This was
talk given
the graduating
at Annapolis
7

In the brief time at my disposal this afternoon, it will be impossible to touch upon all phases of code work. Hence I shall confine myself chiefly to those phases which will probably at some future time concern most of those present; namely, the safeguards and precautions which must be observed in code or cipher operations in order to maintain the secrecy of the system of communication adopted.

A preliminary word of explanation with regard to the two terms "Code" and "Cipher" may be necessary. To most of you, the two words mean practically the same thing, but such is not the case. Modern cryptography draws a rather sharp distinction between the two terms.

A CIPHER, taken in a broad sense, is the name applied to any system of cryptography which involves the transformation of the individual letters of the original, intelligible text of a message into a secret or unintelligible form by means of previously established agreements which subsequently permit of the reconstruction of the original text from the secret text.

The original, intelligible text of the message is called the PLAIN TEXT. The resultant unintelligible or secret text is called the CIPHER TEXT.

The operation of transforming the Plain Text into the equivalent Cipher Text is called Enciphering; the reverse operation is called Deciphering.

A CODE is the name applied to a specialized system of cryptography which involves the transformation of the original, intelligible plain text of a message into a secret or unintelligible form by means of a book or a document which gives conventional words, or uniform, arbitrary combinations or numbers as the equivalents of not only the letters, but also the words, phrases, or entire sentences of the original text. It is obvious that identical copies of the Code or Code book must be in the possession of the correspondents. The operations which apply to this system are called ENCODING and DECODING.

While there are some ciphers which resemble code or tend to approach code, yet the distinction which exists and which should be made between cipher and code is this: in cipher one deals with the individual letters as units; in code, while one may deal occasionally with the individual letters, the operation is

principally concerned with the phrases or sentences taken as units.

When the code designations of the encoded words of a message are afterwards enciphered, of in other words, when a message is first encoded and then the code equivalents are enciphered, the result is called ENCIPHERED CODE. For example, if the code word for the phrase, "By order of the Commander-in-Chief" is POBAL, and if this code word is then enciphered into the form CITAX or into the number 17521, the latter is then known as enciphered code.

So far as I am aware, a system of secret communication which is absolutely impregnable against solution by the enemy and which at the same time is suited to the needs of naval, military, or diplomatic offices, is not known to the science of cryptography. I do not know how sufficiently to impress upon your minds the necessity for exercising the most rigid and painstaking care in the use of the codes or ciphers which may at some future time be entrusted to you. I have seen elaborate code and cipher systems rendered absolutely valueless through the carelessness and ignorance of one man. From the point of view of the Intelligence Department it seems to me that a man who flagrantly disregards or violates the rules and regulations laid down by the Code and Signal Section is as deserving of the extreme punishment for a breach of dicipline resulting in the actual or potential loss of life of his comrades as is the man who consciously betrays them by furnishing information to the enemy. Let me tell you of one instance which to my knowledge had disastrous consequences.

You will recall that in March 1918 the Germans launched their last and greatest offensive on the Western front. Careful preparations and provision had been made for nearly everything. On the day of the opening of the offensive an absolutely new type of code went into effect in every sector simultaneously on the whole front. Months of work by the allied intelligence departmentSupon the German trench code were rendered worthless at one stroke. We had to begin all over again and while the general situation on the whole battle front looked very dark, during those critical weeks, things looked especially dark to the members of the code and cipher section.

Among the very first messages, in the new code that were intercepted by our own Signal Corps was a set of three messages passing between two stations opposite the front held by the American forces. Here they are *

* See page 133 Elements of Cryptanalysis

****

This solution was of vastly greater importance than is apparent on the face of the decoded message. The message itself meant, for us, at least nothing. Even to this day I can only surmise what it meant. But the most important feature

of the message was that it at once gave definite clues with regard to the nature and mechanics of the new system. Certain features of the groups in this message led to the making of some assumptions which were tested upon other messages; they proved to be correct. At one blow the whole new system fell like a house of cards.

I have said that this message meant nothing to us; it may have meant but very little more to the Germans between whom the message was exchanged. But this message led to the breaking of the whole code. Certainly the German operator would not have committed this inexcusable blunder had the message been of great tactical importance. But for the code solver all messages are of equal importance - and most often the messages of least consequence as regards the tactical situation, yield the most far reaching results, and are therefore the most disastrous as far as maintaining the secrecy of the code is concerned. (Practice messages) One of the German radio operators used to send regularly at 6:45 A.M. in code the proverb "Morgenstunde hat Gold im munde" - "the early catches the worm." This gave us lots of clues when a new [illegible] were the rule in German service.

I might add that to complete the dramatic situation resultant upon the solution of this first message, the news, together with the date, was sent to the general head quarters of our allies by special aeroplane because at that time direct telegraphic communication between the American and the other code offices had not yet been established.

How many of his comrades lost their lives as a direct result of this one German's blunder, no one can say. He was guilty of violating one of the most important rules of code work, namely, a message once transmitted in code or cipher must NEVER be repeated in any other form whatsoever.

If it must be repeated because of mutilation or garbles, an exact duplicate of the original code or cipher text must be sent. If after several repetitions the message is still unintelligible, because of a failure on the part of the receiving station to be in possession of the necessary data for decodement, then it may be necessary to transmit the message in another form. Whatever this second form be, it should bear no resemblance whatsoever to the first message as regards internal form of the plain text which has been encoded or enciphered. In other words, the plain text of the original message must be altered in form to the greatest extent possible, consistent with the intent and meaning of the message. This process of altering the plain contents of a message for the purpose of changing its form, without material change in meaning, so that a close comparison between the plain text and its equivalent code or cipher text will be impossible, is called PARAPHRASING. I shall refer to it later. As far as possible no information should ever be given in any

plain text communication, code, or cipher message which may connect it in any way with a message previously sent. Of course, I need hardly add that a message once sent in code or cipher must never be repeated in plain text under any circumstances - there is no exception to this rule. The danger of such a procedure is so obvious that it is hard to conceive of any normal thinking person doing it. Yet, let me tell you of an actual instance.

(Case 2) I can't recall it at the moment.

It seems hardly necessary to say that the insertion of plain text in code or cipher text is so highly dangerous that it should never be done under any circumstances. Of course it is possible that in a long report, only one or two paragraphs might be secret, in which case, the rest of the report could be sent in plain text, providing that the plain text matter will give no clue whatever to the encoded or enciphered matter. However, the best plan of all would be to make them separate. The insertion of any signs, abbreviations, or punctuation should be absolutely prohibited. This would seem obvious but let me tell you of an instance in which the insertion of an abbreviation lead to the solution of a message. (Case 3).

The plain text and code or cipher messages should never appear on the same sheet of paper; in the event of the loss of the papers or their capture, there would be less likelihood of the two being compared. As soon as a message has been encoded or decoded, all the work sheets used in the process must be destroyed by burning in strict accordance with the regulations set forth. A waste basket in a code room is the most dangerous article of furniture in it. Charwomen If it is necessary to keep an exact copy of the plain text, the same should be kept in the coding room and guarded with as much secrecy and care as the code itself. Where a plain text copy of the message must be furnished to departments whose files are not secret, the plain text must be carefully paraphrased.

The work of paraphrasing requires considerable skill and practice, and in the case of matters of very great importance, the paraphrasing should be done or supervised by the higher officers. In all cases the paraphrasing must be done before the message leaves the coding room.

To many of you paraphrasing a message is more or less unfamiliar, and it might be advisable for me to give an illustration. It will do no good to change merely the order of a word or two in each sentence. The entire form of the message must undergo the change. The message should be altered by the substitution of

synonyms, the elaboration of phrases, the change from active to passive voice and vice versa, etc. all of which should be without essential change in the significance of the message. Then the sentences may be shifted about so that the final result bears very little resemblance to the original form of the message. The best way of approaching the task is first to read the message over very carefully in order to get a clear idea of its meaning. Once that is done the principal ideas are to be expressed in a form as different as possible from the original, without material alteration in the intent of the message. (Case 4)

With all these precautions, it hardly seems necessary to remind you that encoded or enciphered messages must never be filed with their equivalent plain text. I have personal knowledge of such an instance.

All the precautions that I have mentioned so far are of a general nature, but I must add one more: NEVER SEND CODE OR CIPHER MESSAGES BY WIRELESS OR BY ANY MEANS SUSCEPTIBLE OR EASY INTERCEPTION WHEN A MORE SECRET MEANS IS AVAILABLE AND WHEN THE MATTER DOES NOT REQUIRE IMMEDIATE ATTENTION. If there are reports upon matters of no particular importance at the moment, they might better be sent by courier or through the regular channels rather than transmitting them by wireless. The reason for this is that the greater the amount of traffic an enemy can intercept, the greater his chances for breaking into the code. Furthermore, the enemy may in certain cases gain valuable information merely from the number of messages sent and their length, without being in a position to read a single one of them. That applies more to military affairs, I suppose, than naval. It may be interesting to you to learn a few facts bearing upon this phase of the question by giving you an instance from the recent war.

(Case 5) The Germans used to send their morning reports in code, in standardized paragraphs, numbered, etc.

I should think that it would be wise to regulate the amount of traffic during an actual state of war so that the enemy can draw no conclusions from the number of messages. In regulating the amount of traffic, routine messages such as daily or weekly reports, especially if they are of set forms, must be sent by other means. They are highly dangerous because of the similarities of contents. There is a method of breaking into a code, called the Analogy Method, which makes use of just such messages.

(Case 6)

The sending of short messages should be avoided because the nature of such messages is rather limited and if they are apt to be very frequent they

constitute favorite points of attack. (Case 7.)

One way to eliminate this danger is to make good use of the dummy groups; but their use must be judicious. (Case 8.)

The use of dummies is to be emphasized, especially in phrases or between words likely to be repeated several times in the same messages or in several messages. They must be employed in the spelling of such words as are not present in the code.

Avoid the use of words and phrases not in the code when other words or phrases with the same significance are present, because it is absolutely necessary to avoid spelling out words or phrases as much as possible. There are no advantages in spelling out such words when it is unnecessary and moreover such procedure opens the way for an attack by the enemy because it has been found that the spelling groups in a code constitute the weakest elements ~~of the code~~. The fewer spelling groups used the more secure will be the code. It may sound far-fetched to you if I tell you that the code man, after a careful study of the text of a considerable number of messages, is able to determine, for the majority of the groups that appear, which ones represent punctuation; which, spelling groups; which, military or naval units, etc. In the case of the spelling groups after a sufficient number of them have been classified as being spelling groups, there is involved only a more or less simple case of substitution cipher. Once a few of the spelling groups have been solved a great break has been made into the code. Remember then, use the spelling groups as little as possible, and when they must be used exercise caution and use your best judgment. (Cases 9 and 10)

Another rule, which seems almost too obvious to mention, is that all operations applying to the system of enciphering, or encoding, must be completed. If there are three operations necessary, it would be highly dangerous to leave off one of them, say the final one. I know of two cases in which an encipherer, either through carelessness or a foolish belief that one operation was sufficient, left off the final operation in enciphering. The results were most disastrous.

After a consideration of the general principles and rules that apply in the preparation of messages, we come to a discussion of some special and detailed features.

I suppose, if I were asked what is the most important of the minor rules with regard to all cryptographic processes, for the purposes of making them secure, I should say that it is the principle of random selection or use of anything pertaining to the system. I do not know how to impress upon you the importance of this

principle. One of the factors which most often led to a first break into the German systems, was the methodicalness of the German mind. The typical German mind is so fascinatedwith the idea of doing everything systemically and in accordance with a set form that everything he does must be done according to system; then when he has once adopted a system he never departs from it unless it is specifically called to his attention. It was his slavish adherence to set forms that most often gave the leading clues. And if he was told that he must vary his procedure, he varied it according to a system!!

I must confess,however, that our own forces were not a great deal better in this respect than the German. Time and again we called attention to the flagrant violations of the rules by men in this regiment or that regiment. But the seriousness of the violations, I am sorry to say, was little appreciated by the superior officers of the men who were guilty. You know how difficult it is to get action on things like this through the usual channels. The men in action think that there are a lot of old fogies back at head quarters, who have nothing to do but amuse themselves getting up a lot of "fool rules and regulations" with which to pester them. They say to themselves "How the devil can the enemy get anything out of a code message that is nothing but a jumble of letters? If this thing were not safe they would not give it to us". It may be that it is pyschologically impossible to make most men realize the seriousness of the hundred and one minute precautions that must be observed, except by actually letting them see how solutions are achieved from the most slender of threads and far fetched clues.

For example, in almost every code for secret communication,alternates or variants for the most frequently used groups are given. I cannot tell you how difficult it is to get operators to use these variants and use them at random. A systematic selection of those variants would be dangerous. For example,at first the German operators had the idea that if a word, or a spelling group, or a punctuation sign occurred several times in a message, the variants were to be used in succession, the first one the first time it was used, the second the second time, etc. Or if the group was only used once in a message, the first variant was to be used. Such a procedure as the latter does not accomplish the purpose for which the variants are intended. (Case 11)

Another source of danger is the repeated use of the same expression, whether it be in the beginning, middle, or end of message. I wonder how many of you realize

the danger involved in such important parts of a message as the address and signature. In cipher work especially, these two parts of a message are always the first to be attacked. Now if, as often happens, messages contain the same addresses and signatures many times, solution is particularly easy in certain forms of ciphers. For example, one of the safest ciphers I know can be solved if one has two ~~even short~~ messages in the same key, even though they're short messages, in which the signature is the same. And recently we solved another cipher, which was heralded, even by other experts, as being absolutely indecipherable by taking advantage of the fact that the addresses of the messages were in cipher too, even though they were all different. It is not so much the fact that addresses or signatures are dangerous as the fact that the beginnings and ends of messages are always weak points. It is just as dangerous, if not more so, to have a more or less set form of beginning messages, such as "Acknowledging your message number so and so" or "Referring to your message number so and so". The only guiding point in such matters can be - avoid all stereotyped expressions and adhere to no regular forms in doing anything in cryptographic work.

The use of punctuation in a code or cypher message, except where the sense would be ambiguous without it, should be avoided. I should say that one of the greatest sources of clues in our work on the German Trench Codes lay in the excessive use of all forms of punctuation by the German operators.

There is one more caution that I might mention. Never give the enemy a chance to make any deductions with respect to the contents of any messages if it can possibly be avoided. Let us suppose for example that the units of a squadron are in maneuvers. A short message followed by a certain maneuver would enable a vigilant enemy to make certain deductions as to the contents of the message which dictated the movement. Similarly a message sent from A to B, followed by a short message from B to A, followed by a repitition of the first message by A would certainly indicate a request for repetition on the part of B. Or a long message sent by A, then a short message from B followed by a repetition of the first message from say the thirtieth group would certainly indicate a statement from B to A to the effect that the message was intelligible from the thirtieth group on. All such clues must be suppressed.

I have referred once before to the dangers of short messages. A short message from A to B followed by a longer message from B to A, say within ten or fifteen minutes, would indicate that possibly "question and answer" had been exchanged between the two stations. By watching these short messages the initial groups are apt to be easily solved

because questions most often begin with interrogatives such as "When" "Where" "How" or verbs such as "Is" "Are" "Have" etc.

Those responsible for the use of code books should regard it as part of their duties to send in to head quarters from time to time a list of words or phrases which are not present in the code and which are used sufficiently to warrant their being incorporated. In this connection I may tell you of the most peculiar anomaly of the German trench code. It had no word for code book. Consequently, every reference to it had to be spelled out. Now it was the regular practice to notify the stations, after a new code book went into effect, to return the old codes. Consequently, in the traffic the first day of the life of a new code one or more messages could always be found instructing the stations to send back the old code books. Since the word Code Book had to be spelled out, the finding and solving of such a message at once enabled us to make a great hole into every new code. If I were asked what word in all the German messages gave the most useful clues to solution, I should say it was this word "Satzbuch". This went on for over two years—all for the lack of a man with sufficient initiative and regard for his duty to inform the proper authorities. (Case 12)

I have told you about some of the things which helped us in our work on the German codes and ciphers used on the battle front, and have hinted at successes. Of our failures, I have told you nothing - and they were many. I am of the opinion and have good reason to suspect, that toward the end of the war the German intelligence department gave special courses of instruction in the use of code and cipher to the operators in charge of transmitting communications. The reason I suspect this is that as time went on the material became increasingly difficult to solve in spite of our continued experience with the material. The enemy evidently came to a realization of the importance of the correct use of their codes and ciphers and the result was that a most rigid discipline in communications came to be enforced. They even had inspectors whose duty it was to go from station to station and correct the errors being committed. One amusing incident in this connection may interest you. (Case 12.)

The idea of having an inspector or a sort of a "Security service" is fundamentally a very excellent one. The security service should be, it seems to me, a branch of the Code and Signal Section, because they are in a better position to realize all the mistakes and pitfalls and the seriousness of violations of the rules and they should also be able to keep a close watch over all the traffic. Such a department might seem superfluous but I believe that in the end it would more than

pay for itself. A poor code in the hands of experts can be used more safely than an excellent code in the hands of careless or ignorant operators. Finally, I might add that no code or cipher system known to me may be said to be "fool proof". Since the secrecy of operations is a fundamental prerequisite to success in warfare, it is hardly necessary to point out that the proper training of the personnel which is to be entrusted with the work of encoding and enciphering, and decoding and deciphering, is one of the most important factors in the realm of military or naval science.