THE INFANTRY SCHOOL
Fort Benning, Georgia

ADVANCED COMMUNICATION COURSE
1939-40

# Military Codes and Ciphers

## Their Development and Use

Thomas B. Evans

Thomas B. Evans, 1st Lieutenant, Infantry

TABLE OF CONTENTS

# BIBLIOGRAPHY

| Abbreviations | Text |
|---|---|
| Gylden | The Contribution of the Cryptographic Bureaus in the World War. Written by Mr. Yves Gylden, a well known Swedish code and cipher expert. Translated by the Military Intelligence Division of the War Department General Staff. The translation appeared in installments in the Signal Corps Bulletin. (Library Classification: D 570.346 U 5.) |
| Koch | Cryptography or Cipher Writing. Written by Edward Koch. Published by Buechler Publishing Company. (Library Classification: UB 290.K 81.) An interesting essay on cryptography for the beginner. |
| Yardley | American Black Chamber. Written by Herbert O. Yardley. Published by the Bobbs-Merrill Company. (Library Classification: D 639 S7 Y3.) Yardley was an officer of the United States Army and a famous cryptanalyst. The book is well written and interesting to read. |
| S.C.B. | Signal Corps Bulletin No. 101. Office of the Chief Signal Officer, September 1938. (Library Classification: Ug 573 U 2.) Contains an article, "The Use of Codes and Ciphers in the World War and Lessons to be Learned Therefrom," pp 35-48. Written by Lieutenant Colonel William F. Friedman, Signal Reserve. Lieutenant Colonel Friedman is a well known cryptanalyst of today. |

## I. INTRODUCTION

1. DEFINITIONS.--Before discussing the origin and the use of codes and ciphers, I refer to Webster's Dictionary for definitions of the words "code" and "cipher". Webster defines the word "code" as a "system of words or other symbols arbitrarily used to represent words or phrases for brevity or secrecy." He defines the word "cipher" as "a private alphabet, system of characters, or the like, contrived for secret writing." Note that in both definitions the word "secret" is used. It is imperative that armies maintain the utmost secrecy in transmitting messages and orders over wires and through the ether. It is because of this necessity for secrecy that the development of codes and ciphers has become a major problem of the armies of the past and present.

2. FIRST USE OF SECRET WRITING.--Primitive man expressed himself by means of pictures. Early biblical characters were known to have made use of ciphers. Jeremiah, fearing that the Babylonians would be excited by his letter to his people, used the word "Sheshek" for the word "Babel" (Jeremiah XXV, 26). Instead of using the 2d and 12th letters from the beginning of the alphabet (b and l), he used the 2d and 12th from the end (sh and k). (1) However, only very primitive methods were used throughout the early ages so that little is gained by discussing further this period of cryptography.

## II. PERIOD OF DECADENCE OF CRYPTOGRAPHY

3. DEVELOPMENTS.--The period prior to 1880 is known as the period of decadence of cryptography. (2) During this period little was done in the development of cryptography. The idea grew that persons not qualified in cryptanalysis

---

(1) Koch
(2) Gylden

could compile and employ safe codes and ciphers. There were in use many simple means of sending messages secretly, and, as little work had been done in breaking down these methods, they were fairly successful. The early monks devised ciphers using a simple transposition of the letters of the alphabet. The earliest known cryptographic bureaus were located at Venice under the Doges and at the papel curia in Rome (1300-1400 AD). (3) This work, although technical in nature, was kept secret so that the rest of the world was not allowed to benefit by it. The little work that was done by other individuals of the world was kept very secret. Hence, there was no apparent development of cryptography.

4. RULES OF LORD BACON.--It was during this period that Lord Bacon, a renowned cryptographic expert of his time, gave three fundamental rules to be used in making up a system for codes or ciphers. They were:

a. That they be not laborious to write or read.

b. That they be impossible to decipher or decode.

c. That, in some cases, they be without suspicion.

It can easily be seen that any system that fulfilled these requirements would certainly be perfect. It will be shown later that there never has been any system developed that fulfilled all the requirements Lord Bacon laid down.

5. EXAMPLES.--Some examples of the use of codes and ciphers during the period of decadence are interesting to note. In early history we find that Histeaeus, anxious to get a message through the enemy lines, hit upon an ingenious scheme. He had the hair of a trusted servant shaved off, and he then pricked the desired message on the servant's head. After the hair had grown out, the servant passed safely through the lines. (4)

---

(3) Gylden
(4) Koch

The early Spartans used one of the most secret of all ciphers. Their method was practically indecipherable. A narrow strip of parchment was wound around a stick at a certain angle. The message was then written on the paper. When the paper was unwound it would appear to be a long column of meaningless letters. In order to read the message it was necessary to wind the paper around another stick of the same size and at the same angle. (5)

We also find that ciphers were used by the English in their civil war. A cipher used by the Portuguese brought on the battle of Montejo which gave them their independence in 1644-45 AD.

Both the Federal and Confederate Armies used codes during the Civil War, but they were very unsafe and resulted in misplaced confidence. A good example of the failure to use any code or cipher was at Gettysburg. During the battle General Meade was about to give the order for the withdrawal of his forces on the following day, when a messenger arrived with a message taken from a captured Confederate soldier. The message was a dispatch in clear from President Jefferson to General Lee telling him that it was impossible to assemble another army to threaten Washington. Consequently, the withdrawal order was never issued. If this dispatch had been encoded or enciphered, the withdrawal order would have been issued and the whole course of the remainder of the war might have been changed.

## III. CRYPTOGRAPHY PRIOR TO THE WORLD WAR

6. DEVELOPMENTS.--The period from 1880 to 1914 might well be called the high school of cryptography students. During this period the science of cryptography improved

---

(5) Koch

decidedly. Now we find that countries have begun to realize the importance of cryptanalysis, and hence have organized bureaus and departments for the furtherance of their codes and ciphers. In order to clearly show the cryptographic work that was carried on during this period, I will briefly describe the developments of each of the important powers.

a. French.--The French should be called the dean of the cryptography high school. Prior to the war they had a well organized bureau whose purpose was to develop codes and ciphers. It worked directly under the Ministry of War. All of the bureau's work was very secret. However, it attempted to create an interest in cryptography among civilians by circulation of appropriate literature among them. We shall see that the bureau developed a code that was used with success during the war. Its most famous work was done in connection with the Dreyfus case, when the bureau decoded messages sent by the Italian Military Attache, Panizzardi, to the military authorities in Italy. The bureau had some difficulty breaking Panizzardi's code so a member of the French government asked him to send a secret telegram to the Italian government for him. The bureau knew the contents of the telegram. With an intercepted copy of the encoded telegram, the bureau had no trouble breaking the code. (6)

b. Germans.--The Germans, although famous for their military tactics and equipment, were sadly lacking in cryptographic knowledge. There was very little literature available to them on the subject. There was no cooperation between branches of the government using codes. Most of the cryptographic work was carried on by the Army directly under the General Staff, resulting in a lack of freedom of action.

---

(6) Gylden

Their ignorance of cryptanalysis caused them to rely too much on the safety of their codes and to employ unqualified men to make them up. The French were later to make good use of this ignorance.

c. British.--The British were well organized for cryptographic work. Civilians were organized for the work under the mobilization plans. The most important work was done under the supervision of the Navy. There was close cooperation among all branches of the government that used codes. They employed the French system of ciphers. A Parisian book dealer, who specialized in books on cryptography, stated that Englishmen were his best customers.

d. United States.--Since the United States did not enter the war until 1917, it had time to observe the importance of secret codes. However, in 1913 our so-called "secret codes" were not very secret. Our diplomatic messages were sent in a code which could be easily decoded by anyone versed in cryptanalysis. We had no bureau for breaking down secret diplomatic codes and cipher telegrams of foreign countries. The Army had a text book for a course in cipher solutions which was used at the Signal School at Fort Leavenworth. The types of ciphers it discussed were of the simplest form. Finally a bureau was organized in the War Department under the direction of Herbert O. Yardley. This bureau, starting from scratch, built one of the most important cryptanalytic bureaus developed prior to or during the war. It developed new codes to be used by the departments of the government. Above all, it provided instructors in cryptography for our military branches. Its work was carried on so successfully that, after we entered the war our army was furnished with codes that were secret and played a very important part in our successes in the war. Later we shall see how unprepared our troops were in the use of these codes.

I will only mention here that the cryptographic work done by the other nations of the world was unimportant and wholly unsuccessful. The principal reason for this was due to the fact that literature and instructors in cryptography were not available.

## IV. MILITARY CODES AND CIPHERS DURING THE WORLD WAR

7. PERIOD FROM 1914 to 1916.--More material is available on the use of codes and ciphers during the World War than is available for any other period. This is due mainly to the fact that some nations have published material concerning the cryptographic work of their enemies during the war. This material has been compiled by numerous authors and is now available for an interesting study. Here again I will discuss the cryptographic work of each of the major powers involved in the war.

a. Developments and uses by Germany.--As was stated before, the Germans were lacking sadly in cryptographic knowledge prior to the war. So, at the outbreak of the war, the use of codes and ciphers caused more damage than good. At first they used a double transposition cipher. This not only caused an undesired loss of time but was also a source of many errors. It is known that as much as 24 hours were required to transmit a message by radio using the cipher. Consequently, commanders were reluctant to have important messages enciphered.

The Germans also tried a form of superencipherment in which a certain number or letter was added or subtracted from each group. This proved most disastrous. Changes of keys were carelessly made, and the superencipherment itself put into the hands of untrained men was poorly handled. The

British were praised highly by the Germans for their efficiency in breaking the German cipher, whereas it was the Germans themselves who gave the British such excellent chances. (7)

Due to their lack of cryptographic knowledge, the Germans failed to do much in cryptanalysis. During the period from 1914 to 1916 practically no cryptanalytic work was done by them. Had cryptanalytic work been done in the early stages of the war, they might have been able to discover the weaknesses of their own systems. It was not until 1917 that it may be said the Germans caught up with the allies in cryptographic work, but they never equaled the allies in cryptanalysis. The Germans never acquired the technical ability to do cryptanalysis successfully. They did not establish any intercept stations. The few enemy messages that were obtained by means of radios were obtained by operators passing the time away. The success that the Germans had at Tannenberg was due to the intercepting of clear text radio messages, not to the work of any cryptanalysts.

b. Developments and uses by France.--The French had a well organized cryptanalytic bureau before the war so that when war was declared it immediately expanded with units along the Western Front. By means of intercept stations they were able to obtain many German messages and to break them down in time to be of great use. In some instances messages were received in which parts were in clear and in cipher. Also in some cases, the German receiving operator could not decipher a message, so he would request that it be transmitted in clear. Usually the request was granted. All this made it quite easy for the French to break down the German cipher. The use of stereotyped phrases by the Germans also was a great help to the French in breaking down their ciphers. This use

---

(7) Gylden

of stereotyped phrases in military messages has been and continues to be one of the weakest points in the use of codes and ciphers. It can be seen that if the cryptanalyst discovers the beginning of a stereotyped phrase a lot of the contents of the message can be deduced without further efforts. The French made no effort to keep secret the fact that they had broken the German cipher. Even the privates in the front line joked about it. So it was only a short time until the Germans began using a new cipher. It took the French three weeks to breakdown the new one. However, this time steps were taken to keep secret the fact that the new German cipher had been broken down.

The French had trouble enough in the use of their own codes and ciphers. They found that the clerks who were detailed to encipher messages were not competent so officers especially trained for that work were detailed to encipher all messages. In spite of these specialists many blunders were made in the use of the cipher. Two of the most evident blunders were: (1) the confirming by telephone in clear messages that had been sent by radio in cipher; and (2) sending messages by means of telegraph in mixed text. As these blunders became apparent an order was published in January 1915, requiring all officers who were doing the enciphering and encoding to encryptograph four or five rather long messages every day for one month as necessary training in their work. (8) The French used a code for correspondence between Army Headquarters and General Headquarters and an irregular transposition cipher for correspondence between smaller units.

c. Developments and uses by Russia.--Of all the nations engaged in the war the Russians were perhaps the worst offenders in the misuse of codes and ciphers. They had very few men

---

(8) Gylden

trained in cryptography and none in cryptanalysis. Consequently their cipher was even more difficult to use than that of the Germans. In most cases the clerks could not encipher the messages, and, when they were enciphered, the clerk at the addressee's headquarters could not decipher it. They used a system known as a "Sprungchiffer" which was formed by substituting two-figured groups for letters and periodically changing to other corresponding alphabets. (9) This system was so complicated that by the end of 1914 they went back to a simple substitution cipher which was very simple for the allies to break down. It was broken through a blunder of an operator who sent in the old cipher a message which had previously been sent in the new cipher.

8. PERIOD FROM 1917 to 1918.--a. The use of code books.--The period from 1917 to 1918, often referred to as the "code book period", brings out an interesting study in the use of codes. Prior to this time ciphers had been relied on to a great extent. Little use was made of codes. The French possessed a code book containing about fifty expressions. It is quite evident how inadequate such a code book would be. Then, too, clerks made even more blunders using codes than they did using ciphers. One of the most serious blunders was to mix clear text with code. Another common practice was to make use of "cover" words. As an example, the following message would be sent: "We are in need of herrings. Cannot fish until they arrive." With a little thought it is seen that the message means "We are in need of reinforcements. Cannot advance until they arrive." Such poor results from the use of codes resulted in a failure to use them at all. However, during 1917 we find both the Germans and the French making more use of codes.

---

(9) Gylden

The types of codes used by the Germans and the French during the latter part of the war were very similar in nature. They were similar in structure to the code used in our army at present. The Germans used a group of numbers instead of a group of letters to represent a word or phrase. These codes were changed quite frequently. In fact, the French admitted that they solved thirty German codes before the end of the war. Needless to say, it was the poor handling of the codes by the German clerks that helped the French to break down these codes. The use of superenciphered codes was tried by the Germans. They proved to be difficult for the lower units to use. The higher units used them but handled them poorly, and they were broken down readily by the French.

During the latter part of the war, when the Germans began to realize the weakness of their codes and code personnel, they took steps to correct these deficiencies. Their clerks had become better trained through experience. The codes were improved by the use of auxiliary expressions for the time of day, numbers, and syllables. Nulls were used for the first time. These puzzled the expert cryptanalysts a great deal.

At the same time they were improving their codes they were improving their cryptanalysts. Schools were conducted, and gradually men were developed into capable cryptanalysts. During the last months of the war the central cryptanalytic bureau at Spa did excellent work in breaking down several French codes. All this work in cryptanalysis aided the Germans in developing codes which were safer than any they had used before. It cannot be emphasized enough that men who make up codes must be well trained in cryptanalysis.

When the American troops arrived in France, the only cryptographic equipment they had was the Playfair cipher and the old War Department Telegraph Code. (10) The Playfair

---

(10) SCB

code, also used by the British, was very simple. Captain Yardley, in his book, the "Black Chamber", describes the War Department Telegraph Code as being of a form which was very simple to break down. Nevertheless, the fine work of the American Cryptographic Bureau resulted in the compilation of a good code. The code was so good that by 1918 the French and the British were convinced that it was better than theirs and made plans to change their own in favor of the American system. But the American troops had the same trouble as the troops of the other countries in that they were not trained well enough to use the code. They had had no experience in the use of codes prior to the war.

b. The Wheatstone cipher.--An effort was made in the allied forces to adopt a cipher device to be used by all the allied armies. It was to be one that would be simple for the untrained clerks to use. An Englishman named Wheatstone, of Wheatstone Bridge fame, invented the cipher device which was to be used. The British were very proud of it and submitted it to the United States for test. A group of cryptanalysts working under Mrs. Friedman, having only five short messages in the same key, were able to break the cipher in three hours. Needless to say, the cipher was not adopted.

## V. CODES AND CIPHERS SINCE THE WORLD WAR

9. FOREIGN COUNTRIES.--All countries are keeping matters pertaining to their development of codes as secret as possible. Since the war no material is available on the development of codes and ciphers in foreign countries, and very little is available on the subject in this country. Undoubtedly, all countries now realize the importance of secret messages, and are doing everything possible to develop suitable codes and ciphers and to train personnel in their use.

10. UNITED STATES.--The United States has developed a code for training purposes and they have a cipher device which is quite simple to use. Officers and enlisted men who are required to use them are trained in their use by unit instructors. Certain chosen men are given further training in service schools. Picked officers of all branches are trained in cryptanalysis under supervision of the Signal Corps. Without question, the G-2 section of the General Staff is doing cryptanalytic work and is developing additional codes and ciphers to be used in time of war.

## VI. CONCLUSIONS

11. It has been shown how weak were the codes and ciphers used in the past. This weakness was due to the lack of adequate codes and ciphers, and to untrained personnel who handled them. Whether or not the same difficulties will be encountered in the next war will be discovered very soon in the present conflict in Europe.

The importance of cryptanalysis in the development of codes and ciphers has been brought out many times in this essay. It is my belief that there is not enough training in the subject of cryptanalysis. Our civilian schools should teach it. In that way the civilian population would become interested, and many would take up cryptanalysis as a hobby. Then, in time of emergencies, the Army would have more material to select from for cryptographic work and to train their personnel. If more men were trained in cryptanalysis there would be a better understanding of the proper use of codes and ciphers and, consequently, less violations of the rules for their use.

In closing, I will summarize by quoting the words of General Giveirge, head of the cryptographic service of the French Army from 1923 to 1932:

"Cryptograph well or do not cryptograph at all. In transmitting clear text, you give only a piece of information to the enemy, and you know what it is; in cryptographing badly you permit him to read all your correspondence and that of your friends."