From the day that Ambassador Page sent his cablegram to President Wilson (24 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 ~~was assured.~~ became a certainty, because after assuring himself of the authenticity of the telegram handed over by the British, the President released the text to the head of the Associated Press in Washington, with the consequence that under big black headlines the English text appeared in our newspapers ~~on 1 March~~ the next day. that the United States Congress declared war on Germany and the Central Powers. The date was 6 April 1917. For instance, here is the bold black 8-column headline in the New York Times of 1 March:

GERMANY SEEKS ALLIANCE AGAINST U. S.
ASKS JAPAN AND MEXICO TO JOIN HER;
FULL TEXT OF HER PROPOSAL MADE PUBLIC.

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

MEXICO AND JAPAN ASKED BY GERMANY TO
ATTACK U. S. IF IT ENTERED THE WAR;
BERNSTORFF A LEADING FIGURE IN PLOT

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

There were plenty of senators and representatives who disbelieved the story. It was too fantastic; it was a British plot, unproved; Wilson was being taken in, etc., etc. But when Zimmermann himself foolishly acknowledged that he had indeed sent such a telegram, disbelief changed quickly into vehement anger. Surely war would now be declared on Germany!

Still, notwithstanding all the furor that the disclosure of the Zimmermann Telegram created in America, President Wilson still hesitated and it was not until more than a month later, and after several American ships were sunk without warning on 18 March, In the War Department and in the Navy Department the pace set for preparing for active war operations quickened. There was at the moment in neither of those departments nor in the Army or in the Navy any organizations whatever either for intercepting enemy communications or for studying them. There was, it is ture, since the autumn of 1916 a very small group of self-trained cryptanalysts supported by a private citizen named Colonel Fabyan* who operated the Riverbank Laboratories at Geneva, Illinois. That organization maintained an unofficial relationship with the authorities in Washington and received from time to time copies of cryptographic messages obtained by surreptitious means from telegraph and cable offices in Washington. At that period in our history diplomatic relations with Mexico were in a sad state so that U. S. attention was concentrated southward. Therefore practically all the messages sent to Riverbank were those of the Mexican Government. Under my direction Riverbank was successful in solving all or nearly all the Mexican cryptograms it was given usually returning the solutions to Washington very promptly. It was also successful with certain other cryptograms but I cannot deal with them now because there just isn't time. Soon after war was declared on Germany the Riverbank Laboratories established a school for training Army and Navy officers sent there to learn something about cryptology.

You may like to know what we used for training ourselves for this unusual task, and later, what we used later on for training the student officers sent to Riverbank for cryptologic instruction. As regards our self-instruction training material, there wasn't much but among the very sparse literature in English there was a small book

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

entitled Manual for the Solution of Military Ciphers, which had been prepared by a Captain Parker Hitt and printed by the Press of the Army Service Schools at Fort Leavenworth, in 1916. The Signal Corps School was then one of those 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 ciphers. They foresaw that sooner or later there would be a need for knowledge and training in military cryptology. Capt. Hitt's Manual, was then and still is a model of compactness and practicality. Here is its title page.

FIG. 00

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

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

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

In Lecture II (Fig. 27) there is a picture of the last of the several classes sent by The Adjutant General of the Army to Riverbank for training. It should be noted that this instruction was conducted at Colonel Fabyan's own expense as his patriotic contribution to the U. S. war effort. Upon completion of the last training course I was commissioned first lieutenant and ordered immediately to proceed to American General Headquarters in France where I became a member of the German Code and Cipher Solving Section of the General Staff, a designation that was abbreviated as G-2, A-6, GHQ-A.E.F. As the expanded designation implies, the operations were conducted in two principal sections, one devoted to working on German Army field ciphers, the other, to working on German Army field codes. There were other very small groups working on other material such as meteorologic messages, reports on direction-finding bearings, and what we now call traffic, that is, the study of enemy messages in order to determine enemy order of battle from intelligence and analysis of D.F. bearing, of the direction, ebb and flow of enemy traffic and other data sent back from our radio direction-finding operations at or near our own intercept stations.

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

FIG. 00

This particular chart was drawn up from data based solely upon the ebb and flow of messages in what was called the ADFGVX cipher*, a clever cryptosystem which was devised by German cryptographers and only used by German High Command communications, principally between and among the headquarters of divisions and army corps.

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

Theoretically it was extremely secure because it combined both a good substitution and an excellent transposition principle in one and the same method without being too complicated for cipher clerks. Here is a diagram which, if studied carefully, will give a clear understanding of its method of usage. 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 that system appeared at that time to be absolutely impregnable against solution, a great many messages transmitted in the ADFGVX system were read by the Allies. You may be astonished by the foregoing statement and may desire some enlightenment here and now on this point. Well, in brief, there were in those days three different methods of attacking the traffic in that cipher. Under the first method two or more messages with identical plain-text beginning could be used to uncover the transposition as the first step. Once this had been done, the cryptanalyst had then to deal with a simple substitution in which, two letter combinations of the letters A, D, F, G, V, and X represented single plain-text letters. The messages were usually of sufficient length for this purpose. Under the second method, two or more messages with identical plain-text endings could be used to uncover the transposition and this was easier even then in the case of messages with identical beginnings. You might think that cases of messages with identical beginnings or endings would be rather rare, but the addiction to stereo-typic phraseology in the German military mentality was then--and perhaps still is-so confirmed, that cases were almost invariably found in each day's traffic. This is astonishing considering that the keys changed daily. This system first came into use on 1 March 1918, three weeks before the last and greatest spring offensive by the German Army. Its appearance was almost coincident with that of other new codes and ciphers. The number of messages in the ADFGVX cipher varied from about 25 a day, when the system first went into use, to as many as about 150 at the end of two months. It took about a month to figure out a method of solution, and this was done by a very able cryptanalyst named Capt. George Painvim of the French Cipher Bureau.

The ADFGVX cipher was used quite extensively during May and June of 1918 but then the number of messages dropped very considerably. How many different keys were solved by the Allied? Not many--10 in all, that is, the keys for only 10 different days were found. Yet, because the traffic on those days was heavy about 50% of all messages sent in that cipher were read and a great deal of valuable intelligence was derived. 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 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 devised 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, a similar one was encountered in a book by French General Givierge (Cours de Cryptographie), published in 1925.

The ADFGVX cipher was not the only one used by the German Army in World War I, and there will be time to mention only very briefly two others. The first of these was a polyalphabetic substitution cipher called the "Wilhelm," which used a cipher square with a set of 30 fairly lengthy keywords. The cipher square is shown in Fig. 00 and the set of keys as originally recovered is shown in Fig. 00. Just why the square contains only 22 rows instead of 26 is unknown. Certainly the rows within the square are not random sequences for the letters within them manifest permuted arrangements in sets of vies; nor are the key sequences of random letters. I leave it to you to try to reconstruct the real square and the real keys. The latter problem should be relatively easy; as to the former. I really don't know--I have never tried it myself but I suspect some systematic disarrangement, something typical of German cryptography.

The other cipher to be mentioned is the double transposition, an example of which is shown in Fig. 00. The process consists in applying the same transposition key twice. Solution of the true double transposition usually depended upon finding two messages of identical length. No general solution was known to the Allies during the World War I. Occasionally an operator would apply only the first transposition and when this happended solution was easy. Then the key thus recovered could be used to decipher other messages which had been correctly enciphered by the double transposition. Again, students of the Signal Intelligence Service devised a general solution for the double transposition cipher and during World War II were able to prove to our British Allies that such ciphers could be solved without having to find two messages of identical length. Having demonstrated the weakness of the system even when properly employed, it was probably withdrawn from usage by the British, but we were not told directly that this was done. I should add that I think the devising of a general solution for the true double transposition cipher represents a real landmark of progress in cryptanalysis without the aid of high-speed, electronic equipment. I do not doubt that with such equipment this cipher could hardly be thought to be safe for modern military secret communications.

We come now to the code systems used by the belligerents in World War II. 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." dealt with stupendous success on the code used for the transmission of the Zimmermann Telegram. But that's only part of the story--the most important part remains to be told and unfortunately I cannot divulge that part yet. Excessive pride in German achievement, a wholely unjustified confidence in their cryptosecurity, and a disdain for the prowess of enemy cryptanalysts laid German diplomatic communications open to solution by the Allies to the point where there came a time when nothing the German Foreign Office was telling its representatives abroad by telegraph, cable or radio remained secret from the British. For those of you who would like to learn some details,,I refer you to the following fine 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. This monograph is Confidential; and copies are available in the Office of Training, NSA.

"At the time of America's entrance into the war German codes were an unexplored field in the United States, says Dr. Mendelsohn." About a year later we received from the British a copy of a partial reconstruction of the German Code 13040 (about half of the vocabulary of 19,200 words and 800 of the possibly 7,600 proper names). This code and its variations 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 of historical interest, which were now read with the aid of the code book." The vocabulary of the German diplomatic codes contained 189 pages eontaining exactly 100 words or expressions to the page, arranged in two columns of 50 each accompained by numbers from 00 to 99. Here is a copy of a typical page in Code 13040. In each column the groups in the left-hand column, for instance, 00-09, 10-19, etc., to 40-49; than 50-59, etc., were in blocks of 10. The pages in the basic code were numbered at the top from 10 to 239 and from this code several derivative codes were made by the use of conversion tables. This enabled the original single basic code to serve as the framework for codes for several different communication nets. What the number of the basic code was is unknown, but we do know that from the derived code designated 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 (penultinate 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 can by no means be considered as being different codes. They were all relatively minor equivalents of one another. Also to be mentioned is the fact that in certain cases 3-digit numbers were added to or subtracted from the code numbers of a message and that in practically every case it was not difficult to determine the additive or subtractive.

In none of the cases or codes mentioned thus far was there one that could at least be considered to be a randomized," hatted," or true two-part code, since the same book served for both encoding and decoding. Some of these, besides the ones already mentioned (13040 and 5950) were designated by indicators, such as 12444, 1357, 18470, 1777, 2815, 4565, 5717, 44499, 58585, 2310, 98989, 1111, 80574; there were others besides these. It is my belief that conversion tables were not used by the code clerks but by the compiling authorities in Beolin. In other words, the various versions of the basic code were not actually printed as separate books but that the original page number on each page was altered by hand, the original number being crossed out and written either at the top or the bottom of the page, perhaps in both places. Similarly, the block numbers were probably changed byhand. In both cases the alterations were in accordance with some system, the idea of randomicity seems foreign to the German mentality, and I am sure that if randomicity were a desideratum they would figure out a system therefor. However, the German Foreign

Office later on did compile and use true two-part, truly randomized codes of 10,000 groups numbered from 0000 to 9999. One such code had as its indicator the number 7500. And that there were several others like it I have no doubt.

When one reviews Dr. Mendelsohn's monograph one becomes overwhelmed by the multiplicity of the codes and variants thereof used by the German Foreign Office. Many were basic codes but many were derivatives, or superencipherments thereof. It is even hard to ascertain the exact number of different methods. Yet a great deal of the traffic in these codes was read. Considering the rather small number of persons on the cryptanalytic staff of G-2 in Washington and its homologous organization in London, in the British Black Chamber, one can only be astonished by the great achievements of the efforts of these two collaborating organizations 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 cousequent 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 or expression, terminology and style, and these items became of great importance in cryptanalysis when German cryptosystems improved. For the German Army learned by hard experience something about is shortcomings in this area of warfare and began to improve to the point where we must credit the Germans with being the initiators of most of the new and very important developments in field military cryptography. In fact, the developments and improvements began not longer 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 traffic during that war have appeared same for one very brief article by a not very bright German cryptanalyst. One could of course assume that they kept their successes very well hidden but the German archives taken at the end of World War II contain nothing significant in regard to cryptanalysis during World War I although a great deal of important information in this field during World War II was found. A detailed account of the cryptologic war between the Allied and German forces in World War II would require scores of volumes, but 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 cipher systems that were used. There remain to be discussed the field codes. It was the German Army which first proved that the old idea that codebooks were impractical for use in the combat zone for tactical communications was wrong. They had two different types of field codes, one which the Germans called the SCHLUESSEL HEFT or "key" but which we called the "three number code"; the other the "three-letter code". The former was a small standardized code with a vocabulary of frequently used words and expressions, digits, letters and syllables totally 1,000 items for which the code equivalents were 3-digit numbers. A cipher was applied only to the first two digits of code numbers and this cipher consisted of a 10 x 10 matrix for the numbers from 00 to 99. The last digit of a code group remained unenciphered. Each division compiled and issued its own table, which was in two parts, one for encipherment the other for decipherment. The three-number code was intended for use in all forms of communication within or to and from a 3-kilometer front-line danger zone. Although this code was compiled by the end of January 1918 it was not put into use until the opening day of the last and greatest German offensive, 10 March 1918. The nature of the new code was ascertained and a few groups in it were solved the very same day because an operator who was unable to translate a message in the new code requested and received repetition in the old code, the three-letter code, and the letter had been solved to an extent which made it possible to identify homologous code groups in both messages. The three-number proved rather easy to solve on a daily basis and much useful intelligence was obtained thereby.

The solution of the three-letter code, however, proved much more difficult. In the first place, it had a much larger vocabulary, with nulls and many variants for frequently-used words and numbers; in the second place and what constituted 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, OO 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 the code was really a painfully slow, very difficult and generally frustrating experience. On my reporting for duty Colonel Frank Moorman, who was Chief of the whole unit and whose photograph I show you here, asked me whether I wished to be assigned to the cipher 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. I gained the experience I wanted and needed to broaden knowledge and practice in cryptology but little did I realize what a painful and frustrating period of learning and training I had undertaken. Still, I have never regretted the choice I made; in fact, it turned out to be a very wise and useful one. If any of you would like to read about my experience in this area, let me refer you to my monograph entitled Field Codes Used by the German Army during the World War, copies of which are on file in the Office of Training, NSA. I will quote a few paragraphs from my "estimate of the three-letter code" as it appears on page 65 of that monograph:

What sort 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:

FIG. 00

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 will show a picture of one of them. Then, in addition, there was a much more extensive code which was not only a two-part, randomized book, 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, "telegraphic par sol", or earth· telegraphy. Here is one of the tables used for enciphering (and deciphering) the code groups:

FIG. 00

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

FIG. 00

You will notice that the enciphering process breaks up the 4-digit groups in a rather clever manner by enciphering 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 suceeds 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 cryptosystems is that theoretically at least, it certainly was the most secure of all the systems used by the belligerents but I don't know how much usage was made of it. I venture the opinion that it was not used often, or successfully, with the superenciphering method provided for the basic code.

Now how about the cryptosystems used by the British Army? First, they used the Playfair Cipher, a system of digraphic substitution considered in those days to be good enough for unimportant messages in the combat zóne. But today, of course, its security is known to be so low as to be unworthy of placing any reliance in it. The British also used a field code. It 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 unfortunately am not in a position to describe it. I don't even have a copy of their code--only a typewritten transcript which was furnished us quite reluctantly and I will show a typical page thereof.

FIG. OO

What about the cryptosystems used by the Italian Army in World War I? The general level of cryptologic work during that period was quite low in character, a fact which is all the more remarkable when we consider that the birthplace of modern cryptology was in Italy several centuries before this period. There appears to have been in Italy a far greater knowledge of cryptologic techniques in the 15th and 16th Centuries than in the 19th, paradoxical as this may seem to us today. Perhaps this can be considered as one of the consequences of a policy of secrecy which not only makes filing away in dusty archives records of cryptanalytic successes a desideratum but also hinders or absolutely prevents those who might have been born with what it takes to develop a flair for cryptologic work from profitting from the progress of predecessors who have been successful in such work. Should we be astonished to learn, therefor, that when Italy entered into World War I the Italian Army put its trust in a very simple variation of the ancient Vigenere cipher, a system called the "cifrario militaire taseabile" 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 cryptologic work in World War I? So far as Russian cryptographic work is concerned we know that there was during Czaristic days an apparently well organized and effective bureau for constructing and compiling diplomatic codes and ciphers, organized by a Russian named Savinsky, formerly Russian Minister to Stockholm. He had all codes and cipher in use up to then improved, introduced strict regulations for their use, and kept close watch over the service. He also was head of a cryptanalytic activity and it is known that Turkish, British, Austrian and Swedish diplomatic messages were solved. After the Bolshevik revolution of 1916 some of the Russian cryptanalysts managed to escape from their homeland and I had the pleasure of meeting and talking with one of the best of them during his service in the black chamber of one of our Allies in World War II. He wore with great pride on the index finger of his right hand a ring in which was mounted a beautiful large ruby, the ring having been presented him by the last Czar in recognition of his cryptanalytic successes while in his service.

But the story is altogether different as regards cryptology in the Russian Army.

The Military Cryptographic Service was poorly organized and, besides, it had adopted a cryptographic system which proved to be too complicated for the ignorant and poorly trained Russian cipher and radio operators to use when it was placed into effect toward the end of 1914. Here is an example of that cipher, which has an enciphering and a deciphering table:

FIG. 00

In the enciphering table the letters of the Russian alphabet (33 in all) appear in the top line; the 2-digit groups in random order within the 8 rows below are their cipher equivalents and these rows therefore constitute a set of 8 cipher alphabets preceded by key numbers from 1 to 8 in random order, also subject to change. Indicators were used to indicate how many letters were enciphered consecutively in each alphabet, the indicator consisting of one of the digits from 1 to 9 repeated five times. The alphabets were then used in key-number sequence enciphering the first set of letters (5, 7, etc., according to the indicator) by alphabet 1, the next set by alphabet 2, and so on. After the 8th set of letters, which was enciphered by cipher alphabet 8, return is made to cipher alphabet 1, repeating the sequence in this manner until the entire message had been enciphered. In enciphering a long message the cipher operator could change the number of letters enciphered consecutively by inserting another indicator repeated five times and then continuing with the next alphabet in the sequence of alphabets. The cipher text was then sent in 5-digit groups. The use of the deciphering table hardly requires explanation but a 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 remains a puzzle to me.

I have told you that this cipher system proved too difficult to use, so difficult that messages had to be repeated over and over, with great loss of time. It is well known that the Russians lost the Battle of Tannenberg in the autumn of 1914 was largely because of faulty communications. Poor cryptography or failure to use even simple ciphers properly on the field of battle, and not brilliant strategy on the part of the enemy, was the cause of Russia's defeat in that and in subsequent battles. The contents of Russian communications became known to the German and Austrian High Commands within a few hours after transmission by radio. The disposition and movements of Russian troops, and Russian strategic plans were no secrets to the enemy. The detailed and absolutelyreliable 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 read a message to a unit that had not yet received the new key and then repeat the identical message in the old one. I suppose the Russians committed every error in the catalog of cryptographic criminology. No wonder they lost the Battle of Tannenberg, which one military critic said was not a battle but a massacre, because the Russians lost 100,000 men in the 3-day engagement, on the last day of which the Russian commander-in-chief committed suicide. Three weeks later another high Russian commander followed suit and the Russian Army began to fall apart, completely disorganized without leadership or plans. Russia itself began to go down in ruins when its Army, Navy and Government failed so completely, and this made way for the birth of the October revolution, ushering in a regime that was too weak to put things together again and to hold them together. The remnants picked up by a small band of fanatics with military and administrative ability, with treachery, violence and cunning, welded together what has now become a mighty adversary of the Western World, the USSR.

I have left to be treated last in this lecture the cryptosystems used by the American Expeditionary Forces in Europe during our participation in World War I.

When the first contingents of the AEF arrived in France in the summer of 1917, there were available for secret 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 Fig. 00, and will let you assess its security yourself.

FIG. 00

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

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

Just as the invention of Morse wire telegraphy had a remarkable effect upon military communications during the American Civil War, as related in the preceding lecture, so the invention of radio also played a very important role in field communications during World War II. Now, althoggh 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 had been determined that field codes were needed little time was lost in getting on with the job that had to be done. Since I had no part in this effort I can say, without danger of being misunderstood as to motives, that the Code Compilation Service executed the most remarkable job in the history of military cryptography up to the time of World War II.

The first work entrusted to it was the compilation of "Trench Code", of which 1000 copies were printed, together with what were called "distortion tables". These were simple monoalphabets for enciphering the 2-letter groups of the code. I show a picture of a page of this code and of one of the "distortion tables".

FIG. 00
(p. 132)

FIG. 00
(p. 142)

The danger of capture of these codes was recognized as being such that the books were not issued below battalions. Hence, too meet the needs of the front line, a much smaller book was prepared and printed, called the "Front Line Code". Distortion tables, 30 of them in all, were issued to accompany this code of which an edition of 3,000 copies was printed--but not distributed, because a study of its security showed defects. AEF cryptographers were grouping in the dark, with little or no help from allies and with personnel inexperienced in cryptanalysis. Finally, the light broke through: the Code Compilation Service began to see the advantages of the German 3-letter randomized 2-part code known as the Satzbuch. I've told you about this code and what the AEF learned about its advantages. Here, then, was the origin of the AEF real Trench Codes--copying from the experience of German code compilation and then going them one better. The first code of the new series, known as the "Potomac Code", the first of the so-called "American River Series," appeared on 24 June 1918, in an edition of 2,000 copies. It contained approximately 1,700 words and phrases and, as the official report so succinctly states, "was made up with a coding and decoding section in order to reduce the work of the operators at the front." The designation "two-part" or "randomized," or even "hatted" code was still unknown--but the principle was there nonetheless. Let us see what the official report goes on to say on this point; let us listen to some sound commense 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!7, and put the burden of work upon general headquarters, where it preperly belonged. Under this system one issue of codes could be distributed down to regiments; another issue held at Army Headquarters; and a third issue held at General Headquarters. As a matter of record this first book, the Potomac, was captured by the enemy on July 20, just one month after issuance, but within two days, it had been replaced throughout the entire Army in the field."

The replacement code was the Suwanee, the next in the River Series, followed by the Wabash, Allegheny, and the Hudson, all for the American First Army. In October 1918 a departure in plan was made and different codes were issued simultaneously to the First and Second Armies. This was done in order not to jeopardize unnecessarily the life of the codes by putting in the field at one time 5,000 and 6,000 copies of any one issue. Thus the Champlain, the first of what came to be called the "Lake Series" for the Second Army was issued with the Colorado of the "River Series" for the First Army; these were followed by the Huron and the Osage, the Seneca and the Niagara, in editions of 2,500 each.

In addition to the foregoing series of codes were certain others that should be mentioned, as for example, a short code of 2-letter code groups to be used by front line troops as an emergency code; a short code list for reporting casualties; a telephone code for disguising the names of commanding officers and their units, and so on. But there was in addition to all the foregoing one large code that must be mentioned, a code to meet the requirements for secure transmission of message among the higher commands in the field and between these and GHQ. This was a task of considerable magnitude and required several months study of messages, confidential papers concerning organization, replacement, operations, and of military documents of all sorts. The code was to be known as the AEF Staff Code. In May 1918, the manuscript of this code was sent to press and the printing job was done in one month by the printing facilities of the AEF Adjutant General. Considering that the code contained approximately 30,000 words and phrases, accompanied by code groups consisting of 5-figure groups and 4-letter groups, the task completed represents a remarkable achievement by a field printing organization and I believe that this was the largest and most comprehensive codebook ever compiled and printed by an army in the field. More then 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.