect to a renaissance of interest in cryptologic studies in Europe is said by some authorities to have been about the year 1880; but we must confine ourselves for the most part to developments in America, ~~not in Europe~~, in order to keep this lecture within bounds of what can be told within a period of an hour or so.

In our Navy it seems that simple monoalphabetic ciphers 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 designed for naval communications. The system they worked out was embodied in a very large codebook, 18" long, 12" wide and 2" thick, which had the official title The U. S. Navy Secret Code. There was also an accompanying but separate cipher book, almost as large, and designated as The Book of Key Words. In addition to these ~~two~~ ~~books~~ was a third large book called "General Geographical Tables". The system was placed into effect on 1 December 1887. Later I will show you a most historic message sent in that system of secret communication, which today impresses one as being extraordinarily clumsy and slow.

In our Army, in the middle eighties, a code was also prepared. It is no pleasure to have to tell you that its composition and format hardly shed laurels upon those responsible for its reproduction, because it was merely <sup>a</sup> simple and acknowledged adaptation of a commercially available small code for use by the general public, first published in 1870 with the title Telegraphic Code to Ensure Secrecy in the Transmission of Telegrams. It had been compiled by the Secretary of the French Trans-Atlantic Telegraph Company, a man named Robert Slater, and it became known everywhere as "Slater's Code". As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using this work," in a sort of preface to the 2nd Edition:

It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No. (from 00001 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 number 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 number in the Code, of the "Dummy Word" to find the word meant. (Punctuation as in the original)

Here we have a sentence of 116 words. Though it is rather long and a bit murky I think you will gather its import. The system as thus far described is what we now call <sup>the</sup> additive or subtractive method. But in the detailed instructions Slater goes one step further and suggests that instead of telegraphing the code number resulting from addition or subtraction of a key number, the word standing alongside the sum (or difference) of the mathematical operation be sent as the telegraphic code word.

Slater's 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. As for a copy of the very first edition, 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 an adaptation of Slater's Code for its use and the use of the Army. Here is a picture of its title page, the only difference between it and that of Slater's Code being in the spelling of the word "secrecy", as you can easily see in the picture I show you next. It would appear that the "compiler" of this code, Col. Gregory, was just a bit deficient in imagination, because not only did he merely borrow the basic idea and format of Slater's Code, but even when it came to explaining and giving examples of enciphering the code groups, the Colonel used not only the identical rules but also the very same wording and even the very same type of examples of transformations that are found in Slater's original. Let me show an example in Slater's code side by side with the same example from Gregory's:

You will note that Col. Gregory just couldn't use the same text for his examples of encipherment that Slater used, which was: "The Queen is the supreme power in the Realm." Instead he used the enigmatic text: "War is a punishment whereof death is the maximum."\*

All the other methods and examples of encipherment in the two codes are practically identical. Colonel Gregory gives credit in the following terms to a civilian <sup>admiral</sup> in his great work: "The labor of compiling the new vocabulary has been performed by Mr. W. G. Spottswood." What did the latter do? Well, Mr. Spottswood's work consisted in casting out from Slater's list such words as ABALIENATE and ABANDONEE 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 and satirical about the performance 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 Colonel Gregory and Mr. Spottswood.

Col. Gregory prepared a confidential letter addressed to Lieut. General Sheridan, "Commanding Army of the U.S.", to explain the advantages of the new code. But in this letter Col. Gregory quotes very largely from Holden's little brochure and deals almost solely with the ways in which additional security may be gained by changing the additives to the code numbers in Slater's Code. For example, for all messages sent in January add 111; for all messages sent in February add 222, in March 333, etc. Another suggested way: Send out a simple message in ordinary English: "Add 1437 to all ciphers until further orders."

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 a simple additive, because in a copy in my collection the additive is written on the inside of the front cover. It <sup>is</sup> ~~was~~ 777; perhaps it was the additive for the month of July, but the number 777 was written in ink, so it may have been the permanent additive for the whole of the war. In pages 41-42 of The American Black Chamber the author throws an interesting sidelight on this code system:

\*I wonder what that sentence means. It sounds sort of "anti-American" to me. Punishment to whom? To the soldiers and sailors and airmen who defend our country? If not to them, then to whom? To the people of a whole nation fighting for liberty? I just don't understand the sentence. Do you?

The compilation of codes and ciphers was, by General Orders, 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 high 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 communications. 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.

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 satiric comments in this regard, it grieves me to say, are unfortunately fully warranted.

During or perhaps shortly after the end of the Spanish-American War, the War Department must have begun to realize that there were shortcomings in the code based upon Slater's Code, the one which was in current usage and upon which I have already dwelt. On 16 January 1898 the publication of a new War Department Telegraphic Code was authorized by General Orders No. 9. The code was to be prepared under the direction of General A. W. Greely, then Chief Signal Officer of the Army. The cited General Order makes it quite clear that the War Department version of Slater's Code was still in use, but the Western Union Telegraphic Code was to be used in connection with Slater's until the new War Department Code was completed, which apparently was ready in December 1899, when Slater's was withdrawn from use with this statement in General Orders No. 203: "By direction of the Secretary of War, the Telegraphic Code to Insure Secrecy in the Transmission of Telegrams, will on and after January 15, 1900, only be used for correspondence in such cases as may be specially ordered by the Secretary of War." On 12 December 1899 the new War Department Code was issued. It comprised a specially-compiled list of tables, words, phrases and sentences to which code numbers and code words were assigned for specific use in War Department and Army communications. The code numbers began with 78201 and went to 95286; the accompanying code words were foreign, outlandishly unusual real words, and artificial words, beginning with KOPERKIES,

KOPERKLEURS, KOPERMOLLEN, etc, etc., down through the L's, M's, and ending with words such as NAZWELGEN, NEANPHE, NEAPELGELB, etc, etc. You may wish to know why the code numbers didn't begin with 00000 and go to 99999; or why the code groups began with K and went for thousands and thousands of words down to N. The answer is that this brand new War Department Telegraphic Code was to be used, as Slater's Code was used, in conjunction with the Western Union Telegraphic Code, a code of 78,200 groups beginning with numerical code groups 00000 accompanied by literal code words beginning with BEERKAR, BEERKARNEN, BEERMELDE . . . and going to KOOTJONGEN, KOOTKRUID, KOOTSPEL.

The introduction to this code explains this puzzling fact. "Through lack of time it has been impossible to incorporate in the WAR DEPARTMENT TELEGRAPHIC CODE all desirable phrases, and in consequence the first 471 pages of the Western Union Telegraphic Code now in use by the Army will continue in use as a supplementary code. This affords the Army the telegraphic use of 100,000 code words, of which numbers 1 to 78,201, inclusive, are in the Western Union Telegraphic Code and numbers 78201 to 100,000 are in the War Department Telegraphic Code".

It thus becomes clear that for several years the new War Department Code was to be used in conjunction with the commercially available public Western Union Telegraphic Code. This was stated to be for the purpose of economy. For secrecy the additive or subtractive method was to be used. The futility of such an old and simple method for achieving communication security needs no comment. I wish there were time to read you the instructions in that new War Department <sup>telegraphic</sup> Code as regards the use of these ciphers for secrecy. They are practically the same as those in the 1885 version of Slater's Code and are unbelievably futile, but what else could be expected when cryptology is relegated to a position of military science far inferior to that of teaching the use of a rifle or bayonet, subjects which are taught, as a rule, by experts? Why was cryptology left to inexperienced amateurs during all those years about which I am talking you? Was it stupidity? No, just a lack of appreciation of the importance of secure communications in military operations.

How long this combination of two codes continued to be used I don't know. Some time during the years 1900 to 1915 this absurd system must have proved itself entirely unsatisfactory, for in 1915 another brand new War Department Telegraph Code was put out, under direction of Brigadier General George P. Scriven, the Chief Signal Officer of the Army who succeeded Greeley. The book bears no security classification, for even as late as in 1915 there was no classification system for security purposes. The instructions recommended certain precautions. "The

War Department Telegraph Code," says paragraph 5 of the instructions, "while not absolutely confidential, will be guarded with the greatest care and will never be out of the immediate possession or control of the officer to whom issued or of his confidential agent. Care will be taken to prevent theft, loss, use, or inspection except by those whose duties require them to employ the code. Special pains will be taken to prevent the code from falling into the hands of unauthorized persons or of the enemy."

This new code, as the case of its predecessor was, "intended to serve two purposes: First, secrecy, and second, economy." "When secrecy is desired it is to be used as a cipher code, as is explained in subsequent paragraphs under 'Enciphered Code'." But there are no subsequent paragraphs in which this is explained. Apparently some change in this regard was decided, because I have seen, as a separate pamphlet, a set of cipher tables for use with this code.

The code itself embodied some of the latest ideas of code compilation. It had over 113,000 code groups, and these were both figure groups and, for the first time, 5-letter groups. The latter embodied the principle of the 2-letter difference, but the instructions do not mention this fact and no permutation table was included in the code itself. The book has a very extensive vocabulary of words, phrases, and sentences. I feel sure that a great deal of thought and effort went into the production of this code but I must tell you two things about it. First, I must tell you that my immediate predecessor in the O C Sig O told me on my return from France in 1919 that that particular <sup>edition</sup> ~~edition~~ of the War Department Telegraph Code had been printed in Cleveland by a commercial printer, and second, that when the United States became a belligerent in World War I our British Allies found it desirable to notify <sup>our government</sup> ~~us~~ that our War Department Telegraph Code was not safe to use, even with its superencipherment tables. The implications of this notification are rather obvious and hardly require comment. The compilation of a new code in 1917 was initiated but this time the work was done within and under the direction of the Military Intelligence Division of the General Staff, and in particular within the section devoted to cryptanalysis. This undertaking, which indubitably was a direct affront to the Signal Corps of the Army, met with no objection, it seems, from that Corps; perhaps it deserved the intended insult because of its long-standing neglect of its clear responsibilities for cryptography and cryptographic operations in and for the Army.

We have noted how inadequately the Army and the War Department were equipped for cryptocommunications in the years from 1885 to 1915. 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 vocabulary and tabular contents of the codebook and its accompanying two large books, one for enciphering the code groups, the other for geographical names. For the 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. He forthrightly and frankly favored a strong foreign policy, backed by adequate military and naval strength - "speak softly but carry a big stick", <sup>was his motto</sup> He was looking forward, in fact, to <sup>C</sup>for~~cing~~ 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, Navy Secretary John D. Long, he took it upon himself to initiate the preparations which he had in vain tried to persuade 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 into activity. On a Saturday afternoon, ten days after the U.S. Battleship 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, at Hong Kong. Here it is, with his bold signature at the bottom:

That is the now historic message which alerted Dewey and which resulted in our taking over, under U. S. protection in the war which was declared ten days later on Spain, the Philippine Islands. ~~I don't think we really wanted them.~~

You will note that the message bears on its face a security classification, but the classification, "Secret and Confidential", was crossed out. That must have been many 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 with its strange and outlandish code words, as it was received in Hong Kong:

And now I show you the deciphered and decoded text, which I was fortunate in being able to produce by courtesy of the Chief of the Navy Security Group, who permitted me to consult and use the necessary code books which I found were still in Navy Security archives. To translate a message in the code then in use three steps are necessary. First, the cable words (the peculiar, outlandish words in line 2 - WASSERREIF, PAUSATURA, BADANADOS, ~~XXXXXXXXXX~~, etc.) are sought in the cipher book, and their accompanying cable-word numbers set down. WASSERREIF yields 99055; PAUSATURA yields 62399, BADANADOS, 11005; ~~XXXXXXXXXX~~, ~~XXXXXX~~, etc. 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, 990556, is then sought in the basic code book and its meaning is found to be "Secret and Confidential." The transfer of the first digit, 6, of the second cable-word number, 62399, makes it become code-number 2399, to which must now be appended the first two digits of the third cable-word number, 11005, thus making the second code group of the code message 239<sup>9</sup>11, which

is sought in the basic code book and yields the meaning "Order the squadron." And so on. It's painfully slow work, and I haven't told you about some of the difficulties I encountered in the process, including having to refer to the third book, the General Geographical Tables. It took an hour to translate this one relatively short Roosevelt message. I feel sure a naval <sup>operation</sup> ~~strategic plan~~ in World War II or in World War I, for that matter, could never have been executed before a message of the length of the Roosevelt one could be deciphered and decoded by this cumbersome system, even if all the digits had been transmitted and received correctly. Generally speaking, naval battles are fierce and quickly over. For instance in two minutes, on 4 June 1942, from 10:24 to 10:26, the war with Japan was decided when the U.S. Pacific Fleet under Admirals Nimitz, Fletcher and Spruance won the Battle of Midway, in which the Japanese lost four fast carriers, together with their entire complement of planes, and almost all their first-string aviators. When our Navy entered World War I a much more practical system was put into effect, using a cipher device known as the NCB, standing for "Navy Cipher Box", to encipher 5-letter groups of a basic code.

Later, I'll show you a picture of this box, probably the very prototype of what we now often call a "black box."

We come now to European events of importance in this cryptologic history. During the decades from the end of the Civil War in America to the first decade of the 20th Century there was some progress in cryptologic science in Europe but it was not of a starting nature. German Army Major Kasiski's demonstration of a straightforward, mathematical method of solving the Vigenère cipher was published in Berlin during the mid-period of the Civil War in America. If the book created an 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,\* the name Kasiski doesn't even appear in it. Other books on cryptologic subjects appeared in Europe during this period, and two of them deserve special attention. 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 now show you. But our own Thomas Jefferson anticipated Bazeries by a century, and here are two slides describing Jefferson's "Wheel Cipher", copies from the original manuscript among the Jefferson Papers in the

\*Capt. Parker Hitt's Manual for the solution of military ciphers, Fort Leavenworth, Kansas: Army Service Schools Press, 1916.



Library of Congress. The second book which deserves special attention is one by another French cryptologist, the Marquis de Viaris, in which he presents methods for solving cryptograms prepared by the Bazeries cipher cylinder, and, although unknown to him, the ciphers of 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 so-called "Black Chambers", organized for solving one another's secret communications. 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 passing in transit through them. This was true in the case of every country in Europe with one very important exception: Great Britain. The story, which is given in detail in a recently published and very fully documented book,\* is highly interesting but I must condense it to a few sentences.


In England, from about the year 1540 onward until 1844, there was a "black chamber" ~~was~~ in constant operation. It was composed of three collaborating organizations within the Post Office respectively called "The Secret Office", the Private Office", and "The Deciphering Branch".

In the first of these highly secret organizations, letters were opened, copies of them were made, the letters replaced, the envelopes resealed, and if the wax seals were intact they were merely replaced. If the seals were not replaceable, duplicates were forged and affixed to the envelopes. Copies of letters in cipher were sent to the "Deciphering Branch" for solution and the results, if successful, were then sent to the Foreign Office. A famous mathematician, John Wallis, took part in the letter activities. The "Private Office" took care of similar activities but only

\*Ellis, Kenneth L. The Post Office in The Eighteenth Century: A Study in Administrative History. London: Oxford University Press, 1958, pp. 176. In conjunction with this book one should by all means also read the following extremely interesting and revelatory article by the same author: "British communications and diplomacy in the eighteenth century", Bulletin of the Institute of Historical Research, Vol. XXXI, No. 84, Nov 1958, pp. 159-167.

in connection with internal or domestic communication's. In 1844, a scandal involving these secret offices caused Parliament to close them down completely, 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 England's black chamber had to start from scratch. But within a few months British brains and ingenuity built a cryptologic organization known as "Room 40 O.B.", which contributed very greatly to the Allied victory in 1918. Although the British Government has never issued a single official publication on the activities and accomplishments of "Room 40 O.B.", several books by private authors have pushed aside the curtain of secrecy to make a most fascinating story too long to tell in this lecture. But I must tell you at least something about what was perhaps the single greatest achievement of "Room 40 O.B.", an achievement which just in the nick of time brought this country into World War I as an active belligerent on the Allied side and saved England from complete destruction, as well as France. The operation involved the interception and solution of a message known as the Zimmermann Telegram, deservedly called the most important single cryptogram in all history. On 8 September 1958 I gave before an NSA audience a detailed account of this amazing cryptogram. I told about its interception and solution; I told how the solution was handed over to the United States; how it brought America into the war on the British side; and how all this was done without disclosing to the Germans that the plain text of the Zimmermann Telegram had been obtained by interception and solution by cryptanalysis, that is, by science and not by treason. My talk was given under the auspices of the NSA Crypto-Mathematics Institute, was recorded, and is on file so that, if you wish, you can hear it. It took two and a half hours to deliver and at that I didn't quite succeed in telling the whole story. But you may read an excellent account of this episode, set forth in great detail in a book entitled The Zimmermann Telegram, by Barbara Tuchman, published in 1958 by the Viking Press, New York. Also, you should consult a book entitled The Eyes of the Navy, by Admiral Sir William James, published in 1955, by Methuen & Co., London. 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 "Room 40 O.B.", that is, the British Black Chamber. To summarize, as I must, this fascinating and true tale of a very important cryptanalytic conquest, let me show you again the telegram as it passed from Washington to Mexico City, for if you will remember I showed it to you in the very first lecture of this series, as Fig. 1



thereof, and promised to tell you about it later. Here I show it to you once again, and as you can easily see, the code groups are composed of three, four, and five-digit groups, mostly the latter. Here is the English decoded translation of the message as transmitted by our Ambassador Page in London to President Wilson.

From the day that Ambassador Page sent his cablegram to President Wilson on 28 February 1917, quoting the English translation of the Zimmermann Telegram 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 became a certainty. Under big black headlines the English text appeared in our newspapers, because after assuring himself of the authenticity of the telegram handed over by the British, and that it had been decoded and checked by a member of Ambassador Page's own staff, President Wilson directed that the text of the message be released to the Associated Press. Its publication the next day was the first of a momentous and sensational series of reports and accounts of the Zimmermann Telegram and its contents.

But there were plenty of members of Congress who disbelieved the story. Here are a few of their comments. "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. Thus, it came about that Americans in the Middle West and Far West, who had thus far been quite unconcerned about a War that was going on in Europe, thousands of miles away and wanted no part of it, suddenly awoke when they learned that a foreign power was making a deal to turn over some rather large slices of U. S. real estate to a then hostile neighbor across the southern border. They were aroused to the point where they, too, as well as millions of other Americans in the East, were ready to fight. Surely war would now be declared on Germany.

Notwithstanding all the furor that the disclosure of the Zimmermann Telegram created in America, President Wilson still hesitated. He was still determined that America would not, must not, fight. It was not until more than a month later, and after several American ships were sunk without warning on 18 March, that a now fully aroused President got Congress to declare war on Germany and her allies. 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. It is difficult to believe, but I assure you that it was true, that there was at the moment in neither of those departments, nor in the Army or Navy, any organizations or technical groups whatever, either for intercepting enemy communications or for studying them, let alone solving such communications. There was, it is true since the autumn of 1916, a very small group of self-trained cryptanalysts, sponsored and supported by a private citizen named Colonel George Fabyan,\* who operated the Riverbank Laboratories at Geneva, Illinois. I served as leader of the group, in addition to other duties as a geneticist of the Laboratories. Riverbank, through Colonel Fabyan, had initiated and established an unofficial or, at most, a quasi-official relationship with the authorities in Washington, so that it received from time to time copies of cryptographic messages obtained by various and entirely surreptitious means from telegraph and cable offices in Washington and elsewhere in the U. S. At that period in our history diplomatic relations with Mexico were in a sad state, so that U. S. attention was directed southward, and not eastward across the Atlantic Ocean. Therefore, practically all the messages sent to Riverbank for solution were those of the Mexican Government. Riverbank was successful in solving all or nearly all the Mexican cryptograms it was given, usually returning the solutions to Washington very promptly. The great majority of them were of the Vigenère type but using mixed sequences with relatively long key phrases. Riverbank was also successful with certain other cryptograms with a background of the war in Europe but I cannot deal with them now because there just isn't time. Soon after the U. S. declared war on Germany Col. Fabyan at Riverbank established a school for training and he invited the Services to send him

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

Army and Navy officers to learn something about cryptology, in formal courses established for the purpose. Each course lasted about six weeks, full time.

You may like to know what we novices used for training ourselves for this unusual task, and what we used later on for training the student officers sent to us for cryptologic instruction. As regards our self-instruction training material, there wasn't much available in English but among the very sparse literature there was a small book entitled Manual for the Solution of Military Ciphers, which had been prepared by <sup>a</sup>U. S. Army Captain of Infantry named Parker Hitt and which had been printed by the Press of the Army Service Schools at Fort Leavenworth, in 1916. Colonel Fabyan managed to get a copy of that Manual for use to study. The Signal Corps School was then one of the Army Service Schools 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 cryptography. They foresaw that sooner or later there would be a need for knowledge in that important branch of military technology. Capt. Hitt's Manual, was then, and still is, a model of compactness and practicality. Let me show you the title page of the first edition. Here it is.

It was the succinctness of Parker Hitt's Manual that caused us much work and perspiration in our self-training at Riverbank, and we later came to know and admire its author, whose photograph I now show you as he looked when he became a Colonel in the Signal Corps.

There was one other item of training literature which we also studied avidly. It was a very small pamphlet entitled An Advanced Problem in Cryptography and its Solution, and it too was put out by the same Leavenworth Press in 1914. Here is its title page. You will note that its author was then 1st Lieut. J. O. Mauborgne; he advanced to become a Major General and Chief Signal Officer of the Army. The "advanced problem" dealt with in that pamphlet was the Playfair Cipher, about which I shall say only that at the time Mauborgne wrote about that particular cipher it was considered much more difficult than it now is regarded.

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

In Lecture II I showed you 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 and it gives me considerable pleasure to tell you that this instruction was conducted at Colonel Fabyan's own expense as his patriotic contribution to the U. S. war effort. I can't in this lecture say much more about this than that it involved the expenditure of many thousands of dollars, never repaid by the government--not even by some decoration or similar sort of recognition. Upon completion of the last training course I was commissioned a first lieutenant in Military Intelligence, General Staff, and ordered immediately to proceed to American General Headquarters in France, where I became a member of a group officially referred to as the Radio Intelligence Section. But it was the German Code and Cipher Solving Section of the General Staff, a designation that was abbreviated as G-2, A-6, GHQ-AEF. As the expanded designation implies, the operations were conducted in two principal sections, one devoted to working on German Army field ciphers, the other, to working on German Army field codes. There were also very small groups working on other material such as meteorologic messages, direction-finding bearings, and what we now call traffic analysis, that is, the study of what we call "the externals" of enemy messages in order to determine enemy order of battle and other vital intelligence from the study of D.F. bearings, the direction, ebb and flow of enemy traffic, and other data sent back from our intercept and radio direction-finding operations at or near the front line of the combat zone.

In connection with the last-mentioned operations you will no doubt be interested to see what is probably one of the earliest, if not the very first chart in cryptologic history, that shows the intelligence that could be derived from a consideration of the results of traffic analysis. Its utility in deriving intelligence about enemy intentions from a mere study of the ebb and flow of enemy traffic, without being able to solve the traffic, was of unquestionable value. Here's that historic chart, which I must tell you was drawn up from data based solely upon the ebb and flow of traffic in what we

called the ADFGVX cipher\*, a clever cryptosystem which was devised by German cryptographers and which was restricted in its usage to German High Command communications, principally those between and among the headquarters of divisions and army corps. Its restriction to such high command messages made a study of its ebb and flow very important. Theoretically, that cipher was extremely secure. 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 will give a clear understanding of its method of usage. (Explain slide.) If you wish further details I suggest you consult documents available in the Training Literature Division of the NSA Office of Training. In this lecture there is only time to tell you that although individual or isolated messages in the ADFGVX system appeared at first to be absolutely impregnable against solution, a great many messages transmitted in it were read by the Allies. You may be astonished by the foregoing statement and therefore may desire some enlightenment here and now on this point. In brief, there were in those days three and only three different methods of attacking that cipher. Under the first method it was necessary to find, as the first step, two or more messages with identical plain-text beginnings because they could be used to uncover the transposition, which was the second step. Once this had been done, the cryptanalyst had then to deal with a substitution cipher 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, which amounted to solving a monoalphabetic substitution. Under the second method, two or more messages with identical plain-text endings could be used to uncover the transposition. This was easier even than 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 military communications is so prevalent in all military communications, and especially in German messages, that cases were almost invariably found, in each day's traffic, of messages with similar beginnings or endings, and sometimes

\*Initially this cipher employed only the letters A, D, F, G, and X, for a matrix  $5 \times 5$ ; later, the letter V was added, for a matrix of  $6 \times 6$ , for the 26 letters of the alphabet plus the ten digits.



both. This system first came into use on 1 March 1918, three weeks before the last and greatest offensive by the German Army. Its appearance was 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 first done by a very able cryptanalyst named Capt. Painvin of the French Army's Cipher Bureau.

The ADFGVX cipher was used quite extensively on the Western Front with daily changing keys during May and June of 1918 but then, for reasons somewhat obscure, the number of messages dropped very considerably. How many different keys were solved by the Allies during the four months from 1 March to the end of June? Not many--10 in all; that is, the keys for only 10 different days were solved. Yet, because the traffic on those days was very heavy, about 50% of all messages ever sent in that cipher, from its inception to its discard, were read, and a great deal of valuable intelligence was derived from them. On one occasion solution was so rapid that an important German operation disclosed by one message was completely frustrated.

Although the ADFGVX cipher came into use first on the Western Front, it later began to be employed also 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, solution depended upon the three rather special cases I mentioned. No general solution for it was thought up by the Allies despite a great deal of study. However, members of our 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, in the course of writing up and describing their method, I happened to find a similar one in a book by French General Givierge (Cours de Cryptographie, published in 1925). Givierge was by then the head of the French Black Chamber, which was <sup>called the</sup> ~~em-tje~~ "Deuzieme Bureau", corresponding to our "G-2".

The ADFGVX cipher was not the only one used by the German Army in World War I, and there will be time to mention very briefly only two others. The first of these was a polyalphabetic substitution cipher called the "Wilhelm," which used a cipher square with disarranged alphabets and with a set of 30 fairly lengthy keywords. Here is the cipher square. Just why the square contains only 22 rows instead of 26 is probably connected with the fact that German can get along very well with fewer than 26 letters. Certainly the rows within the square are not random sequences, as you can see, for the letters within them manifest permuted arrangements in sets of five letters. And here is a slide showing the keys used--31 of them. The key sequences are not composed of random letters. I leave it to you to try to reconstruct the <sup>or</sup> real square, if possible; you should be able to reconstruct the real keys. The latter problem should be relatively easy.

The other German Army cipher to be mentioned is the double transposition, an example of which is shown in this next slide. The process consists in applying the same transposition key twice to the same matrix, once horizontally and once vertically, as seen in this slide. Solution of the true double transposition usually depends upon finding two or more messages of identical length. (You will remember what I told you about Capt. Holden in this connection.) No general solution was known to the Allies during World War I, and messages of identical length were few indeed. But it happened that occasionally a German operator would apply only the first transposition and when this fortunate situation occurred solution was easy, because the key thus recovered from the single transposition could be used to decipher other messages which had been correctly enciphered by the double transposition. Again, the Signal Intelligence Service devised a general

solution for the double transposition cipher and during World War II were able to prove that such ciphers could be solved without having to find two messages of identical length. I think the devising of a general solution for the true double transposition cipher represents a real landmark of progress in cryptanalysis.

We come to the code systems used by the belligerents in World War I. And first, let us differentiate those used for diplomatic communications from those used for military communications. What sorts did the German Foreign Office use? We have noted that the British Black Chamber, "Room 40 O.B." enjoyed astonishing success with the code used for the transmission of the <sup>2</sup>Zimmermann Telegram. Excessive pride in German achievements in science, a wholly unjustified confidence in their communications cryptosecurity, and a disdain for the <sup>1</sup>impotence 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 telling its representatives abroad by telegraph, cable or radio remained secret from their cryptologic protagonists. For those of you who would like to learn some details, I refer you to the following monograph 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. Copies of it available in the Office of Training, NSA. Says Dr. Mendelsohn:

"At the time of America's entrance into the war German Codes were an unexplored field in the United States. 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 of encipherment 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 historical interest, which were now read with the aid of code book."

The vocabulary of the German diplomatic codes comprised 189 pages each having 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 were the five blocks from 00-09, 10-19, etc., to 40-49; then 50-59, 60-69, etc., were in blocks of 10 in the right-hand column. The pages in the basic code were numbered and from this code several codes were made by the use of conversion tables. This enabled the original signal basic code to serve as the framework for apparently unrelated and externally distinguishable codes for several different communication nets. What the number of the basic code was is unknown, but we do know that from the code designated as Code 13040 came codes 5950, 26040, and others, derived merely by means of tables for converting the page numbers in the basic code into

different page numbers in the derived code. These conversions were systematic, in blocks of fours. Thus, for example, pages 15-18 in code 13040 became pages 65-68 in code 5950, etc. Then there were tables for converting line numbers from one code into different 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. The other five blocks (on the 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 by re-numbering pages and shifting about the contents of pages in blocks can by no means be considered as being different, and entirely unrelated codes, and once a relationship between two externally different but internally related codes was discovered the two could be handled as equivalents of one another. Also to be mentioned is the fact that in certain cases numbers were added to or subtracted from the code numbers of a message and this gave rise to what seemed to be still difficult to determine the additive or subtractive and thus get to the basic code numbers.

In none of the cases or codes mentioned thus far was there one that could be considered to be a randomized, "hatted," or 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 real 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 not doubt.

When one reviews Dr. Mendelsohn's monograph one becomes overwhelmed by the multiplicity of the codes and variants thereof used by the German Foreign Office. Some were basic codes but many were derivatives, or superencipherments thereof. It is even hard to ascertain the exact number of different codes and superencipherment 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 in the British counterpart organization in London, in the British Black Chamber, one can only be astonished by the great achievements of the efforts of these two collaborating organizations that worked on German diplomatic codes during World War I.

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 the knowledge gained about these items became of great importance in cryptanalysis when German cryptosystems improved. The German Army learned by hard experience something about its shortcomings in this area of warfare and not only soon began to improve but it did so to the point where we must credit the Germans with being the initiators of new and important developments in field military cryptography. In fact, the developments and improvements began not long after 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 inventions, 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 radio traffic during that war have appeared; one Austrian cryptanalyst, a man named Figl, attempted to publish a book on cryptanalysis but it seems to have been suppressed. 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 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 Gylden, under the title Chifferbyraernas Insatser I Varldskriget 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.

In this lecture, however, we are principally concerned with German military cryptography during World War I, and I have already told you something about the cypher systems that were used. There remains 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 types of field codes: one which they called the SCHLUESSELHEFT but which we called the "three-number code", the other which they called the SATZBUCH but which we called the "three-letter code". The former was a small standardized code with a vocabulary of exactly 1,000 frequently used words and expressions, digits, letters and syllables, etc., for which the code equivalents were 3-digit numbers. A cipher was applied only to the first two digits of the code numbers and this cipher consisted of 2-digit groups taken from a  $10 \times 10$  matrix for enciphering the numbers from 00 to 99. This table was called the GEHEIMKLAPPE or "Secret Key", and here's a picture of one. The last digit of a code group remained unenciphered. Thus, code group 479 would become 629. Each division compiled and issued its own secret key table, which was in two parts, or sections, of course, 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 completed by the end of January 1918, it was not distributed or put into use until the opening day of the last and greatest German offensive, 10 March 1918. Our code solving section, through good fortune and careful attention, ascertained the nature of the new code and a few groups in it were solved the very same day the code was put into effect because a German cipher operator who was unable to translate a message in the new code requested and received repetition in another code which had been solved to an extent which made it possible to identify homologous

code groups in both messages. The three-number code proved rather easy to solve on a daily basis because only the encipher-decipher table was changed. Much useful intelligence was obtained from the daily solution of this key.

The solution of the SATZBUCH or three-letter code, however, proved to be a much more difficult problem. In the first place, it had a much larger vocabulary, with nulls and many variants for frequently-used words, letters, syllables and numbers; in the second place, and what constituted 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 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 within a quiet sector of the front and trying to solve a few messages in this code was really a painfully slow, very difficult and generally discouraging experience. On my reporting for duty to Colonel Frank Moerman, who was Chief of the whole unit and whose photograph I show you here, I was asked whether I wished to be assigned to the cipher 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 asked to be assigned to the code solving unit, in order to broaden my professional knowledge and practice in cryptology. Little did I realize what a painful and frustrating period of learning and training I had undertaken, but my choice 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, written in 1918-19, 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 the last two paragraphs from my "estimate of the three-letter code" (on page 65 of that monograph) and will remind you that although they were written over 40 years ago they are still applicable:

"In the light of this limited experience (of less than six months with the 3-letter code) it is impossible to say absolutely what the degree of security offered by such a highly developed system really is. There is no doubt but that it is very great. There is no doubt but that, with the proper precautions, careful supervision and control the employment of such a code by trained men offers the highest possible security for secret communication on the field of battle.

But no code, no matter how carefully constructed, will be safe without a trained, intelligent personnel. A poorly constructed code may be in reality more safe when used by an expert than a very well constructed one when used by a careless operator, or one ignorant of the dangers of improperly encoded messages. This point cannot be overemphasized. It is hardly necessary to point out, therefore, that the proper training of the personnel which is to be put in charge of the work of coding messages is an essential requisite to the maintenance of secrecy of operations, and thus of success on the field of battle."

So much for the German Army field codes, about which a great deal more could be said but we must hurry on to the cryptosystems of some of the other armies in World War I.

What sorts of cryptosystems did the French Army use? First, as for ciphers, they put much trust in transposition methods and here is an example of one type. Perhaps you remember one of those special route ciphers I showed you in the preceding lecture, the one with the diagonal that produced complexities that made the use of that route too difficult for the cipher operators of the USMC. This French transposition cipher was much more complicated by those diagonals and I wonder how much use was made of this cipher by the French.

As for codes, like the Germans they used a small, front-line booklet called a "Carnet Reduit", or an "Abbreviated Codebook". Various sectors of the front had different editions and I show you now 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, 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 and here is the example of superencipherment 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 enciphering 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 field cryptosystem is that, theoretically at least, it certainly was the most secure of all the field systems used by the belligerents.

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 messages in the combat zone. But today, of course, its security is known to be so low that it hardly merits confidence for serious usage. The British also used a field code. It 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 superencipherment, the nature of which was not disclosed even to their Allies, so I am not in a position to describe it. We did not even have a copy of their code--only a typewritten transcript which was furnished us quite reluctantly. This next slide was made by setting up in print a typical page thereof.

What about the cryptosystems used by the Italian Army in World War I? The general level of cryptologic work in Italy during that period was quite low, a fact which is all the more remarkable when we consider that the birthplace of modern cryptology was in Italy several centuries before. There appears to have been in Italy a 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 the need for secrecy which requires filing away in dusty archives records of cryptanalytic successes; but it is to be considered also that this prevents those who might have a flair for cryptologic work from profiting from the progress of predecessors who have been successful in such work. We should ~~therefore~~ not be too astonished to learn, therefore, that when Italy entered World War I the Italian Army put its trust in a very simple variation of the ancient Vigenere cipher, a system called the "cifrario militare 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 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 (page 23) "still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on his part."

What about Russian cryptology in World War I? As regards cryptographic work, it is known that there was, during the era of the last of the Czaristic rulers, an apparently well organized and effective bureau for constructing and compiling diplomatic codes and ciphers, which had been organized by a Russian named Savinsky, formerly Russian Minister to Stockholm. He saw to it that all codes and cipher in use were improved; he introduced strict regulations for their use; and he kept close watch over the cryptographic 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 with one of our Allies in World War II. He is no longer alive but I vividly recall that he wore with great pride on the index finger of his right hand a ring in which was mounted a large ruby. When I showed interest in this unusual gem he told me the ring had been presented him as a token of recognition and thanks for his cryptanalytic successes while in the service of Czar Nicholas, the last of the line.

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 poorly trained Russian cipher and radio operators to use when it was placed into effect toward the end of 1914. Here is a picture of that cipher, which was composed of two tables, one arranged for convenience in enciphering and the other arranged to convenience in deciphering. In the enciphering table the letters of the Russian alphabet (33 in all) appear in the topmost row of characters, the 2-digit groups, in random order within each of the 8 rows below the top row, are their cipher equivalents. These rows therefore constitute a set of 8 cipher alphabets, these alphabets being preceded by key numbers from 1 to 8 in random order. Both the cipher equivalents and the indicators were subject to change. Indicators were used to tell 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 digit 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 this question may be in order: Why the aversion to the use of zero and to the use of double digits such as 11, 22, 33, etc.? This probably was thought to be helpful to the telegraph operators as well as to the cipher clerks in straightening out errors in transmission and reception.

I have told you that this cipher system proved too difficult for the Russians to use, and I think you can see why. It was so difficult that messages had to be repeated over and over, with great loss of time. It is well known to all historians by this time that the Russians lost the Battle of Tannenberg in the autumn of 1914 largely because of faulty communications. Poor cryptography and failure to use even the most 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 disposition 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 on learning this then repeat the identical message in the old key. 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 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 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 communications 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 this slide and will let you assess its security yourself.

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 as a consequence of advances in electrical communications technology. When measured by today's standards it must be said that not only was the AEF on its arrival in Europe wholly 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 technical advances both sides had made, 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 II. 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, that I've mentioned. When it has 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 charged with impropriety, 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 so-called "Trench Code", of which 1000 copies were printed, together with what were then called "distortion tables". These were simple monoalphabets for enciphering the 2-letter groups of the code. I will show you a picture of a page of this code and of one of the "distortion tables". 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 the code was not distributed, because a study of its security showed defects. The truth is that AEF

cryptographers with personnel inexperienced in cryptanalysis were groping in the dark, with little or no help from allies. Finally, the light broke through: the Code Compilation Service began to see the advantages of that German 3-letter randomized 2-part code I've told you about, the one called the Satzbuch. Here, then, was the origin of the Trench Codes which were finally adopted and used by the AEF, when it was decided that copying and benefitting from the experience of German code compilation was no dishonor. The AEF then went them one better, as you shall now learn. The first code of the new series of the AEF field codes was known as the "Potomac Code"; it was the first of the so-called "American River Series," and it 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," "randomized," or, least of all, the British nomenclature "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 common 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 messages 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 remains 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, 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 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. Copies are on file in the Office of Training. 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.

In Lecture No. 4 two USMC cipher messages were given and I said that their solutions would be presented at the conclusion of the next lecture. Here they are, both being from Major General Buell to General in Chief Halleck, relating to the relief and reinstatement of Buell.



Louisville, Ky., September 29, 1862

Maj. Gen. Halleck, General in Chief:

I have received your orders of the 24th inst., requiring me to turn over my command to Maj. Gen. G. H. Thomas. I have accordingly turned over the command to him, and in further obedience to your instructions, I shall repair to Indianapolis and await further orders.

D. C. Buell,  
Major-General

Louisville, Ky., September 30, 1862

General Halleck:

I received last evening your dispatch suspending my removal from command. Out of a sense of public duty, I shall continue to discharge the duties of my command to the best of my ability until otherwise ordered.

D. C. Buell,  
Major-General