CAUTION: THESE RECORDS WILL BE USED FOR OFFICIAL PURPOSES ONLY, DO NOT REMOVE PAPERS NOR REVEAL CONTENTS TO UNAUTHORIZED PERSON(S)

RECORDS CHARGE-OUT

10201

DATE OF REQUEST	SUSPENSE DATE
25 Jan 61	10 Feb 61

FILE OR SERIAL NUMBER AND SUBJECT

From File of Special Consultant (Friedman)
American Army Field Codes in the American Expeditionary Forces during the First World War.
Serial No. 1007

Confidential

TO

NAME AND EXTENSION OF PERSON REQUESTING FILE	ORGANIZATION, BUILDING AND ROOM NUMBER
Mr. William Friedman LI 6-8520	310 - 2nd Str., S. E., Wash., D. C.

RETURN TO

	DATE RET'ND.	INITIAL HERE
Mrs. Christian, AG-24, NSA, Ft. Geo. G. Meade, Md.		

INSTRUCTIONS

WHEN TRANSFERRING FILE TO ANOTHER PERSON, COMPLETE SELF-ADDRESSED TRANSFER COUPON BELOW, DETACH, STITCH TO BLANK LETTER-SIZE PAPER AND PLACE IN OUT-GOING MAIL SERVICE.

2ND TRANSFER COUPON

10201

TO:

FILE (serial number and subject)

TRANSFERRED TO: (name and extension)

ORGANIZATION, BUILDING, AND ROOM NUMBER

DATE	(sig)	(ext.)

WAR DEPARTMENT
WASHINGTON

AMERICAN ARMY FIELD CODES IN THE AMERICAN EXPEDITIONARY FORCES DURING THE FIRST WORLD WAR

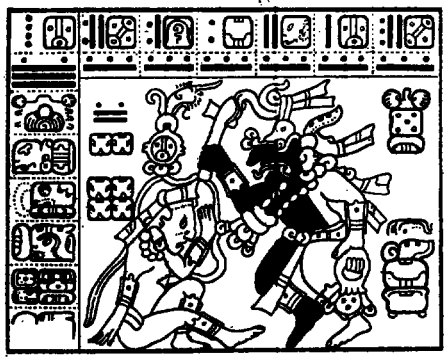
William F. Friedman
Washington
1942

Umol-huun tah-tiyal

William Frederick

yetel

Elizebeth Smith Friedman



Lay ca-huunil kubenbil tech same.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a lo toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

---

30 April 1959

This document is re-graded "CONFIDENTIAL" UP of DOD Directive 5200.1 dated 8 July 1957, and by authority of the Director, National Security Agency.

Paul S. Willard
Paul S. Willard
Colonel, AGC
Adjutant General

WAR DEPARTMENT

WASHINGTON

AMERICAN ARMY FIELD CODES IN THE AMERICAN EXPEDITIONARY FORCES DURING THE FIRST WORLD WAR

By

WILLIAM F. FRIEDMAN

Head Cryptanalyst

SIGNAL INTELLIGENCE SERVICE

OFFICE OF THE CHIEF SIGNAL OFFICER

June 1942

UNITED STATES

GOVERNMENT PRINTING OFFICE

WASHINGTON : 1942

TABLE OF CONTENTS

AMERICAN ARMY FIELD CODES IN THE AMERICAN EXPEDITIONARY FORCES DURING THE FIRST WORLD WAR[1]

1. Introduction

When the first units of the American Expeditionary Forces arrived in France in the summer of 1917, there were available for secret or confidential communication within the AEF but three authorized means: (1) An extensive code for administrative telegraphic correspondence, the 1915 edition of the War Department Telegraph Code, which had been printed for the War Department by a commercial printing firm in Cincinnati, and which while it was fairly well adapted for confidential administrative correspondence, was not at all suited for rapid and efficient tactical correspondence; (2) a cipher system known as the *repeating key system*, which used a simple celluloid device called "the Army Cipher Disk," the basic principles of which were understood and described as far back as the year 1500; and (3) a cipher system called the *Playfair cipher*, which had been frankly copied from the British, who had used it as a field cipher for many years before the World War and continued to use it during that war. In addition to these authorized means there were from time to time current in the AEF apparently several—how many, no one now can tell—unauthorized or locally improvised "codes" of varying degrees of security, mostly nil. Of both authorized and unauthorized means, we shall hear more details in their proper place later on in this paper. Seen in retrospect, when the AEF was first organized it may have been unprepared in respect to means for secret communication in the field, but it is certain that it was no more unprepared than was any other of the belligerents upon their respective entries into the First World War. An inquiry into the causes of this situation does not come within the scope of the present paper, but at this point it will merely be said that never before in the history of warfare had cryptography and secret communication methods played so important a role. When measured by standards of 1940, it must be said that not only was the AEF unprepared as to secret communication means and methods but for a limited time it seemed also almost bereft of hopes of being able to catch up with the times, for their allies, the British and the French, were at first most reluctant to disclose much of their hard-earned information about these vital affairs.

Nevertheless, and despite so inauspicious a commencement, by the time November 1918 and the Armistice came, not only had the AEF caught up with their allies but they had surpassed them in the preparation of sound cryptographic methods, as may be gathered from the fact that the British and French had by then decided to adopt the American system of field codes and methods for their preparation. It is the purpose of this paper to relate some of the important steps in this remarkable progress.

2. Electrical Communications and Cryptography

The great inventions in the field of electrical communications, and especially radio communication, have exercised a profound influence upon the science of cryptography as applied to the military art. Let us see how this situation arose.

[1] This paper was submitted on July 9, 1940, as thesis constituting one of the requirements for promotion to the grade of colonel, Signal Reserve.

Although the necessity for the occasional use of cryptography in military operations has been recognized from time immemorial, it was only in comparatively recent years that the widespread employment of codes and ciphers became a factor of vital importance in warfare. Four primary factors may be recognized as contributing to this situation. In this paper they need only be referred to very briefly.

First of all came the great inventions of the nineteenth century in the art of wire communications, which made it practicable for the first time in history for a single individual effectively to command the innumerable tactical and service elements constituting a large modern army. Such a situation also necessarily calls for adequate signal communication means whereby subordinate commanders can keep in touch with one another as well as exercise control over the movements and operations of their smaller tactical, supply, and service units scattered over an extensive and irregular terrain. Now in a well-developed country, and in the usual defensive situations in friendly territory, wire-communication facilities today may, and usually do, serve adequately in this respect. In this paper we are concerned, however, not so much with the adequacy of such communication facilities as with their safety from enemy surveillance. Although no thoughtful student would consider wire communication so secure against enemy intelligence services that the cryptographing of messages may be considered to be wholly superfluous under all circumstances, nevertheless, for the large majority of such messages exchanged over well-protected wire lines in friendly territory at a sufficient distance from the front to make earth interception impossible or improbable, the additional protection that would be afforded by employing codes and ciphers for these messages is commonly and rightly deemed hardly worth the large amount of labor that would have to be expended in the cryptographing and decryptographing processes. This applies, of course, only to the minor signal communications of supply and replacements; cryptography is still essential for the tactical communications of major strategy, even if well-policed wire routes are employed in friendly territory. The picture changes, however, if these communications must pass over wire routes in occupied enemy territory, where enemy agents or sympathizers may well be in a position to tap the lines or copy the signals by one means or another. Cryptography then becomes advisable, and in many cases essential, especially when consideration is given to the modern means for electrical interception by inductive methods.

The second factor which led to the increased use of cryptography in military operations involves a consideration of the results of the many inventions involved in the development of modern transport facilities based upon the steam and gas engines, for the latter, for the first time in history, made the rapid shifting of forces and, particularly, the remarkable mobility of modern high-power weapons practicable of accomplishment on a large scale. The mobility of men and artillery is in fact so striking today that it is obvious that even our most modern facilities for the establishment of wire routes can hardly keep pace with the speed with which movements of whole divisions and their fire equipment may be effected. Especially is this true in a rapid advance, when maintaining wire communication becomes extremely difficult. In fact, as armies grew larger and transportation facilities improved, it soon became apparent that either new and much more rapid means of laying wire would have to be devised to keep pace with this mobility or else some new means not requiring wire would have to be invented.

This need had hardly become apparent before it was met with the third of the factors mentioned above; namely, the invention of radio communication and its speedy adoption in the military art. Now, although it can hardly be said that all commanders from the very earliest days of this application of radio to the military science recognized one of the most important of 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 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 employment of cryptography that this science had ever experienced.

There was perhaps another factor which should be mentioned in this connection, and that is that the excessive demands for wire in a war of extensive movement made a heavy drain upon the resources of some of the belligerents, such as Germany and France, so that radio, as a means of communication in which this drain was no longer felt, was most welcome.

The last of the factors alluded to above may almost be regarded as a concomitant of the second, since its existence was also dependent upon the invention and development of the gasoline engine. It was the invention and development of aircraft and the speedy adaptation of aircraft to military operations. This introduced not alone the factor of mobility but also the factor that wire communication between aircraft or between aircraft and ground stations is manifestly impossible, so that radio naturally became the most practicable means of such communication. This, of course, had been true for about a decade, as regards communication between ships at sea and between ship and shore stations.

A very brief résumé of the early history of the use of radio in military operations may not be amiss. In his very interesting article entitled "The Powers and Limitations of Radio Communication Within a Modern Field Army," [2] Maj. Richard B. Moran, Signal Corps, gives a succinct summary which is quoted in full below:

> Radio was not put to any practical military use in the field prior to the World War, although some experiments were made involving the use of radio by the British in the Boer War in South Africa in 1899. Since 1906 the principal armies of the world have had some radio equipment. The first field radio equipment made its appearance in our army in 1903 and was used in maneuvers held in Kentucky under General Bates.
>
> Radio was early recognized as a valuable means of signal communication for forces whose movements were rapid. The British entered the World War with radio provided in a meager manner for independent cavalry. The increase in the use of radio during the World War as a means of signal communication continued throughout its length, as is ably demonstrated by Priestly's account of the British Signal Service, Carlsward's description of the German Signal Service, and the report of the Chief Signal Officer, United States Army, 1919. Its value is shown not only to cavalry but to aviation, artillery, tanks, and forward infantry units.
>
> One of the first uses to which radio was put was that of providing communication between airplanes in flight and ground stations. While radio was early employed for this purpose, other means, such as dropped messages and visual, seemed to be preferred both in the British and American services. There was one type of operation, however, which required the use of radio, that was "spotting" for artillery. Prior to the Aisne offensive in the fall of 1914 spotting for artillery by observation aviation was unknown in the British service. On October 1, 1914, the first experiment in spotting was conducted, using radio for communication, with conspicuous success.

The following extract from the same article is also worth quoting.

> One of the outstanding characteristics of radio transmission is that waves radiated at the transmitter travel in all directions. The extent of travel in all directions is not the same but, except in the case of ultrahigh frequencies, this fact may be neglected in military sets since they are designed to transmit over a minimum distance in any direction.
>
> This characteristic is both advantageous and disadvantageous. The advantage is that communication can be established quickly between stations without orientation and usually regardless of intervening terrain. It has the important disadvantage that enemy receivers located within range of friendly transmitters may pick up any transmission and make use of information thus obtained. * * * Since the enemy may and will intercept radio messages, they must be sent and received, and the information they contain utilized before the enemy can make use of it. The use of codes and ciphers increase the delay to the enemy although their use consumes time in the transmission of messages.
>
> It has, therefore, become the policy of all nations to encode or encipher all radio messages containing information of value to the enemy, and to send in clear only messages which, if intercepted by an enemy, will be of no value to him. The idea must not be gained that encoded or enciphered messages cannot be read by the enemy. They can. The advantage of cryptographed messages is that they force the enemy to consume time in securing the information he seeks.[3]

[2] The Signal Corps Bulletin, Nos. 91 and 92, 1936. The first extract is quoted from page 34, the second from page 33 of Bulletin No. 91.

[3] Annual Report of the Chief Signal Officer, 1919, p. 216.

When the United States entered the war on April 6, 1917, field radio was by no means a novelty in the United States Army, for the radio activities of the Signal Corps dated from 1903, and several years prior to 1917 a Signal Corps radio laboratory had been established at the Bureau of Standards, in Washington. The Signal Corps had kept abreast of progress in the new art, and in some respects had been in advance of others. Small portable field sets had been developed, and in 1912 small high-frequency (then 500-cycle!) pack sets had been placed in service. A number of these sets were in operation on the Mexican border at the time of the Villa affair, and communication was maintained in some cases with stations over a distance of 200 miles.

Soon after the first units of the AEF reached France, a radio division was established in the office of the Chief Signal Officer, AEF. With increasing knowledge of the methods of the French and the British, and with the increasing size of the American forces in Europe, the field of activity of the initially small radio division greatly expanded. Radio communication within the AEF was soon practically continuous but—remarkable to relate—it was seldom used! To telephone was the American way, and thus arose the story which will always be history in Signal Corps circles—that concerning the message from a brigade commander to division, by radio, saying "I am absolutely out of all communication" when only his telephone lines had been shot out.[4] Nevertheless, there was sufficient radio communication within the AEF to make cryptography a necessary adjunct to correspondence by this agency.

3. Ciphers, Cipher Systems, and Cipher Devices in the AEF

Coming now directly to the subject of the present paper, cryptography in the AEF embraced all forms: Ciphers, cipher devices, codes, and enciphered codes. We shall take these up in turn.

A detailed discussion of the cipher systems employed by the AEF will not detain us very long. The only cipher device (if it may properly be called a device) which was known to the AEF was the simple United States Army Cipher Disk, a photograph of which is shown as appendix 1. It had been in use a good many years in various field exercises in which units of the United States Army engaged at irregular and infrequent intervals. The 1916 Signal Book of the United States Army gives instructions for the use of the cipher disk, and these apply clearly to the simple form of repeating-key or multiple-alphabet system, using quite short keywords. The origins of this system can be traced back several hundred years; by 1916 it was certainly unworthy of use in serious military operations, for not only is it extremely slow in operation but also it presents hardly any security worth mention. The records of the AEF show that this system was certainly studied and taught at the Army Signal School (see appendix 2), but I have been unable to find any evidence that the system was actually employed for the exchange of official messages in the AEF. This surely is a gratifying finding.

The only other cipher system that was taught at the Army Signal School in the AEF was the so-called Playfair cipher. The appendix last referred to also describes this system. The fact that it was actually used for secret communication is proved by the exhibit contained in appendix 3, which was found by me among some miscellaneous records of the World War. The British used the Playfair cipher, too, but with some modifications which consisted largely in a greater disarrangement of the letters within the square than can be obtained by merely inscribing a key-word mixed sequence in normal fashion within the square. Even with such modifications the Playfair system presents very little security. How widely the various tactical units of the AEF used the Playfair system is not known to me, but it could not have been extensive, for by the time that the AEF grew to any appreciable size or engaged in any important operations the various field codes devised, prepared, and issued by the Signal Corps, AEF, were available and were probably given preference over the Playfair cipher. It is, therefore, desirable to enter at once into a discussion of these important codes, their origin, development, and usage.

[4] Ibid, p. 448.

4. The Origin and Development of Field Codes During the World War

Although it is well known that long before 1914 the use of code and even of enciphered code was by no means a novelty in the armies of the various belligerents, including the United States Army, code systems were restricted in their employment to communications exchanged among only the highest headquarters and headquarters staffs. Practical military cryptographers of those days maintained, for reasons which may seem obscure or perhaps incomprehensible to military cryptographers of today, that code books would be entirely impractical for tactical operations in the field and hence it would be useless to try them out in the field. It is pertinent to this paper to inquire into the reasons for such an attitude.

It must be emphasized that the adoption of a code system for field use entails certain disadvantages of no small importance. First of all comes the question of production and reproduction of the books themselves. Then comes that of the proper distribution of the copies which must be issued to many and perhaps widely scattered organizations, and this alone constitutes a problem of no mean proportions when a large army is in the field. Finally comes the matter of the proper safeguarding and accounting of these copies, for it is obvious that the capture, theft, or loss of a single copy is sufficient to compromise the entire edition and necessitates an immediate replacement. Each of these questions will be examined in turn. It may be that the early objections to the use of code in tactical operations are still of serious nature and are not to be overlooked even today.

First let us consider the matter of the production and reproduction of codes by field forces and under field conditions. If the question were merely one that could be disposed of for good, once an edition of the requisite number of copies had been produced, there would obviously be no difficulty. By this is meant, of course, that under such a system a single edition of the code would be all that would be required and once copies were in the hands of troops only such additional copies would have to be issued as were necessary to meet the needs for replacement due to ordinary wear and tear.

Now it is obvious that the degree of cryptographic security that would be afforded by such a code would be almost negligible after a short time. This would of course be true whether the code were of the one-part or two-part type. For if it were of the former type, solution could be achieved rather readily; if it were of the latter type, solution would require more time and traffic, but once accomplished both types remain on an equal footing. And of course the danger of capture, theft, or loss is as great in one case as in the other.

Now if the security afforded by such codes is to be sufficient to make the trouble that their use involves at all worth while, it becomes obvious that in the case of a one-part code it is essential to resort to superencipherment; that is, apply a cipher system to the code text of the messages. In the case of a two-part code it is essential to adopt a system of more or less periodic replacement of editions, dependent upon such factors as volume of traffic, loss by capture or theft, etc. Let us consider each of these alternatives from a technical and practical viewpoint.

At best, plain or unenciphered code is a rather slow means of cryptographic concealment of the intelligible text of a message. To superimpose a cipher system upon this simple structure seems easy enough. But when a simple and rapid encipherment is employed, the additional security afforded is usually quite illusory; and when a complex encipherment is employed, the process becomes hopelessly slow and too intricate for successful application by the average military code clerk in the field. Superencipherment of a complex nature may be practical and satisfactory for employment at large, fixed headquarters or offices where speed is not vital or where the work can be parceled out among the various members of a numerous personnel in case rapidity in cryptographic operation constitutes a very important factor. But in tactical operations in the field, speedy communication is vital and anything which acts as a brake upon speed,

such as the necessity for cryptographing and decryptographing these communications, is usually tolerated by commanders in the field only after urgent insistence from higher headquarters upon such necessity. Even then there seem to be occasions when the rules must be disregarded. Hence, it follows that a cryptographic system using a one-part code with a complex superencipherment is hardly practical for field use. It did not take the Signal Corps in the AEF a long time to reach this conclusion, as will presently be shown by presenting the facts attendant upon certain experiments which were made very soon after the Signal Corps Code Compilation Section at GHQ was organized.

There remained to be tried the system using a two-part code without superencipherment, which involves the problem of production and distribution of replacement editions upon a more or less regular schedule. This was finally the solution adopted by the Signal Corps, and we shall soon see how well it worked. But at this point it may merely be said that it is well to remember that it is only in comparatively recent times that technical or rather mechanical advances in the art of printing, and the science of electric-power production and distribution have made the printing of codes in the field a practical matter. For instance, it would not have been practicable in our Civil War to generate electric power in the field for printing presses. Furthermore, neither the linotype nor monotype machine was available in those days.

So much for the theoretical considerations which should alone have led directly to the solution that was ultimately adopted by all the belligerents. But theoretical considerations are not enough, and "hindsight" is usually easier than "foresight." Let us see how this solution was attained in actual practice. This will involve a brief examination into the history of the field codes used by the French, British, and German Armies during the World War, before the AEF appeared upon the scene in any considerable numbers.

Some attention was given above to the factors which led to the introduction of radio communication in military operations. The progress in this art was rather slow until the invention of the vacuum tube, which came a very short time before the outbreak of the World War. But a great step forward was made after this important invention. Suffice it to say that by 1916 radio communication with radio sets employing thermionic valves was well established and in common use by all the belligerents on all fronts. Now the possibilities and consequences of enemy interception of the radio messages were more or less well recognized by most of the belligerents before our entry in the World War, and it will be interesting to recall the authoritative though brief account of the effects of the recognition of the dangers attendant upon the use of radio, given by Col. Marcel Givierge in an important article which appeared in the June and July 1924 issues of the *Revue Militaire Française*, a translation of which was published in the Signal Corps Bulletin: [5]

However, a new element was to make its appearance in the cryptographic war. It was a consequence of the development of wireless telegraphy in the front-line units. We mean the code notebooks.[6]

Those notebooks were introduced with us to facilitate secrecy of telephonic communications. It had taken a long time, despite the cautions of experts, to comprehend that the telephone was not a safe means of communication; but after a few cruel experiences, in which it was evident that the enemy had been advised of a relief or a surprise attack by an intercepted telephone message, a means was sought to conceal the meaning of the messages. There had been placed in service in our Army, for the sole purpose of permitting the encoding of important words in telephone messages, leaflets containing in essence tables serving to replace letters by groups of two figures, by selecting now one table and now another. These notebooks showed for 50 common expressions the way to encode them in a single group of three figures. When the communications by wireless telegraphy between small units developed, the use of these notebooks was authorized, by way of exception, to add to the signals which the posts were to employ—as a rule, a few encoded expressions. There was developed later the table of words in addition to the tables for encoding by letter. Then the idea of making this notebook a document for encoding, especially letter by letter, was abandoned, and it was made into a small dictionary of words and syllables. For the large

[5] See Nos. 33 and 34, March and May 1926.

[6] The original French reads "carnets de chiffre," literally, "cipher notebooks." These are merely short lists of code equivalents for letters, syllables, and a few common words.

units, documents more voluminous than the notebook designed for troop units were prepared, and they were called codes. Both of them, at the end of the war, were based on the same principle as the code book of the general staffs but on a smaller scale.

With the Germans, a similar evolution had been seen. The small units had at first used encoding tables, in which the most usual sentences were represented by groups of letters or figures. Some of these, *Befehlstafel* (command tables) or *Geheimtafel* (secret tables), were captured in surprise attacks. In order to modify the encoding work, certain of these tables were of a circular form, the words to be encoded being written on the radii, at uniform distances from each other, of a large circle, while the groups were on the radius of a small concentric circle. The latter was movable, and by changing the position of it the correspondence of the groups to the words was varied. Others of the documents were in the form of a notebook with variable pagination. Then, without these transformations succeeding each other according to a precise chronological order, our enemies adopted notebooks nearly similar to ours. Was this merely one example among many which might be found in the history of cryptography, a science in which each guards his secrets, of those "ideas which are in the air"? Was it the result of information given by documents found on the field? It matters little, in any case, in June 1917 the system had become general.

Let us take careful note of what this authority says of the earliest *carnets de chiffre* or code notebooks. Givierge states that the first ones were (1) intended solely for use in telephone communication; (2) they had "tables serving to replace letters by two-figure groups, by selecting now one table and now another"—in other words, a sort of polyalphabetic scheme of encipherment; and (3) they also had 50 common phrases which were representable by three-figure groups. Then later, when radio communication between small units developed, and "the use of these notebooks was authorized, by way of exception," a few expressions were added to the signals which the posts were to employ. "There was developed later the table of words in addition to the tables for encoding by letter. Then the idea of making this notebook a document for encoding, especially letter by letter, was abandoned, and it was made into a small code of words and syllables."

Let us devote a few moments to a consideration of these early codes. The writer is fortunate in possessing in his personal collection of cryptographic items examples of some of the French codes of this early period. Appendix 4 shows a photostatic copy of a page of one of these early French codes. It is, to be sure, not one of the first of the type to which the French applied the name *carnet réduit*, but it well illustrates the principles upon which it was based.

It will be noted that it was to be used by telephone, earth telegraphy, radio telegraphy, and visual telegraphy. It had a name "Olive," to be used as a signal in telephone conversations, and an *indicator* "O.O.O." (the initial letter of that name given three times) to be used as a signal when this code was used in telegraphic communication. It was not strictly a one-part code, since there was a division into several sections: Alphabet, numbers, verbs, verb tenses, measures, orientation, place indications, infantry, artillery, common words, and phrases. It will be noted, however, that the three-letter code equivalents, while in strict alphabetic order, show breaks in sequence. For example, the first group is not AAA but AIC, followed by AKE, then AKI, ALB, etc. These skips in sequence were intentionally quite irregular, the purpose being threefold, as discussed below.

First a somewhat greater degree of security than would be the case if there were no breaks is provided by such an arrangement, since enemy cryptanalysts are not in a position to know approximately how many groups intervene between any two which had actually appeared in the traffic. For example, suppose that the groups AKE and AKI have appeared in the traffic. If an unbroken alphabetic sequence of code equivalents were the basic principle, then the cryptanalyst would know that there must be three groups intervening between these two groups, and this would have an important influence upon his assumptions for the probable meaning of AKE and AKI. But where there are breaks in the sequence he is not in so good a position to make these assumptions. The more irregular the number and extent of these breaks in alphabetic sequence are, the harder it becomes to make these assumptions. But of course the difficulties in this respect

hardly begin to approach those encountered in the true two-part code, where the principle of parallelism in progression between code equivalents and plain-text elements no longer obtains even to the slightest degree.

The second purpose of having breaks in alphabetic sequence of code equivalents is that it affords opportunity for the preparation and issue of a new edition after an earlier one has been in use for so long a time as to have been solved or has been captured or otherwise compromised. The new edition may employ new code groups with a different arrangement of breaks in alphabetic sequence so that any information the enemy cryptanalysts may have derived from the preceding edition will be valueless.

The third purpose of having breaks in alphabetic sequence of code equivalents is that it permits of the simultaneous use of several editions of the basic code by organizations fighting upon different fronts or in different sectors of the same front, since the skips in one edition may be quite different from those in another.

The writer is unable to state how long the French continued to use this type of one-part code. It is quite clear from what Givierge says about the way in which codes came to be employed by the French Army that the success which attended these earliest codes soon led to their increase in size and to their widespread use, for he says: "For large units, documents more voluminous than the notebook designed for troop units were prepared, and they were called codes." It is important for us to note also his statement that "both of them (i. e., the *carnets de chiffre* and the *codes*) at the end of the war were based on the same principle as the code book of the general staffs but on a smaller scale." By this he can only mean that the principle of the one-part code was abandoned in favor of that of the two-part code. This conclusion is corroborated by two exhibits in the writer's possession. One of them is the carnet "Urbain," a true two-part code notebook of about the same number of words and phrases as the carnet "Olive," but in which the sequence of code equivalents no longer presents a parallelism with the alphabetic order of the plain-text elements. (See appendix 5.) The other exhibit is a much more extensive two-part French field code of approximately 2,300 groups. (See appendix 6.) This code also provided for a method of superencipherment, but how much this was used is unknown to me. A copy of an enciphering table is shown in appendix 7.

So much for the French field codes.

A few words must be added concerning the field codes of the German and the British Armies. For a good account of the cryptographic systems used by the German Army from the outbreak of the war until the time that field codes had been developed by that Army, the reader is referred to the interesting brochure of Yves Gyldén, a translation of which appeared in seven successive installments in the Signal Corps Bulletin beginning with the November–December 1933 issue. Suffice here to indicate that they employed several different types of systems, including simple substitution, simple columnar transposition, combined substitution-transposition, double transposition, and polyalphabetic systems of a rather complex nature. Of these, only two were really practical and successfully employed for any length of time: (1) A double transposition cipher system, and (2) a cipher system using only the letters ADFGVX in the cryptographic text and therefore called the ADFGVX cipher system. But these were reserved for use in communications between only the highest headquarters and a detailed discussion of them falls outside the scope of this paper. As for the other systems, we may summarize them by quoting from Gyldén:

> The German systems employed during the first few months of the World War were particularly impractical. * * * This explains the uncommonly great proportion of repeated telegrams and the unnaturally long delays mentioned above. * * * The systems were far too difficult to handle by radio personnel not especially trained in that line; they were likewise far too time-consuming for practical purposes and useless when there was interference. * * * As a rule, the correspondence was in cipher. However, frequently names in clear text occurred, as well as words and even whole sentences which had not been understood by the person for whom the (original) message was intended. * * * Still more important was this telegraphing in clear

text because of the fact that it accustomed the French cryptanalytic experts to the ordinary telegraphic style used by the Germans and to their ordinary abbreviations, as well as to the nulls which they interpolated in their messages [7].

In appendix 8 is shown a sample page of each of three German field codes. It will be seen there that the general vocabulary of the *Schlüsselheft* was a simple one-part code, whereas the *Satzbuch* was a true two-part code. The former was enciphered by a cipher key called the *Geheimklappe* which changed about every 7 to 10 days. It will be seen that this system was very similar to the very first field code which was produced by the AEF but which was hardly used before it was superseded by the excellent two-part "Potomac" code, which was similar to the German *Satzbuch* and required no encipherment.

As for the British field codes, I am unfortunately able to offer very little information. So far as I am aware, they adhered throughout the war to their peculiar type of code called technically a *caption code*, in which the contents are subdivided into headings or captions such as "punctuation," "common words and phrases," "attack," "bombing and bombing attack," etc. Under each caption there were several items to each of which was assigned a three-figure code group. *The code groups were in serial order* except in two particulars: A very few breaks were introduced in sequence, probably to allow for additional insertions, and the code groups assigned to the 26 individual letters of the alphabet (for a spelling table) were in random order. Obviously, superencipherment must have been used. A few pages in appendix 9 give a good idea of what this code was like.

5. The Preparation of Field Codes by the AEF

The following extracts are taken from the official Report of the Code Compilation Section of the AEF, prepared by Maj. Howard R. Barnes, the officer in charge of that Section from the time of its organization in December 1917 until its demobilization shortly after the Armistice in November 1918:

> It must be borne in mind that at the commencement of the war no permanent experienced organization existed in the American Army either for the building up or the breaking down of codes.
>
> * * * * * * *
>
> When the Code Compilation Section was organized in December 1917, it consisted of a captain, three second lieutenants, and one corporal. These men were assigned to duty at General Headquarters, American Expeditionary Forces, and began the task of compiling codes for the Army in the field.
>
> The data on the subject of codes was most limited in scope. Previous to this war the United States Army had never had a code book, properly so called, for field service, and had had recourse to the cipher disk or short-lived emergency codes. Moreover, the Army was confronted with a foe who had profited not only by their own experiences of 3 years but the mistakes of the Allies which they had observed through their interception of wireless messages and the information gained from captured code books. At first the British and French were rather reluctant to disclose the systems which they had adopted for their codes, but eventually copies of obsolete editions were turned over to this Section for reference and study. With this meager data the compilation of a front-line code was begun. The fundamental principle upon which the books were founded was a complexity sufficient to delay solution with a simplicity sufficient to afford ease of operation.
>
> The first American Trench Code, a small book consisting of some 1,600 words and phrases, was intended for distribution down to and including companies actually in line. Accompanying it were certain tables containing a distorted alphabet. It was proposed to change these tables at frequent intervals and thus delay the solution of intercepted messages. This Trench Code was never in fact actually delivered to the front line, and went no farther down than regimental headquarters because of the danger of capture. An edition of 1,000 was printed. This book was about 4½ by 7 inches and could easily be slipped into a breast pocket. The three-letter group system was adopted with an alternative four-number series. [See appendix 11.—*W. F. F.*]
>
> * * * * * * *
>
> To provide for the needs of the firing line, a smaller code book was prepared for emergency use and issued down to companies. This code contained about 500 carefully selected words and phrases. Before compilation,

[7] Signal Corps Bulletin, No. 77, p. 47.

an officer of this Section spent some time at the front in an effort to obtain some first-hand information as to the specific needs of the front line.

An edition of 3,000 copies was issued.

This code book, known as the "Front Line Code," was about 3 by 6 inches and could be carried in an inner pocket. Two-letter groups were assigned to each word and phrase arranged alphabetically beginning with AB and ending with ZZ. A few blanks were left at the end for emergency use. [See appendix 19A.—*W. F. F.*]

In this book were inserted a number of "nulls" by the use of the parenthetical phrase, "This group means nothing."

To facilitate operation in the use of the two codes it was so arranged that the same distortion cards could be used with the Front Line and Trench Codes. [See appendices 12 and 19B.—*W. F. F.*]

Major Barnes summed up the experimental work that was done on these first two field codes in the following words:

Before these codes had become widely distributed or much used, it was seen that the effort to provide a quick-operating, simple code had proved a failure by reason of its very simplicity.

He does not give the details of how this failure was established but the writer is fortunately in a position to supply some of the elements lacking to complete the story of these two early attempts to produce a satisfactory field code.

Major Barnes does not indicate exactly how long this first Trench Code was used. He merely says "before these codes had become widely distributed or much used." For reasons which will soon become apparent it seems clear that at most, this period could not have exceeded a couple of months, and there is even reason to believe that this type of code was never actually used except for training purposes.

In collecting the data for this paper the writer encountered in the World War files references to a report, dated May 17, 1918, in which a series of 44 messages prepared by means of this first Trench Code and its "distortion alphabet" formed the subject of a study of security.

The report referred to of course became the object of a search and was readily found. It is of considerable interest in connection with this study. It was written by First Lt. J. Rives Childs, a member of a section of G–2 of GHQ known as the Enemy Code Solving Section, G2–A6 being its abbreviated designation. Code compilation, however, was a function of the Signal Corps under the Chief Signal Officer, AEF, and a section for this purpose was in existence. It would appear then that either G–2 directed that a test of the first Trench Code be made or the Chief Signal Officer of the AEF initiated such a project and called upon G–2 to make the test. In any case, the test seems to have been a highly successful one from the standpoint of demonstrating the weaknesses of this first code and its enciphering system, for it led to their quick abandonment. This report is so interesting a document in itself that it is included in toto herein as appendix 10.

There is another reason for including this report in its entirety. In a book [8] which, in most libraries, is undoubtedly cataloged under the class of nonfiction and which seems to bear the stamp of authenticity because of the official position held at one time by its author, there appears an allegedly factual account of the codes and ciphers employed by the AEF. Attention will be confined only to those portions of that account which are pertinent to this paper, viz, those dealing with the alleged work of a "young officer who without any knowledge of the American method of encipherment * * * solved within a few hours" a series of extremely important messages which had actually been transmitted within the American sector. The following is a verbatim quotation of the paragraphs of interest (they have been numbered below for purposes of reference):

(1) The compilation of codes and ciphers was, by general orders, a Signal Corps function, but the war revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer of the Signal Corps who had just been appointed a military attaché to an allied country.

[8] Yardley, H. O. The American Black Chamber, Bobbs-Merrill, Indianapolis, 1931.

It was not intended that attachés should actually encode and decode their own telegrams, but as part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.

(2) When the new attaché, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communication. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which as children we read in Poe's The Gold Bug.

(3) He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard of going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it."

(4) He outranked me greatly or I might have added that we were not at war with medieval Spain but with twentieth-century Germany, who had gathered the brains of her empire behind the greatest war machine the world had ever seen.

(5) Amazing as it may seem, his attitude was characteristic, even at the front. One of the young officers whom we had trained confirmed this when he arrived at General Headquarters in France. He had received his instruction and practical experience in my Bureau. Having observed the necessity for revising the War Department's communications in this country, he was eager to learn whether the codes and ciphers of General Pershing in use at the front were safe.

(6) The first thing which this young officer did after arriving in France was to induce his superiors to intercept by wireless our own radio code and cipher messages along the American sector. These codes and ciphers were used to transmit the most secret and important messages and by those who employed them they were considered safe.

(7) Without any knowledge of the American method of encipherment, the young officer solved these messages within a few hours. The system was wholly inadequate and as a means of insuring secrecy was little more than a farce.

(8) Through decipherments of German intercepted cipher messages, our Cipher Bureau in France knew that the enemy maintained a large staff of skilled cryptographers. All radio messages of the Allies and of the Americans were intercepted and sent to the German Cipher Bureau for attack. If this young American officer, who was still merely a student cryptographer, could solve these messages, the German crytographers, with their long experience of code and cipher solution, without question had also solved and read these telegrams even more quickly than he. And once the system was broken, the enemy could solve every message as easily as the person to whom it was addressed.

(9) As it happened, the contents of this particular decipherment were so important and their secrecy so imperative that the young officer's memorandum on the matter threw the General Staff into a panic of confusion. From these wireless intercepts he learned the disposition of troops along the St. Mihiel salient, the number and names of our divisions, and, finally, the actual hour at which the great American offensive would be launched. This, then, the enemy knew!

(10) The herculean effort of flattening out the salient, which for 4 years had formed a huge "pocket" inside the French lines, cutting off communication and stopping railways between Verdun and Toul, was the task of the Americans. And by reading the intercepts, the Germans had already learned in detail, just as easily as this young officer had learned, plans and preparations for the great American offensive. Incredible! No wonder the General Staff was in a panic. In these messages were contained some of the most important stratagems of the World War.

(11) The Germans considered their position in the salient impregnable. General Pershing knew that the enemy had several lines of defense, the second known as the Schroeter Zone, another as the Hindenburg Line or Kriemhilde Position. What was to happen to the great American offensive of 1918 if the enemy was prepared for it? Or, if the defenses were not considered strong enough now to meet the offensive, was the enemy, warned by our messages, withdrawing?

(12) The latter was the case. Our young officer had shown the General Staff the leak in the offensive, but it was too late to swoop down upon the Germans in a surprise attack. The messages were already in their possession and a retreat had begun. The American offensive of September 12, 1918, was considered a triumph, but it represents only a small part of what might have been a tremendous story in the annals of warfare had the Germans not been forewarned. The stubborn trust placed in inadequate code and cipher systems had taken its toll at the front. The enemy had actually been taken into American confidence, through the nonsecrecy of communications. It was not a surprise attack which was achieved. Pershing pursued an already retreating horde and entered St. Mihiel on September 13. The salient was broken, but the surprise attack never came

to pass. Too many staff officers in France had, like our authorities in Washington, placed a childish unfounded trust in any encipherment which could not be read at sight.

The author does not name this "young officer" but he need not be nameless, for he was beyond all doubt the author of the report referred to above, First Lt. J. Rives Childs, who was indeed a member of the Code Solving Section (G2–A6) GHQ–AEF. It was certainly not within this young officer's province to be "eager to learn whether the codes and ciphers of General Pershing in use at the front were safe" but we may assume that he was not merely presumptuous and that perhaps he did express such a desire. At any rate, the official records show that he was assigned such a project; and since only one report on the subject was found in the files of the World War, it seems certain that the "young officer" was Lieutenant Childs.

Let us now analyze the paragraphs quoted from the Yardley book in the light of the Childs report and the facts which are established by studying that report.

First of all, the messages which Childs used were one and all test messages which had been prepared for the specific purpose. *Not a single one of them had been actually transmitted. There was no interception whatever involved in the matter.*

Secondly, Childs not only *had* a complete "knowledge of the American method of encipherment" but was given a copy of the code used, for let it be noted that strictly speaking this officer was given, not a complex problem in enciphered code, but a simple problem involving the solution of a single mixed alphabet. This statement is based upon evidence in the report itself, for no other conclusion can be drawn from several remarks contained in it, such as the following [the numbers at the side refer to the correspondingly numbered paragraphs in appendix 10]:

(3) The solution of the cipher alphabet * * *
(5) Reference was had to the book and the result * * * was confirmed.
(6) These results were than checked up by means of the code book, and confirmed.
(6) If the verb "work" is encoded on page 35. [The copy of the code book in possession of the writer (one of the valuable souvenirs of his participation in World War I) shows the word "work" on page 35. (See appendix 11.) Childs could certainly not have been aware of this fact unless he had a copy of the code.]
(9) What letter was there in the code whose initial and final letters were the same? There was only one, "H"; we were not even under the necessity of trying and fitting from among several. [Childs would certainly not have been able to make such a statement had he not had the code.]
(12) Suppose we turn to pages 14 and 15 of the code book. * * * [Several references of similar import occur in this same paragraph.]
(13) And again, it might be further added that the fact that there exist no blind groups or nulls anywhere in the code * * *

It is believed that these references beyond all question establish the fact that Childs was given a copy of the code, told what the encipherment system was (or given an exemplar of the enciphering card similar to that shown in appendix 12) and asked merely to solve the single mixed alphabet involved. This was a particularly easy problem even in those days, as it would be today. *Had Childs been given nothing but the 44 messages*, the story would have been quite different; he might have reached a solution of the alphabet, and have read some of the messages in part, but the problem would have taken a good many days, perhaps 10 days instead of only 10 hours.

Obviously, from the foregoing facts Yardley's story collapses like a house of cards. Other evidence is hardly needed, but attention may be called to one other misstatement of fact which is glaringly patent: The Childs report is dated May 17, 1918, and Yardley talks about the reduction of the St. Mihiel salient, which did not begin until September.

Yardley completes his account with the following statements:

In a history of the World War, one reads the story of this amazed young officer, in some short uninformative generalization. He knew that the code and cipher systems were inadequate; but all he could do was reveal his findings and give warning to the General Staff. The story of his revelation is one which, like many others enacted

behind a curtain of warfare, is seldom told. It was too late to undo the damage after the young officer had revealed the inadequacy of the codes and ciphers.

* * * * * * *

The Signal Corps in France was using inexpert and ineffective codes and ciphers to carry over the wireless the secret orders of the General Staff in France.

How far from the truth these statements are can easily be shown. As soon as it became clear that the first Trench Code and its simple encipherment scheme did not afford adequate security the whole system and the code were discarded. It was then, in the words of the Barnes report, that—

a code constructed upon the "chance" plan, provided with encoding and decoding sections was adopted, * * * and * * * in June 1918 the first issue of the new series was published and 2,000 copies were turned over to G–2 for distribution.

Of this and the succeeding codes more will be given presently, but before leaving the subject of the Childs report one more remark must be made. When the important statement of Major Barnes—the one to the effect that "before these codes had become widely distributed or much used, it was seen that the effort to provide a quick-operating, simple code had proved a failure by reason of its very simplicity"—is weighed in the light of the evidence, it must be admitted that the reason he assigns for the withdrawal of these two early codes is hardly an adequate one. For from the point of view of providing "a quick-operating, simple code" any two-part code without encipherment is certainly to be preferred over a one-part code which must be enciphered, since in the case of a two-part code (as regards both outgoing or incoming messages) there is only operation, and this step is exactly the same as in the case of a one-part code; whereas in the case of a one-part code with encipherment, an incoming message must first be deciphered and then decoded, an outgoing message must first be encoded and then enciphered. So Major Barnes' reason for the withdrawal of these two codes hardly tells the complete story. Of course, from the point of view of code compilation there is no question as to which of the two systems (one-part superenciphered code or two-part unenciphered code) is preferable. But while the production of two-part codes involves considerable additional labor for only a very few persons in the Code Compilation Section, the use of superenciphered one-part codes involves much labor for hundreds of code clerks working under the difficult physical and mental handicaps usually found in the field of active military operations. It is evident that this conclusion was the one soon reached by the Code Compilation Section, as is attested to by the following extract from Major Barnes' introduction to his report:

Two methods of compiling codes presented themselves. First, to construct a code book containing words and phrases in common use and supplement it by a series of distorted alphabets and cipher keys which could be rapidly distributed to organizations in the event of the capture of a code book. Second, to take away from the front area and place upon General Headquarters the burden of distortion and substitution by the printing and distributing of new code books at frequent intervals.

The first method imposes upon the front-line code men the double duty of putting up a message on code and changing by the use of a cipher table. In view of the fact that code work is frequently done under heavy bombardment and gas or in the critical moments of an advance, it does not seem advisable to add any additional burdens of code operators.

The second method, by avoiding the use of the cipher tables, does away with this double encipherment and puts upon headquarters the work of double encipherment which is accomplished by the reissuance of editions of code books compiled in the comparative quiet of the back area under more or less normal conditions.

If any apologia is necessary in extenuation of the facts concerning the first two unsuccessful codes put out by the Code Compilation Section of the AEF, we need go no farther than Major Barnes' own report, which states the matter quite succinctly in the following words:

It must be borne in mind that at the commencement of the war no permanent organization existed in the American Army either for the building up or the breaking down of codes.

Major Barnes, whom the writer knew rather intimately from 1919 until his death in 1926, himself never set forth any claims of cryptanalytic skill or experience. He was a code clerk in the State Department when the United States entered the war, and he was chosen not for any pretensions he may have put forth as a cryptanalyst but because he had at least some experience with codes and their handling in communications. It is doubtful if anybody else would have avoided any early mistakes he might have made, for, as he says, there did not exist any organization "either for the building up or the breaking down of codes." Another very illuminating sentence must be quoted from the Barnes report:

> At first the British and French were rather reluctant to disclose the systems which they had adopted for their codes, but eventually copies of obsolete editions were turned over to this Section for reference and study.

It would be very interesting to know definitely when these obsolete editions were made available. That by the time Lieutenant Childs made his study the relations between the Code and Cipher Compilation Section of the AEF and of the British and French were quite close—if at the beginning of American participation they had been rather distant—is attested to by the fact that on June 13, 1918, Maj. Frank Moorman, officer in charge of the Code Solving Section, G2–A6, GHQ–AEF, addressed the following letter to Maj. M. V. Hay, the officer in charge of Code and Cipher Solution Section of the British War Office, in London:

GENERAL HEADQUARTERS,
GENERAL STAFF, SECOND SECTION (G–2 A–6),
France, June 13, 1918.

CAPT. M. V. HAY, GENERAL STAFF,
M. I. 1 B., British War Office, London.

DEAR CAPTAIN: The enclosed sheets are messages encoded by use of our new code.
No enciphering is required. Code books are to be rearranged and republished at frequent intervals.
Would be very glad to receive any suggestions or criticisms that occur to you.

Very sincerely yours,
FRANK MOORMAN.

An identical letter was addressed to Capt. O. T. Hitchings, the officer in charge of the Code and Cipher Solution Section at the General Headquarters of the British Expeditionary Forces in France. The messages referred to in the letter will be found in appendix 13.

The following reply was received from Major Hay:[9]

M. I. 1 B./890/Cy.

M. I. 1 B., WAR OFFICE,
24th June, 1918.

DEAR MAJOR MOORMAN: Many thanks for your encoded messages. We have not been able to solve them or even to get any light. The security appears of a high order.

I enclose a memorandum embodying my views on this code.

Yours sincerely,
M. V. HAY,
Major, General Staff.

MAJOR MOORMAN,
General Staff, 2d Section (G–2),
AEF, France.

[9] The memorandum mentioned in the second paragraph of Major Hay's letter is given in full in appendix 14 hereto.

The following reply was received from Captain Hitchings:

SECOND SECTION,
General Staff, AEF

DEAR MAJOR MOORMAN: I am sending you a short survey of our observations on the 41 messages you sent me for criticism and eventual solution. As I told you in my last letter we have not succeeded in solving them, but you will see in the enclosed survey a few possible lines of attack.

Certainly up to date I have not the slightest doubt but that you have produced a code which if easily workable is far sounder than the present German system.

I shall be interested to know how it works in practice.

Yours sincerely,
O. T. HITCHINGS.

INTELLIGENCE E (c),
2d Echelon,
30th June 1918.

The "short survey" to which Captain Hitchings referred is given in appendix 15.

The following memorandum from Major Moorman to Col. D. E. Nolan, then A. C. of S., G2, GHQ–AEF, will also be found to be of interest in this connection:

GENERAL HEADQUARTERS,
GENERAL STAFF, SECOND SECTION (G–2, A–6),
France, July 13, 1918.

Memorandum for A. C. of S. (G–2):

I have recently had a number of messages prepared and encoded by use of our "Potomac" Code which is used for radio messages in divisions.

Copies of these coded messages were furnished code men in my office and were also sent to Major Hay of the British War Office and Captain Hitchings at British G. H. Q., for test as to security of code.

Reports from code men in my office were made verbally. They were uniformly to the effect that while, by no means "unsolvable," this code was more difficult than any employed by the Germans.

The enclosed letters from Major Hay and Captain Hitchings show that these officers, both of whom are expert code men, approve of our system.

Each also furnishes an interesting but rather long and highly technical discussion of possible means of attack. These are filed in my office and are available for your inspection if desired.

The Potomac Code has been furnished corps for all divisions except those which have just arrived from the United States. Its general use will begin July 15.

New books will be issued at irregular intervals varying from 2 to 4 weeks. One complete edition is now held in reserve for immediate issue in case of loss or "accident" to one or more copies now in service.

I think the Signal Corps is to be congratulated on having turned out an excellent book.

FRANK MOORMAN,
Major, G. S., AEF.

The foregoing memorandum formed an inclosure to a letter from Colonel Nolan to Brig. Gen. E. Russel, then Chief Signal Officer, AEF. The letter and its 1st Ind. are given below.

GENERAL HEADQUARTERS,
GENERAL STAFF, SECOND SECTION (G–2),
France, July 20, 1918.

From: A. C. of S., (G–2).
To: Chief Signal Officer.

1. There is enclosed for your information copy of memorandum in regard to the "Potomac" Code, recently compiled by the Signal Corps.

2. The favorable comments of our own and British code men have been brought to the attention of the Commander in Chief.

D. E. NOLAN,
Colonel, General Staff.

1st Ind.

Hq. SOS, OCSO, July 24, 1918—To A. C. of S., G–2, GHQ, AEF.

1. It is very gratifying to learn that the work of our code officers has met with the approval of your office, and the thanks of all concerned is tendered for your bringing it to the attention of the Commander in Chief.

E. RUSSEL,
Brigadier General, N. A., C. S. O.

About the time that a copy of the new Potomac Code was submitted to the British for comment, Col. Ralph H. Van Deman, who had recently been Director of the Military Intelligence Branch, Executive Division, of the War Department General Staff in Washington, was making a visit at GHQ–AEF, where he apparently had a conference with Major Moorman. The following memorandum resulted therefrom:

GENERAL HEADQUARTERS,
GENERAL STAFF, SECOND SECTION (G–2, A–6),
France, July 13, 1918.

Memorandum for A. C. of S., (G–2):

Colonel Van Deman suggested the advisability of sending to the Military Intelligence Branch a copy of our Trench Code with brief statement of how and by whom it was used. I have added a request that faults discovered be pointed out.

I request that letter be returned to me for enclosure with code book.

FRANK MOORMAN,
Major, C. S., AEF.

The following letter was thereupon sent to Washington:

GENERAL HEADQUARTERS,
GENERAL STAFF, SECOND SECTION (G–2.),
France, July 13, 1918.

From: A. C. of S. (G–2),
To: Chief Military Intelligence Branch, Executive Division, General Staff, Washington, D.C.
Subject: Trench Code.

There is enclosed for your information copy of our "Potomac" Code. This is designed for use within divisions for messages sent by Radiotelegraphy or other means liable to interception by the enemy. It is proposed to change these books at irregular intervals varying from 2 to 4 weeks.

As future editions will differ from this in little besides the arrangement of the code groups, copies will not be furnished you unless specially called for.

A reserve edition is on file for immediate issue in case of loss or "accident" to one or more copies of books in service.

Copies of coded messages have been furnished code men of this section and the British War Office. All have reported favorably.

It would be appreciated if you would have tests of this code made and any faults pointed out.

D. E. NOLAN,
Colonel, General Staff.

It was at this very time that Yardley was in charge of the Cipher Bureau (M1–8) at Washington, and this letter with its accompanying code must have come to his attention, but I have not been able to locate a reply to this letter. It is pertinent to inquire: If the AEF field code was so faulty, why did he not call attention to the weaknesses it contained—if indeed it contained them?

A final letter in this connection will also be of interest:

JULY 16, 1918.

CAPT. H. R. BARNES, Sig. R. C.,
Office of Assistant Chief Signal Officer,
GHQ, AEF, APO 706.

MY DEAR CAPTAIN BARNES: I am in receipt of a letter from Colonel Hitt, enclosing a copy of the comments made on your Potomac Code by the British General Staff. They are very complimentary about this code, and Colonel Hitt has supplemented their remarks with the following comments:

> * * * We believe that this code system will be better than anything now in use on either side, and that messages intelligently sent will be perfectly safe.
>
> In this connection, I would like to call attention to the excellent work which has been done on these Front Line Codes and on the Staff Code by Capt. H. R. Barnes and his assistants in the Code Compilation Division. They have worked without regard to hours, and have given their best ideas and most painstaking attention to their work. The result is a series of military codes that are better than anything I know about. I commend these officers and soldiers to your attention for their zeal and professional ability in an important and highly specialized branch of our work. * * *

I have recommended Lieutenants Chambers and Ryan for promotion, in accordance with recommendations which were sent me. I wish you would acquaint them of my pleasure on noting the good work they have done, and I think it just to express my appreciation of your and their devotion to the important duties which you have to perform.

With best wishes,
Very truly yours,
E. RUSSEL,
Brigadier General.

6. THE "RIVER" AND "LAKE" SERIES OF AEF FIELD CODES

The principle of the two-part code having been adopted as the basis of the AEF field codes, the first of the remarkable series of such codes was, as already stated, the "Potomac Code," named of course after the famous river marking the location of the Capital of the United States. This code was issued on June 24, 1918, in an edition of 2,000 copies. There then followed a series of 14 codes prepared in a period of 5 months from June to November 1918, nearly 3 codes per month, an achievement which will on consideration be found most noteworthy in comparison with what other belligerents accomplished within the same period. But let Major Barnes' excellent report tell the story in his own words:

In June 1918, the first issue of the new series was published and 2,000 copies were turned over to G–2 for distribution.

This code book, known as the "Potomac Code," the first of the so-called "River Series," contained approximately 1,800 words and phrases, and with the decoding section made a pamphlet of 47 pages. It was approximately 7¼ by 9¾ inches printed in "typewriter type," a type selected for its good legibility under the poor lighting conditions of the field.

Each page contained 2 columns of 50 lines each, or 100 lines to the page. At the margin of each column were printed in a small block a "null" and the following spelling combinations:

"ed, en, er, es, ing, ion, ll, ly, nd, re, s, st, th"

Thirty-five different nulls were provided and the instructions were that 1 at least should be used with every 10 groups and invariably between groups used to spell out words.

The "Potomac Code" marked the inauguration of the policy of taking away from the front line all possible extra work in connection with coding and decoding and putting upon headquarters the burden of affording security by replacing and reprinting the books. The reissuance of code books provided the necessary secrecy since no particular code was intended to be in service for a great length of time, and, therefore the amount of intercepted messages would be comparatively small. In accordance with the plans of G–2, who distributed the code books, one edition was to be distributed down to regiments; another edition sent down to Army Headquarters; and a third edition held in reserve at General Headquarters. That this plan was well conceived was demonstrated by the fact that when this particular book was captured, 1 month after publication, the two sets were ready in reserve and were reissued to the entire Army organization, within 2 days.

* * * * * * *

The following points were considered in the actual construction of the Trench Codes:

1. *Clearness of type*, account being taken of the poor lighting facilities at the front.

2. *Simplicity of operation*, believing that the absence of complication would tend to reduce error in preparation and transmission and increase the number of coded messages.

3. *Size of the book*, in order to make it convenient to handle and preserve.

4. *Vocabulary*, large enough to provide a working basis for all ordinary conversation, yet not too large to be easily handled.

5. *Paper*, of a quality sufficiently good to last for the short life of the book, yet poor enough to permit of rapid destruction if necessary to prevent capture.

6. *Variants*, to provide safeguards to avoid repetitions as much as possible of common expressions, and,

7. *Certain accentuated features*, to call particular attention to things to be remembered or to make them conspicuous.

* * * * * * *

The "Potomac" was followed on July 15 by the "Suwanee" in an edition of 2,500 copies. No radical change was made.

The "Wabash" followed on July 31 in an edition of 2,700 copies. This code followed the same general plan, but was slightly smaller.

The "Mohawk" followed on August 3, in an edition of 3,200 copies. This code was the first one with four-number code equivalents, running from 2,500 to 5,000, making a total of approximately 2,500 groups provided for some 1,600 words and phrases. This book was captured in October.

The "Allegheny" followed on August 12, with 3,200 copies and the number groups were selected from numbers ranging from 1,500 to 5,000. Fifty blanks for the emergency use of organizations were also provided. This book was captured in October, making the third to be put out of commission in this manner.

The "Hudson" followed on September 2, with 3,200 copies; also a number group code. In this code a group of 5 different "nulls" was printed on the margin of each 50 lines with a view to encouraging their use by making them conspicuous. With the object of providing a group for transmission from memory in the event of the loss of a code book, the group "2222" was printed in red ink on the outside cover of the book where it might be readily and often seen.

The "Colorado" followed on September 24, with 3,200 copies, using letter groups instead of numbers. The code books had been slightly reduced in size from time to time, but this issue marked the last reduction. Without reducing the legibility of the type, the lines were closed up and the outside margin reduced to 5½ by 7½ inches as against the 7¼ by 9¾ inches of the first issue. For the first time spelling combinations were printed at the bottom of each page, 16 in all being provided, with 2 or more variants for each combination. On the cover the group "DAM" was printed to be memorized and used if the code were lost.

It was believed that the issuance of the large number of copies necessary to supply both the first and second Armies would needlessly jeopardize the code, and it was decided to issue different series to the two armies. Accordingly, the "Lake Series" of codes was begun, commencing with the "Champlain" on October 7, and an edition of 2,500 copies of each code was put out. To accentuate the difference in the series, the cover printing on the "Lake Series" was in red ink and that of the "River Series" in black ink. The "river" codes were issued to the First Army and the "lake" codes to the Second Army.

Instructions were issued directing that all messages sent in these codes should be preceded by a 3-letter code combination which would indicate the particular code used. Thus a "Hudson" message was preceded by "HUD"; the "Colorado" by "COL"; the "Osage" by "OSA," etc.

After the "Champlain" came the "Huron" on October 15, the second of the "Lake Series." This book differed from its predecessors in that it contained in the front the "Emergency Code List," which was also issued separately down to companies for emergency use. In the back of this code there appeared a double receipt easily detachable, for the convenience of officers receiving and delivering the code books.

The instructions were so altered as to include the telephone alphabet which was intended to simplify the transmission of code messages by telephone.

The "Huron" was followed by the "Osage" on October 28. The changes consisted in the additional printing on the cover of the order to—

"Precede every message in this code by OSA"

and:

"NOTE.—The * indicates new word or phrase"

This last direction was added in order that officers might have their attention quickly directed to new words or phrases which previously they had been spelling letter by letter.

After the "Osage" came the "Seneca" on November 6. This code differed only on the first page of the Encoding Section where on the margins were printed the variants for "minutes," "o'clock," "battalion," "regi-

ment," etc., and the ordinals from first to tenth inclusive, and the printing of the initial letters of each word or phrase in small letters rather than in capitals. This last change was made as an aid to the eye in constructing sentences.

This book contained nearly 1,900 words and phrases as against 1,750 in the early issues of Trench Codes. Many changes had been made in phraseology, however, and of the original list of words and phrases 1,045 alone remained unchanged.

At the time of the Armistice this Section had in press the "Niagara" Code, and the "Michigan" and "Rio Grande" in manuscript. Thus, during the Armies' operations 15 codes were actually compiled in the Trench Code Series. To be more exact, 14 codes were prepared in the period of 5 months from June to November 1918, nearly 3 per month.

In the 10 months of active operations the Section completed and printed more than 80,000 code books and pamphlets, all numbered, recorded, issued, and receipted for when issued. The record is complete, no copy being missing.[10]

7. The "Staff Code"

At the same time that the Code Compilation Section of the AEF was engaged in preparing the field codes, it embarked upon an even larger project, that of preparing a "Staff Code." The story is tersely told in Major Barnes' report:

The American Army in the field had no comprehensive code for headquarters work except the War Department Code which was intended primarily for cable work and not for active operations in a foreign country. The demand for a substitute was so insistent that a code was compiled primarily for communication within France.

The preliminary work covered a wide range of activities and required several months' study of confidential papers of organizations, replacements, operations, and military documents generally.

In May 1918, the "Staff Code" went to press and was completed 1 month later. This code contained approximately 30,000 words and phrases. Among other things it embodied a list of several thousand French towns and villages and a complete list of the Army organizations up to May. It is believed that this is the largest and most comprehensive code book ever printed in the field. It contained both number and letter group equivalents. More than 50,000 telegraphic combinations were sent over an instrument in order by selection to reduce to a minimum the chances of error in transmission over the telegraph lines. One thousand copies of this code were printed and bound with a flexible cover.

This code differed from many others in that it was an alphabetical rather than a subject code. It was divided into what was known as a right-hand and left-hand column series. The left-hand series of code combinations differed in plan from the right-hand. This was done to confuse as much as possible enemy code experts. The complete Army organizations and all proper names appeared in this column, the right-hand column being reserved for the usual words and phrases of a code.

With this code were provided five different tables of distortion for G–1, G–2, G–3, G–4, and G–5. These gave a cipher combination to the original group and made an added security.

These distortion tables were prepared with an Enciphering and a Deciphering Section. They consisted of certain selected two-letter combinations from AB to ZY, arranged alphabetically with two-letter equivalents selected at random.

For example, the code group FSNB might be distorted to read, VKXV. This was done simply by dividing the four-letter group FSNB into two parts and distorting each part separately.

The decipherment consisted in the reversal of this process by consulting the table and translating VKXV to read FSNB.

Five different tables were provided for use with the Staff Code but there was no limit to the variety which could have been made under this system of distortion.

A page of the Staff Code, and a sample of the enciphering table are shown in appendix 17.

8. Miscellaneous Codes Prepared in the AEF

Among the miscellaneous codes[11] prepared by the Code Compilation Section, AEF, the following deserve mention, as described in Major Barnes' report:

In March 1918, an addenda sheet was compiled in order to provide code equivalents for a number of words omitted from the "War Department Code" and in addition to provide code groups for transports and a number of French cities and towns. One thousand copies of this supplement were issued.

[10] A page of each of these field codes is shown in appendix 16. In addition to those mentioned in the Barnes report will be found Field Code No. 1, Field Code No. 2, and Field Code No. 3. These were printed in the AEF but were never issued. They were transported to the United States after the Armistice, kept in reserve for about 3 years, and then destroyed as obsolete.

[11] Samples of the various codes mentioned will be found in appendix 18.

In March 1918, what was called a "Telephone Code" (sometimes called the "Female Code") was prepared for disguising the names of organizations and commanding officers. Originally intended for use over the telephone, it was principally used in messages to conceal organizations. Its code equivalents were the first and last names of women, and it was so arranged that the name "Mary Brown," for example, might mean the "Chief Signal Officer of the First Army." Five hundred copies of this code were printed on a single sheet of letter-sized paper and turned over to G–3 for distribution. In October 1918, this code was reissued with the addition of a decoding section.

In June 1918, a short three-letter group code was prepared for use in certain principal telegraph offices in order to conceal troop movements. In July 1918, a more complete code of some 1,300 words and phrases was issued to replace the former edition. These codes were photostated and distributed to six telegraph offices.

In May 1918, a short code list for reporting casualties was prepared and printed. This list was printed later as a general order.

In September 1918, a short code of two-letter combinations was prepared to meet in part the needs of the front line who had no access to the "Trench Codes" or other means of secret communication. Six thousand copies of this "Emergency" Code were printed and distributed down to companies. It contained some 50 commonly used phrases with an encoding and decoding section. A new edition of these lists was put out to accompany each issue of Trench Codes. When the "Huron Code," the second of the "Lake Series," was issued on October 15, the list was printed in the front of the code book in order to provide a ready reference for communication between the users of the large codes and the front line who had but the small list.

This "emergency" list was but in its infancy at the conclusion of the war and the experience gained by observation and criticism would no doubt have grealy improved it.

Up to October 1918, the French Radio Code had been used by the American Army as a service code, but the difficulty in language was a constant source of trouble.

In October, therefore, a new American Code was compiled, consisting of about 1,000 words and phrases, and has been in use up to the present moment.

As an emergency measure, all the work of compilation, printing, and delivery to the First Army was done in a period of 6 days. This code was known as American Radio Service Code No. 1, and 2,000 copies were printed.

In connection with the confusion arising from the use of a multiplicity of codes, authorized as well as unauthorized, Major Barnes says:

Although not properly speaking a function of the Code Compilation Section, the demands made upon it to determine what particular code was being used in the preparation of certain messages were so frequent that the need for centralization of code work was made conspicuous.

At certain times messages were being sent by different organizations in "Playfair"; "Hudson" and "Mohawk" Trench Codes; private organization codes regarding replacements; private casualty codes; ammunition codes; and in addition messages in plain containing such code groups as "Nellie Smith," and giving a location as "Windfall" or "Laredo."

The Code Compilation Section was never able to ascertain how many codes were in actual use at any one time; when they were put into service or withdrawn; or who issued these codes. Moreover, it did not know of any one office that did know. One instance of the confusion which naturally arose out of this multiplicity of codes is the case where a message was received at General Headquarters addressed to an officer in "London." After it had been put on the wire and forwarded to London, England, and a reply received that he was unknown, an investigation developed the fact that an organization in the field had assigned the code word "London" to an adjoining village but had not notified headquarters of its code list. This particular difficulty was straightened out, but not even Military Intelligence had a complete list of the codes in use.

There were far too many codes in use in the American Army, codes prepared to meet an emergency by men who had no special knowledge of such work. These codes must have presented no great difficulties to enemy code men and no doubt gave away much valuable information.

In connection with the latter statement it seems worth while to give in its entirety what must be considered as the gem of the collection of unauthorized "codes" issued and perhaps used by certain units of the AEF, perhaps only for training, perhaps for a few actual messages. The "baseball code" shown in appendix 19 was found among the World War files and the writer vouches for its authenticity. The code words of that gem are the names of famous baseball players of a generation now gone and forgotten. Hence, much of the zest in the reading of the text of that code must be reserved for those old timers who "can remember way back when."

In addition to these miscellaneous codes, mention must be made of a special edition of the French "carnet réduit" which was issued in a French-English parallel column form, for use by AEF troops which at one time were either situated in a French sector or were brigaded with certain French units.

9. Printing of Codes in the AEF

The printing of codes was by Army Regulations a function of The Adjutant General's Office and while the work was done by that office, it was conducted in cooperation with the Signal Corps and under the close supervision of the Code Compilation Section.

The following is taken from Major Barnes' report and will give a clear picture of the operation:

> The codes compiled by the Code Compilation Section were printed at the printing office of the AGO at General Headquarters.
>
> By an arrangement with that office these codes were given preference over all matter except general orders and bulletins. In general this plan proved satisfactory, but at times, owing to an unusual pressure of work, an issue of codes was considerably delayed. As a rule, this delay was comparatively unimportant, but there was always the danger that a code would be captured and a new issue needed at once to replace it. As a matter of practice two complete codes were always kept in stock for issue, except upon the occasion when three different series were in use on three different fronts at the same time. But the danger was too great to permit of this hazardous plan of control being long used. Frequently a code could be set on the linotype, carried through the composing room, proofread twice, printed and bound in about 5 or 6 days of normal work, but this only under the most favorable conditions. Under pressure, working three shifts of men during the 24 hours, the linotype could complete its work in 48 hours. However, upon occasions all work on codes was stopped for several days and this delay became too prevalent to make for the best results.
>
> During the process of printing, the codes were under the constant supervision of an officer whose duty it was to destroy all spoiled sheets containing impressions even to the mats on the presses. All copies were counted and accounted for and the metal type melted down after the final impression. In many cases two or three officers were on duty in the printing office keeping the various operations in sight.

The number of copies to be printed of each edition of a code was determined by G–2.

10. Distribution of Codes in the AEF

The problem of the proper and rapid distribution of codes was one that gave considerable difficulty. According to Army Regulations this was a function of The Adjutant General's Office, but for one reason or another the work apparently could not be performed satisfactorily by The Adjutant General.

In the final report of Lt. Col. Frank Moorman, the officer in charge of the Radio Intelligence Section G–2, GHQ–AEF, there occurs the following paragraph:

> On account of the uncertainty of the courier service and their refusal to carry heavy packages, the lack of interest in the distribution of code books by other departments and urgent need of making distribution on time, the work of distributing the Trench Code books was taken over by this Section.

Officers from the Radio Intelligence Section at GHQ served as special couriers to carry the heavy packages referred to by Colonel Moorman to Army Headquarters. From there further distribution was made by personnel of the Radio Intelligence Section of Army to division, corps, and Army troops.

Major Barnes says in connection with this subject:

> The problem of distribution was a difficult one to solve inasmuch as the whole question was without precedent in the American Army and was changing from day to day by the peculiar conditions of the front and by the formation of the Second and Third Armies. In the main the centers of distribution were the officers of the G–2 section who had manifold other duties of equal importance to perform.

Today the situation in this respect is far more satisfactory, since the War Department has realized the importance of this matter and has concentrated all code work, including the compilation, printing, distribution, and accounting of codes, in the Signal Corps.

11. Cooperation With G–2

The following remarks are quoted from Major Barnes' report:

> During the entire period of the war this Section was cooperating closely with G–2 at General Headquarters. A careful study of the errors committed by the enemy was made and later, when the American intercept stations were established, close examination was made of the American messages both by G–2 and by this Section to determine the common errors of commission and omission. When grave mistakes or violations of orders occurred the attention of the offending officers was invited by G–2 to the danger of such practices, and helpful suggestions were given them for their better understanding.
>
> Lieutenant Colonel Moorman was indefatigable in his endeavors to educate, encourage, and assist the code men of the Army, a task made the more difficult by the vast amount of "propaganda" necessary to popularize these codes. This work he assumed in addition to the already heavy burdens of enemy-code destruction. To his unfailing courage of conviction and clearness of vision the Code Compilation Section is indebted for a large part of its achievements.

The present writer is able to elaborate somewhat upon Major Barnes' statements.

The inexperience and perhaps early faulty training of American troops caused numerous messages to be sent in plain language. Other messages violated the regulations adopted for the control of radio communication within the AEF. The intercept stations of the Signal Corps, working in close cooperation with G–2, were given the additional function of listening in upon our own transmissions with the result that the need for stations which should specialize in copying messages from American nets was soon demonstrated. The first station of this sort was established at Toul on July 11, 1918, for intercepting American damped-wave transmissions and soon afterwards another control station was established for copying continuous-wave transmissions. When the First Army Headquarters moved to Souilly, two undamped-wave stations were established to monitor American radio traffic in this sector. These stations monitored the messages transmitted and, by promptly reporting messages sent in clear, on several occasions succeeded in nullifying slips which might otherwise have been disastrous. However, messages in code could not, of course, be monitored so easily. These had to be sent on to GHQ, where they were studied by a special section set up for this purpose under the Code Solving Section of the Radio Intelligence Section, G–2, GHQ.

It is important to note that the personnel of this control or "Security Section," as it was called, consisted of trained officers who worked in very close collaboration with the cryptanalysts who were working on the solution of German codes and ciphers. Thus, the benefit of the experience from the study and observation of German code traffic could immediately be transferred to our own traffic.

When serious violations were noted, letters were sent to the responsible commanders calling attention to the dangers resulting therefrom. Many such letters were sent, but regretfully it is to be said that little good was accomplished thereby.[12]

12. Security Service

The following is quoted from the Barnes report as being pertinent to this question of communication security, already alluded to in the foregoing section:

> Although it may seem a paradox, the most striking feature of the use of Trench Codes was the general inclination to avoid them whenever possible. This idea had its root in the proverbial inclination of the American for the before-mentioned short-cut. It received its nourishment either directly from commanding officers by orders to refrain from codes or indirectly through inattention or general lack of knowledge on the subject. Under this encouragement and on such fertile soil the idea grew so amazingly that even instructions from General Headquarters and the advice of code men were ignored or overlooked. As an instance of this, it is a matter of record that on one occasion a general in command in the field gave positive orders that prior to and during a certain important movement absolutely no code was to be used by his division.

[12] See appendix 22.

On the other hand it was found that in actual practice the very men who might have been expected to shun codes were the ones who used them most. Thus it developed that the officers of the Signal Corps, whose primary duty it was merely to transmit the messages, were in many cases using the codes freely for the transaction of their own business, and moreover, in many instances actually coding and decoding messages for the infantry, artillery, and other organizations. With but few exceptions it was from these officers that all the constructive criticism was received.

As a matter of fact Signal Corps officers had received no more actual instructions in the use of Trench Codes than had the Infantry or Artillery officers, but the course of their instruction contained enough information on the general subject to remove the mystery from the word "code" and make it commonplace to be handled with impunity, so that to them it had no terrors.

* * * * * * *

It will be found difficult to bear in mind under extraordinary conditions all the minute directions which may be laid down for the use of a code, yet a slight deviation from those directions may give to the enemy who has intercepted the message the clue not only to that particular message but to many others. In other operations of an army in the field, an error in judgment or of carelessness may rebound upon the unfortunate officer to his rapid undoing, but an error in code operation may be apparent at once, may not in any way affect the responsible officer, but may wreak havoc upon the plans of the supporting troops adjoining. This might be the immediate result of such error. The late result might be that his mistake had provided the key which could unlock messages hitherto undecipherable, and such messages as might be sent until the notice of error was disseminated. When it is remembered that the secret correspondence of the entire Army may be jeopardized and delayed by one man's carelessness or failure to carry out instructions, officers should treat the preparation of code messages with the seriousness which the gravity of the situation demands. These remarks are apropos of what may seem to be errors of small magnitude, but are made emphatic because they might otherwise be considered of small moment.

Referring to the "Secret Instructions for the Use of Army Codes," the following practices are expressly forbidden:

(*a*) To use plain language in the same message with code or cipher.

(*b*) To repeat a message in any code or cipher other than that in which first sent.

(*c*) To repeat a code or cipher message in plain language.

(*d*) To repeat a plain language message in code or cipher.

Under section (*a*) it is so obvious that the use of a word in plain affords a ready clue to the adjoining words that no comment is necessary. Such words usually would be used to avoid the labor of spelling out letter by letter, and if nothing were lost save that particular message no great harm would result. But the solution of a group by the enemy may mean not only the gain of that group but be like the ever-widening circles in the water caused by the dropping of a stone.

Section (*b*) emphasizes the fact that repetition in another code may jeopardize the secrecy of the second code, inasmuch as the first may have been intercepted and deciphered.

Section (*c*) is almost axiomatic in its directions, since it is evident that such a procedure simply presents the enemy with just that many code groups, plus the ratio of the widening circle.

Section (*d*) is but the reversal of (*c*), and its importance is equally obvious.

The reference to "Secret Instructions for the Use of Army Codes" is the only time such an item is mentioned in the Barnes report, but a copy of this complete publication is given in appendix 21.

In addition to the foregoing it is thought that certain extracts from Colonel Moorman's report on this subject will be extremely interesting:

Security Service. Listening Stations

This service, almost unthought of in 1917, was established by practically all belligerents in 1918.

In our own service its scope should be greatly enlarged. It should include all means of giving false information to the enemy and of keeping real information from him. That part which relates to codes and the use of our own means of transmitting information should be handled by the Radio Intelligence Section under the supervision of the officer having general charge of the entire service. Only officers who have made a scientific study of codes and the information to be obtained from them, even when they cannot be solved, are in a position to know what will or will not give information to the enemy.

One of the main duties of code men is that of taking advantage of the enemy's mistakes. It is hardly possible that we will ever have a sufficient number of trained code men to handle the business of an army in the field. It will therefore be necessary to entrust to untrained men the duty of coding and decoding messages. If this is

done carelessly the enemy will certainly take advantage of the situation and obtain information of the greatest value. Our own experience in the St. Mihiel and the Argonne-Meuse Battles furnished ample proof of this.

An effort to control the use of code by the issue of orders and instructions was unsuccessful. Commanders were too busy to give the matter their personal attention and subordinates to whom code work was entrusted were changed too frequently to permit of all being familiar with the rules and the absolute necessity of following them.

The policy of writing a letter to the appropriate commander in the case of each offense was then adopted and many letters sent out. Only a few of these were answered and in these cases the action taken was entirely inadequate. In one case an officer was reprimanded by his commander. In others the excuse was made that officers did not know or were too busy or thought they were justified in their action. That these unanswered letters or those in which action did not suit the case were not followed up was due at first to the inadvisability of worrying commanders too much with the question of code when their time was fully taken up with the more urgent and important matter of actual combat. Later the signing of the Armistice made further action unnecessary.

In any case the writing of letters to commanders is too slow and cumbersome a method of handling the matter. The commander cannot possibly give his personal attention to the question of whether or not message number 506 was properly encoded. He therefore refers the letter to some overworked staff officer, usually an inspector general, who files it awaiting a favorable opportunity to make the investigation. When the turn of this letter is finally reached it is found that the responsible officer perhaps has been transferred or is sick or can find no record of the message and does not remember of it having been sent out. In the few cases where connection is actually made with the responsible officer the whole matter is so old that it has lost its interest. Under our system of control it has been everybody's business to carry out instruction in reference to use of code. The natural result has been that it has been nobody's business, and in trying to check up and eliminate faults we have found great willingness and ability to refer us to someone else. Some doubts probably as to exactly which one of several persons, but certain to someone else. This is the natural result of our system.

I have recommended an officer at each headquarters from the company up who shall be definitely responsible for this service. When faults occur it will be his business to know by whom they were committed and to take steps to prevent a repetition. When faults are noted by officers at higher headquarters, it should then only be necessary to inform the responsible officer and direct him to call on the offender for an immediate accounting. The result will be that when an officer decides to save time by disregarding some of those "exasperating and useless" instructions from General Headquarters, he will be called on for an explanation before he has had time either to forget or get transferred, sick, or wounded. The case being fresh will seem more important. Finally, the designation of a particular officer at each headquarters who is definitely responsible for this service will insure at least one officer familiar with instruction to whom the others can go for advice or explanations.

It is interesting to observe that it took 20 years for this recommendation to be put into practice, for it was only in 1938 that the War Department directed that at each headquarters a security officer be designated to insure the observance of the rules of cryptographic security.

In connection with this matter of security it is interesting to add some remarks from Colonel Moorman's report:

Codes were almost unknown in our own Army. The importance of care in their use so as to maintain their secrecy and avoid giving information to the enemy was entirely unappreciated. Previous to, and during the St. Mihiel and Argonne-Meuse Battles, a great amount of valuable information was furnished the enemy through carelessness of our own officers and men in the use of code.

The following indorsement will illustrate the effort made from this office to insure care in the use of code. The fact that such efforts were largely unsuccessful was due to the almost total ignorance of officers in the matter of code and the difficulty of exercising control through commanders, who had neither the time nor the special knowledge required for the purpose.

3d Ind.

Adjutant General, AEF, September 17, 1918.—To: Commanding General, First Army.

1. Returned.

2. Steps will be taken to learn who was responsible for the misuse of code, brought to your attention in attached letter of September 7.

3. Since the organization of the First Army, the First Army radio stations and telephone operators have furnished information of vital importance to the enemy, in regard to your battle order, the organization of your divisions, the location and form of training of divisions in reserve, the location of heavy artillery and tanks while preparing for the attack, and the date the attack was to take place,

as nearly as it could be ascertained by the telephone operators. Your attention has been called, by letter, to many cases of criminal carelessness in the use of our code and the transmission of messages in clear, or in a mixture of code and clear. Even messages entirely in code have, in general, been so carelessly prepared that the enemy will have no difficulty in solving the code.

4. You are directed to conduct a rigid investigation in all cases of reported misuse of code, to take necessary steps to correct such misuse, and to bring to trial officers who wilfully violate existing orders and instructions printed in the code book.

By command of General Pershing:

ROBERT C. DAVIS,
Adjutant General.

The remedy is thought to be the systematic instruction of our officers in time of peace and the placing of representatives of this section at all company and higher headquarters in time of war.

Small tactical code books should be prepared and frequently revised and republished. They should actually be used by student officers at the staff and line schools.

In the extracts quoted above, taken from the Moorman report, it will have been noted that the writing of letters calling attention to violations of the rules for the handling of codes was the course adopted by him in an attempt to produce an amelioration in the conditions to which he refers. But it is apparent that Colonel Moorman ended his labors with the opinion that this method was far from effective. Today, with a much more thorough indoctrination of all services with respect to the importance of communication security, letter writing is a rather effective means of control so far as concerns our Regular Army administrative headquarters, but one may speculate upon the situation that would obtain in time of war, with multitudinous tactical units constituted hurriedly from semitrained and untrained troops. Hence, despite Colonel Moorman's low opinion of "letter-writing" as a method of control the writer deems it interesting to call attention to several examples of actual cases taken from the World Ward records. These have been selected from a number of cases and are shown in appendix 22. They make extremely interesting reading even today.

A final word or two must be said of certain parts of the foregoing extracts from Colonel Moorman's report, which may throw some light upon the source of the greatly exaggerated statements cited on pages 11–12 of this paper, as taken from Yardley's book. Could it be that the third indorsement quoted above came to Yardley's attention and that this is what led him astray? It most assuredly seems that way. Note the parallelism in the sequence as regards the kind of information disclosed: The battle order, organization of divisions, and date the attack was to take place. But note the qualifying phrase in the indorsement, as regards the date the attack was to take place. It is distinctly stated "as nearly as it could be ascertained by the telephone operators." Hence, here was a matter not of a poor code, but of poor telephone security! And, of course, it has already been proved that this had nothing to do with the code messages "solved" by the "young officer" referred to by Yardley.

As a matter of fact it can be stated that if Yardley had obtained his information at first hand he would not have been misled as he was by a single, somewhat ambiguous statement made probably for emphasis in the third indorsement quoted on page 25. After a very careful study of all the facts pertinent to the case the writer is able to throw some further light upon the situation, which to some extent will serve to remove a bit of the blame that falls upon Yardley's shoulders for his unwarranted exaggerations concerning the AEF codes. For it turns out that Yardley learned of two "episodes" and by combining them through his ignorance of the facts produced a single, very confused picture.

The first "episode," if it may so be termed, was the one in which Lieutenant Childs figured so prominently, as detailed on pp. 12-13 of this paper. It has been proved conclusively that what Childs did was merely to reconstruct a single mixed alphabet used to encipher the code groups of a series of test messages, he having been given a copy of the code involved.

The second "episode"—really a series of episodes—concerned itself with the studies made by a young officer of the Security Section, G–2 A6, the Section which was entrusted with the work of studying our own radio traffic and supervising telephone lines with a view to picking up infractions of the rules established for safeguarding our communications.

From correspondence exchanged between the writer and Yardley in 1931 (see appendix 16), it is clear that the latter was present at a lecture delivered to the officers of the Military Intelligence Division, General Staff, in Washington, on February 13, 1920, by Lt. Col. Frank Moorman. The writer was fortunate in finding a copy of the stenographic report of this lecture, from which the following is a verbatim quotation (the entire report is given in appendix 23):

> Last is our control over our own radio communications and that was an important point that we overlooked at first. It was difficult to get those in authority to see the importance of it for a time. We installed several stations to copy the American messages and send them in to our headquarters to be turned over to a man who knew nothing about the battle order or plans. He solved our code, located the divisions, prepared the American battle order and notified the Assistant Chief of Staff that an attack was to take place. He missed the hour of attack by 24 hours. It was the mistake of the Signal Corps man who sent the message, he stating that the attack was to take place the next morning, when it wasn't to take place until the morning after. When we realized what our men had worked out from these messages, every one of which could be copied by the Germans, it gave an impetus to plans for the control of our own service.

It is unfortunate that Colonel Moorman was not more specific in the foregoing statements for he unintentionally misled Yardley and some of his other listeners, for there never was such a single episode as he describes in which an officer solved our code *and as a direct result* "located the divisions, prepared the American battle order and notified the Assistant Chief of Staff that an attack was to take place." This officer, it is true, did solve a few code groups now and then and *occasionally obtained data regarding the American battle order, but data concerning an impending attack were obtained by listening in on telephone conversations.* In any case, it must be emphasized, it was not the code itself which was at fault, but the personnel who used the code. And had Yardley been better informed about the true situation in this respect he never could have drawn the erroneous conclusions which he did draw from Colonel Moorman's lecture, nor could he have been misled by Colonel Moorman's highly generalized statements given in a more or less casual manner, and probably spoken extemporaneously.[13]

13. Concluding Remarks

The author would like to bring this paper to a close by quoting again from Major Barnes' report:

> Throughout a large part of the Army a great deal of criticism was from time to time directed toward the Trench Codes, most of it destructive rather than constructive. This was natural, perhaps, in view of the extremely limited knowledge of codes and ciphers.
>
> The G–2 section sent out a circular letter inviting criticism and requesting suggestions looking to improvement. In the main these suggestions were words and phrases to meet certain local conditions to be added to the vocabulary. Whenever these additions seemed broad enough to cover more than a local need they were added, ofttimes words or phrases being removed to make room for them. It must be borne in mind that the phraseology of war changes very rapidly and words and phrases quickly become obsolete. As an instance "rolling barrage" lived its day and passed out to make way for another phrase of the moment.
>
> Another suggestion, or criticism, frequently made, was a comparison with the French and British code systems. This usually was made by troops who were or had been serving with those forces. The French used groups of three numbers each and were limited therefore to 999, whereas the American codes had nearly twice that number.
>
> Frequent requests were made to provide both letters and numbers for code groups but the peculiar construction of the American codes rendered this impracticable. However, to cover this need the pronouncing alphabet was printed in the instructions in each code book. A study of this would have made the transmission of code groups over the telephone simple and accurate, and it was to obtain this accuracy that numbers were desired.

[13] See appendix 23.

The question of the relative values of letters and numbers for telegraphic transmission was made the subject of an exhaustive study. A large number of telegraph operators, radio operators, code men, and the two most experienced superior officer code experts were consulted. The result was inconclusive inasmuch as opinion was almost equally divided even in each of the various classes.

So far as the actual coding of messages is concerned, I personally prefer numbers for the reason that the combination "2632" is clearer in my mind than the combination "ABZQ," for example.

To return to criticism, it should be said that every effort was made both by circular and by personal solicitation to obtain constructive criticism. Starting as the Section did from absolute zero it was realized that all possible assistance should be sought from the actual users of codes in the field with a view to affording them the maximum assistance. So well in fact was the criticism received that each issue of the Trench Codes was different from its predecessor in material content and in construction; clearness, rapidity in operation, scope and ease of operation being constantly borne in mind. This is illustrated in one comparatively insignificant item by the constant diminution in size of the book itself to meet the wish for a more convenient volume to handle.

Further criticism was invited from the British code experts who first were given a number of messages in the new Trench Code and requested to "break them down" and then requested to point out faulty construction. Later, these same experts were furnished with a copy of the book and further suggestion as to faults was requested and given.

Major Hay, of the British General Staff, after exhaustive study, replied to Major Moorman of G-2:

> We have not been able to solve them or even to get any light. The security appears of a high order.

In his report he analyzes his views on the probable construction of the code and adds:

> I am of the opinion that this code when used with care could not be read by the enemy until he had collected a very large amount of material. * * * Under favorable conditions this code would be safe for at least 2 months * * * but it would be advisable to make a more frequent change. * * *

This is interesting in view of the established principle of changing every 10 days.

The conclusions drawn by the British experts are not always favorable, although but few criticisms occur, but their deductions are interesting and for the emphasis which they, as well as the Germans, place upon errors and carelessness the reports are submitted herewith.

At the very time when the greatest number of flattering references to the superiority of the British system of double-cipher were being made that Army had in contemplation a complete reversal of their system and the adoption of the American. They did indeed effect a partial change in plan before the cessation of hostilities. When I informed a British Code expert that our codes could be compiled in 10 days he was completely dumfounded, saying it would take them at least 30. This, I think, was the greatest obstacle they had to overcome in a change of system.

* * * * * * *

In conclusion, I should like to express my appreciation of the valuable service rendered by Col. Parker Hitt of the Signal Corps during this trying period. His broad knowledge of codes in general, his intimate knowledge of the Army and the General Staff, his unflagging industry added to a never-failing courtesy even under tremendous pressure of work, made my task far lighter in consequence. To him more than to any other officer of the American Army is due whatever success the American Codes may have obtained.

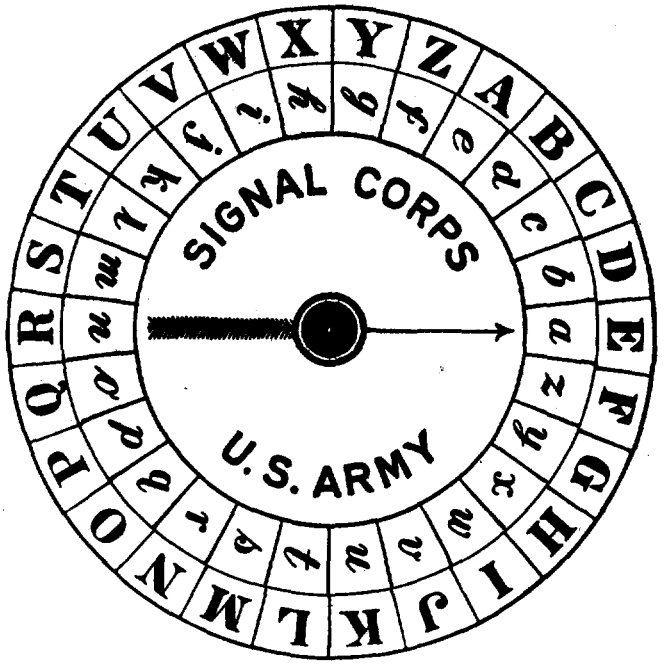
The accomplishments of the Code Compilation Section, AEF, are succinctly summarized in the Annual Report of the Chief Signal Officer for 1919 (p. 536). A copy thereof will be found in appendix 24.

When the difficulties that confronted the Code Compilation Section, AEF, at its establishment are observed in retrospect, and its achievements are measured even by 1940 standards, the present author is of the opinion that one can apply to the work done by this service the salutation so welcome to military personnel: "Well done!"

APPENDICES*

*All appendices except those marked by asterisk are photolithographic reproductions of the originals.

Appendix 1.—THE OBSOLETE U. S. ARMY CIPHER DISK



To encipher a message, the key letter or the first letter of the key word or phrase is set opposite "a." Let us assume it to be "E." The cipher letters to be written are those opposite the text letter when "a" on the circle is set opposite "E" on the card. For example, "send powder" would be written "MARBPQIBAN." To use a key word or phrase, each letter is used in turn to encipher one letter only. When the last letter of the key word is used, repeat until all letters of the message are enciphered. Numbers when enciphered with the disk must be spelled out.

Appendix 2.—A. E. F. INSTRUCTIONS FOR USING THE CIPHER DISK AND THE PLAYFAIR CIPHER

ARMY SIGNAL SCHOOL
AMERICAN EXPEDITIONARY FORCES
FRANCE

VISUAL AND TACTICAL DEPARTMENT

CODES AND CIPHERS

A code is a table of letters, words, or phrases, to every one of which a definite meaning has been assigned. For example:

Plank—Enemy troops in _____
Plant—Enemy troops progressing in _____
Plantain—Enemy troops stopped while progressing in _____
Plantation—Enemy troops retreating in _____
Planter—Enemy troops stopped while retreating _____

Generally speaking, a cipher is one or the other of the following classes:

1st—Transposition cipher.
2nd—Substitution cipher.

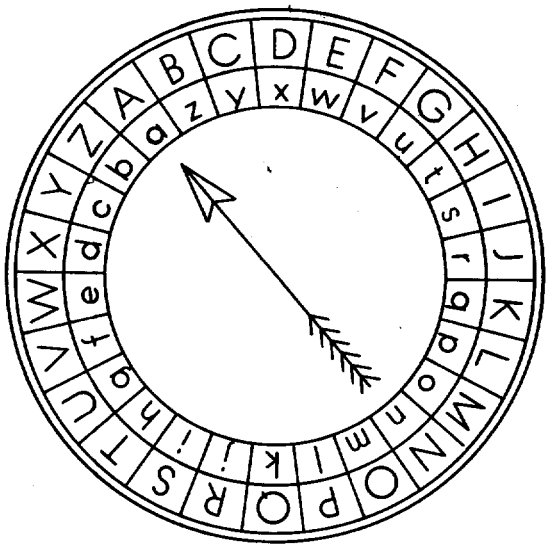
Transposition ciphers are limited to the characters of the original text. These characters are rearranged according to some predetermined plan or key.

Substitution ciphers may be made up of substituted letters, numerals, conventional signs, or combinations of all three, for the letters of the plain text.

If the text is in English, and the cipher is a transposition cipher, a count of the number of letters in the message will show that the vowels AEIOU constitute 40 percent of the whole; consonants LMRST 30 percent. and the consonants JKQXZ, 2 percent. If these proportions do not hold within 5 percent either way, the cipher is undoubtedly a substitution cipher.

By use of a cipher, important messages may be sent with a degree of secrecy. While it is well known that, to date, no practicable military cipher has been devised that is mathematically indecipherable, most military information rapidly loses its value, and it is for this reason that we encipher dispatches, thus hoping to delay the deciphering of the message by the enemy sufficiently for it to have lost its value.

The United States Army cipher disk consists of two plates of celluloid, on the larger of which a fixed alphabet is printed in a circle about the smaller circular plate, pivoted at the center, so that it may be rotated. Around the outer edge of the movable plate the alphabet is also printed, but in reverse order. Coincidence of any letter on the disk with that of any letter on the fixed plate is obtained by rotating the disk.



To place a message in cipher, using the United States Army cipher disk, and a key word, for example, GRANT, the work of enciphering would appear on the original sheet about as follows:

GRANT	GRANT	GRANT	GRANT	GRANT	GRANT	GRANT	GRANT
Enemy	massi	ngsix	teend	ivisi	onsne	arsoi	ssons
CEWBV	URIVL	TLIFW	NNWAQ	YWSVL	SEIAP	GAIZL	OZMAB

Set your cipher disk with A on the movable disk, opposite G on the fixed disk. Each letter of the plain text, under the letter G of the key word, can now be placed in cipher by reading its corresponding letter on the cipher disk. For example, opposite the letter E of ENEMY, on the movable disk, appears C on the fixed disk which is its cipher. Opposite M (of MASSING) is found U, etc. After all letters of the plain text appearing under G have been enciphered, reset your cipher disk with A on the movable disk opposite R, the second letter of the key word, on the fixed disk. Proceed as before, reading the plain-text letters from the movable disk, the cipher from the fixed, etc. Then reset the disk with A on the movable disk, opposite A on the fixed, continuing this operation until the enciphering of the message has been completed.

To decipher a message of this type the procedure is reversed:

GRANT	GRANT	GRANT	GRANT	GRANT	GRANT
BJJVA	SQRJR	NJFJM	GZZJP	TYADP	TRZLQ
First	objec	tiveh	asbee	ntake	nabcd

PLAYFAIR'S CIPHER

A key word is required in which no letter is repeated, and all the letters in the alphabet which do not occur in the key word are entered in the spaces of the square with 25 subdivisions, I and J being treated as similar letter.

With the key word "CLIQUE" the letters would be arranged as follows:

C	L	IJ	Q	U
E	A	B	D	F
G	H	K	M	N
O	P	R	S	T
V	W	X	Y	Z

The letters of the text are divided up into pairs and equivalents are found for each pair, instead of each letter.

Every pair of letters in the square must be—

(a) *In the same vertical line.*—Thus in the above example, each letter is represented in cipher by that which stands next below it, and the bottom letter by the top one of the same column; for instance, DY is represented by MQ.

(b) *In the same horizontal line.*—Each letter in this case is represented by that which stands next on its right, and the letter on the extreme right, by that on the extreme left of the same horizontal line; for instance, EF is represented by AE.

(c) *Or at opposite angles of some rectangle.*—Here the two letters are represented by the two which stand at the two remaining angles of the rectangle, each by that which is in the same horizontal line with it; for instance CM is represented by QG.

If, on dividing the letters of the text into pairs, a pair is found to be composed of the same letter repeated, a dummy letter such as X or Z should be introduced.

If the message to be sent were: "Local attacks of the enemy north of 'Lens' have been repelled," when divided into pairs it would be:

LO	CA	LA	TX	TA	CK	SO	FT	HE	EN	EM	YN	OR	TH	OF	LE	NS	HA
CP	LE	AH	RZ	PF	IG	TP	NZ	GA	FG	DG	ZM	PS	PN	TE	CA	MT	PH

VE	BE	EN	RE	PE	LX	LE	DX
CG	DA	FG	OB	OA	IW	CA	BY

Letters with dots over them are dummies;

Or if written in groups for transmission by signals:

CPLEA HRZPF IGTPN ZGAFG DGZMP SPNTE CAMTP HCGDA FGOBO AIWCA BY

To decipher the message the receiver divides it into pairs, and from his table finds the equivalents for these pairs; taking the letters immediately above each, when they are in the same vertical line; those immediately on the left, when on the same horizontal line; and those at opposite angles of the rectangle, when this can be formed.

Appendix 3.—USE OF PLAYFAIR SYSTEM FOR SECRET COMMUNICATION IN AEF

~~SECRET~~

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES.

~~SECRET~~

France, August 22, 1918.

30

MEMORANDUM:

Key words for use with Playfair Cipher, under the provisions of General Orders, No. 103, these headquarters, 26 June 1918, are announced, as follows:

From 3:00 a.m.	1 Sept.	to 3:00 a.m.	3 Sept.	....	YARMOUTH
" " "	3 Sept.	" " "	10 Sept.	....	BOSTON
" " "	10 Sept.	" " "	15 Sept.	....	ZODIAC
" " "	15 Sept.	" " "	18 Sept.	....	MADAGASCAR
" " "	18 Sept.	" " "	24 Sept.	....	CARANZA
" " "	24 Sept.	" " "	27 Sept.	....	MAGAZINE
" " "	27 Sept.	" further notice		....	SUWANEE

Commanders of lower units will be furnished "extracts" by division commanders as required.

In no case will the complete list be taken in advance of division headquarters.

Any suspicion that list has fallen into unauthorized hands will be reported by telegraph to these headquarters. Its use will be continued until receipt of new list.

Receipt of this list will be acknowledged by mail, giving number of copies received and condition of package on receipt.

Attention is invited to G.O. 103, these headquarters 1918, prescribing use of Playfair Cipher only in case of emergency.

By command of General Pershing:

ROBERT C. DAVIS,

Adjutant General.

Distribution:

1 Copy to Adjutant General's Code Office.
1 Copy to each Army, Army Corps and Division.

Appendix 4.—A FEW PAGES FROM ONE OF THE EARLY FRENCH CODES: CARNET RÉDUIT "OLIVE"

CARNET RÉDUIT

Téléphone - T.P.S. -- T.S.F. - Optique

SECRET

Nom du Carnet : **OLIVE**

Indicatif : **Q. Q. Q.**

Il est interdit de laisser aucun mot ou passage en clair dans les messages par T.S.F. ou T.P.S.

Brûlez ce Carnet s'il est en danger d'être pris

ALPHABET

AIC	A
AKE	A
AKI	B
ALB	B
ALD	C
ALG	C
ANO	D
ANP	D
ANS	E
APG	E
ARS	E
BIC	F
BKT	F
BLN	G
BLR	H
BNO	I
BNS	I
BOA	J
BOG	K
BOI	L
BOS	M
BPC	M
BPD	N
BPG	N
BPQ	O
BPR	P
BPS	Q
BQA	R
BSO	R
BSQ	S
BSS	S
CAR	T
CAZ	T
CBI	U
CBL	V
CBN	W
CCY	X
CDB	Y
CEF	Z
CIA	à
CIC	à la
CIZ	au
CKA	aux
CKB	dans
CKG	de
CKK	de la
CKO	des
CKS	du
CKZ	et
CLA	il
CLI	la
CLR	le
CLT	les
CME	leur
CMG	leurs
CMK	lui
CMM	ma
CMR	me
CMS	mes
CMT	mon
CMV	nos
CMX	notre
CMZ	nous
CNK	par
CNN	pour
DAB	vos
DBA	votre
DBD	vous

NOMBRES

DCD	0 ou nul
DCG	1 ou premier
DCK	2
DCO	3

NOTE.—It would appear that the original intention of using, OOO as the indicator for this *carnet* had to be changed, for the original shows the letter *O* to have been modified, by hand, to *Q.*—*W.F.F.*

QZD	longueur d'ondes
RAP	masque
RAT	matin
RAZ	mauvais (mal)
RCK	médecin
RCN	minenwerfer
RCP	nuit
RDB	observation
RDE	observatoire
REE	occupation
REL	officier
REN	opération
SAR	ordre
SBS	outils
SCK	pertes
SCT	pigeon voyageur
SDE	piquet de terre
SDI	possible
SDR	poste d'écoute
SET	poste émetteur de T. P. S.
SFI	poste récepteur de T. P. S.
SFO	poste mixte de T. P. S
SFY	poste émetteur de T. S. F
SGT	poste récepteur de T S F
SGK	poste optique
SGS	prisonnier
SHO	régiment
SHP	relève
SHQ	réponse
SHS	réseau
SH	réserve
SIO	signaleur de 14 c/m.
SIP	signaleur de 24 c/m.
SKO	situation
SKV	soir
SLY	sous-officier
SLZ	tableau à 4 directions
SMM	tableau à 12 directions
SMO	torpille
SMT	troupe
SMY	tube ou lampe à vide
SNF	tué
SNG	urgent
SNL	vivres

PHRASES TOUTES FAITES

SNV	abritez tout le monde sauf les guetteurs
SOP	alerte
SOV	alerte aux gaz
TAR	attaque dans conditions convenues
TAT	attaque ennemie paraît avoir échoué
TAV	attaque partie
TBK	avez-vous besoin de
TBV	char d'assaut ami
TCF	char d'assaut ennemi
TDI	combat à la grenade en
TEG	compte-rendu écrit va être envoyé
TEK	donnez moi des renseignements (sur)
TEN	en panne
TER	front actuel passe par
TGE	indices d'attaque ennemie en
TGP	infanterie ennemie attaque
THI	infanterie ennemie a atteint
THS	infanterie ennemie progresse dans boyaux
THV	infanterie ennemie se replie
UAA	je n'ai pas de renseignements sur
UAR	je vous envoie matériel demandé
UAV	liaison assurée avec
UBJ	n'envoyez plus de messages chiffrés
UBK	nous avons évacué
UCO	nous avons occupé
UDV	nous avons réoccupé
UDZ	nous nous replions (sur)
UFI	nous occupons sûrement
UFL	nous paraissons occuper
UGB	nous progressons vers
UGD	nous sommes arrêtés en
UHI	objectif atteint
VAB	objectif non atteint
VAK	ordre en voie d'exécution
VAL	où passe la première ligne ?
VAT	pas de liaison avec

VBB	patrouille rentrée
VBD	patrouille sortie
VKK	patrouille va sortir
VKS	placez (ou complétez) la chaine des coureurs
VSE	première ligne passe par
VSK	préparation d'artillerie paraît suffisante
VTA	préparation d'artillerie paraît insuffisante
VTT	quel est le secteur bombardé ?
VTU	que se passe-t-il sur vo re front? (ou vers)
YAA	relève aura lieu
YAD	relève n'aura pas lieu
YAT	relève commencée
YBI	relève en cours
YCC	relève terminée
YCE	renforts ennemis arrivent par
YCF	rien à signaler
YDE	situation rétablie
YGG	surveillez attentivement
YHA	suspendez l'exécution de l'opération

OFN	pont
OFV	position
OGE	quartier
OHA	ravin, vallée
OHT	rivière, ruisseau
OHY	route, chemin
OME	secteur
OMK	tranchée
ONT	trou organisé
ONI	voie ferrée

INFANTERIE

OPA	assaut
OPB	bataillon
OPK	B. C. P.
OPM	canon de 37
ORS	compagnie
ORU	grenade
OSI	I. D. (ou Brigade)
OSK	mitrailleuse
OSN	mortier de 75
OSV	mortier Stokes
OTE	nettoyeurs
OTK	patrouille
OTN	pionnier
OTP	reconnaissance
OTY	renfort
PAE	réserve
PAJ	travailleurs
PAS	troupes d'assaut
PBI	section
PBT	demi section
PBY	soutien
PCO	vague

ARTILLERIE

PCQ	artillerie de campagne (A. C.)
PDE	artillerie lourde (A. L.)
PDL	artillerie de tranchée (A. T.)
PDO	artillerie d'assaut (A. S.)
PDP	artillerie amie va tirer sur
PEI	artillerie amie tire sur
PEK	artillerie amie a fini de tirer (sur)
PET	artillerie ennemie va tirer sur
PFI	artillerie ennemie tire sur
PFR	artillerie ennemie a fini de tirer sur
PFT	batterie
PFZ	bombardement
PGA	bombardement par obus toxiques sur
PGE	casemates
PGK	cesser le feu
PHI	contre avion
PHT	contre char d'assaut
PHZ	fusées fusantes
PKO	fusées percutantes
PKT	instantanées
PLE	observez le tir (sur)
PLG	obus toxiques
PLL	obus lacrymogènes
PME	obus à balles
PNF	obus explosifs
PNA	pièce
PND	tir trop court
PNK	tir trop long
PNL	tir trop à droite
PNT	tir trop à gauche
POO	tir de barrage (sur)
POS	tir de contre préparation sur
POV	tir d'efficacité
POY	tir de harcèlement
PPE	tir d'interdiction
PPG	tir de réglage
PPK	tir de représailles (sur)
PPS	tir de surprise (sur)
PQE	tir sur artillerie en)
PQK	tir sur minenwerfer (en)
PQT	tir sur mitrailleuses

MOTS USUELS

PRE	accumulateurs
PRF	id. de 4 volts
PRT	id. de 10 volts
PRY	id. de 40 volts
PSC	aile
PSF	agent de liaison
PSK	ami
PSS	amplificateur
QAI	antenne
QAS	appareil téléphonique
QAV	artifices
QBI	artillerie
QBT	assortiment
QCE	attaque
QCK	aujourd'hui
QCO	avion
QDI	batterie de piles
QDN	blessé
QEF	bon (ne)
QEL	brancardier
QEV	câble de campagne
QFI	câble léger
QFS	capitaine
QFV	cartouches 86
QFY	cartouches D. A. M.
QGE	casque téléphonique
QGH	cavalerie
QHC	certain (ement)
QHI	char d'assaut
QKE	colonel
QKG	combat
QKP	commandant
QLE	contre-attaque
QLO	corps d'armée
QLY	coup de main
QNI	critique
QMK	défense
QMN	dégâts matériels
QMT	demain
QMZ	demande
QOE	disparu
QOH	disponible
QOK	distance
QOR	division
QOV	douteux
QPE	eau
QPK	ennemi
QPN	escadron
QPP	exécution
QQA	général
QQF	génie
QRB	gradé
QRD	grillage de prise de terre
QRE	groupe
QRH	guide
QRT	hier
QSA	homme
QSS	immédiatement
QST	impossible
QSZ	infanterie
QXI	intact
QXY	lieutenant
QYI	ligne
QYN	ligne ou circuit téléphonique
QYS	ligne enterrée
QZC	ligne en caniveau

DCS	4
DCV	5
DDE	6
DDF	7
DDK	8
EAR	9
EAZ	10
EBI	11
EBR	12
EBZ	13
ECA	14
ECF	15
ECK	16
ECR	17
ECT	18
EDR	19
EDZ	20
EEI	30
EEM	40
EET	50
EFG	60
EFI	70
EFT	80
EGL	90
EGO	100
EHK	1000
EIR	...ième
EIU	...ième

VERBES

EIZ	abandonner
EKA	accepter
EKD	achever
EKG	adresser
ELB	ajourner
ELD	aller
ELK	apercevoir
ELL	appuyer
EMC	arreter
EMJ	attaquer
EMN	atteindre
EOE	attendre
EOR	avancer
EOZ	avoir
EQA	bombarder
EQR	cesser
EQS	commencer
ERC	completer
ESI	conduire
ESL	conserver
ESO	continuer
ESS	déborder
ETE	déboucher
ETG	décider
ETK	défendre
EUI	demander
EUV	détruire
FAR	diriger
FAT	échouer
FAZ	entendre
FCZ	envoyer
FDV	être
FEI	évacuer
FER	exécuter
FET	faire
FIO	faire connaître
FIX	guider
FKA	laisser
FKR	manquer
FKT	mettre
GAI	occuper
GAS	opposer
GAT	ordonner
GBA	organiser
GBO	paraître
GBV	placer
GCI	préparer
GCR	recevoir
GCT	réduire
GCV	rentrer
GDD	répondre
GEA	repousser
GFG	rétablir
GHA	réussir
GLZ	sortir
GMI	surprendre
GNO	téléphoner
GPA	terminer
GPR	transmettre
GPT	trouver
GRU	utiliser
GSC	voir

TEMPS DE VERBES

GSD	présent
HAA	passé
HAR	futur
LMT	impératif

MESURES

NAE	coordonnées
NAK	grand, important
NAN	heure
NBO	jour
NBR	kilomètre
NBT	mètre
NCI	minute
NCK	petit, faible

ORIENTATION

NCV	à droite
NDE	à gauche
NDK	à queue
NDO	à tête
NDR	allant vers
NEG	au centre
NEK	derrière
NES	devant
NFT	direction de
NGA	est
NGK	nord
NGN	ouest
NKV	sud
NKX	venant de

INDICATION DE LIEUX

NKZ	abatis
NLH	abris
NLR	bois
NLT	boyau
NOB	canal
NOK	carrefour
NOV	carrière
NRF	centre de résistance
NRR	cimetière
NSC	coupe
NSE	crête
OAR	église
OAT	entrée
OCE	ferme
OCN	gare
ODE	lisière
ODI	ouvrage
ODV	P. C.
OEG	parallèle de départ
OES	parallèle de surveillance
OFK	parallèle principale
OFL	parallèle de soutien

Appendix 5.—A FEW PAGES FROM THE FRENCH CARNET RÉDUIT "URBAIN"

N°

NOM DE CE CARNET

URBAIN

U. U. U.

SECRET

Carnet Réduit

L'Autorité à laquelle est délivré ce Carnet en reste **propriétaire**, *tant qu'elle demeure sur le territoire de l'Armée, qu'elle soit en secteur ou au repos.*

Elle en est responsable.

Elle doit le restituer *à l'autorité qui le lui a remis lorsqu'un nouveau Carnet est mis en service ou lorsqu'elle quitte le territoire de l'Armée.*

REMARQUE IMPORTANTE : *Ne pas oublier de parcourir ce Carnet avec grand soin dès que vous l'aurez reçu.*

VIIIe ARMÉE

3e BUREAU

ET

= CHIFFRE =

SECRET

CARNET RÉDUIT

NOM

DU PRÉSENT CARNET :

URBAIN - U. U. U.

Ce document est **secret.**

Le brûler s'il est en danger d'être pris.

S'il vient à disparaître, en aviser **immédiatement** l'Autorité Supérieure.

Il doit toujours être en la possession de celui qui, **même momentanément**, commande l'unité pour les besoins de laquelle l'autorité supérieure l'a établi.

Ex. : Un Officier partant en permission, etc..., devra le remettre à son remplaçant provisoire.

CHIFFREMENT

1re PARTIE DU CARNET

Les messages doivent être remis chiffrés au Personnel chargé de leur transmission.

Toujours chiffrer plusieurs mots successifs. - Relire ensuite le message et s'assurer que les mots restés en clair ne font pas deviner la signification des passages chiffrés. - **Quand c'est possible, mieux vaut tout chiffrer.**

Voici les procédés à employer pour chiffrer correctement les différents messages que le Commandement peut avoir à transmettre :

1° MESSAGE TÉLÉPHONÉ

Le commencer par le nom du carnet en clair :

AVEC LE PRÉSENT CARNET CE SERA : URBAIN

Puis substituer à chaque lettre, mot ou phrase que l'on veut chiffrer **le groupe de 3 chiffres** placé en regard dans le tableau de chiffrement.

2° MESSAGE par T. S. F., T. P. S., OPTIQUE, etc.

Le commencer par la lettre initiale du nom du carnet répétée 3 fois :

AVEC LE PRÉSENT CARNET CE SERA : U. U. U.

Puis substituer à chaque lettre, mot ou phrase que l'on veut chiffrer **le groupe de 3 lettres** placé en regard dans le tableau de chiffrement.

3° MESSAGE par P. V.

Utiliser dans toutes leurs prescriptions l'un ou l'autre de ces deux procédés, mais dans un même message, ne jamais mélanger de groupes de 3 chiffres à des groupes de 3 lettres.

DÉCHIFFREMENT 2° PARTIE DU CARNET

Les groupes de 3 lettres ou de 3 chiffres sont classés par ordre alphabétique ou numérique. Les recherches sont donc faciles.

Le déchiffrement est fait par l'Autorité destinataire.

Les **erreurs,** toujours possibles, ne portent généralement que sur un chiffre ou sur une lettre. On trouvera facilement le groupe exact en remplaçant successivement chacun des trois caractères par les autres caractères employés, chiffres ou lettres.

Exemple : on a reçu le groupe 124 au lieu de 127. En remplaçant le 4 par 1, 2, 3, 5..... 9, on aura nécessairement rencontré 127, qui donne le sens voulu.

Aux éléments qui, du fait de leur mission, sont particulièrement exposés (tels que les unités prenant part à un coup de main, les chars d'assaut ou les avions munis d'un poste récepteur de T. S. F., etc.), il est **rigoureusement prescrit** de **ne confier** qu'un **extrait** du présent carnet. L'Autorité qui doit correspondre avec les dits éléments déterminera, dans chaque cas particulier, la composition de cet extrait.

N'oubliez jamais que l'ennemi vous écoute

TABLEAU DE CHIFFREMENT

		ALPHABET			NOMBRES
DQA	162	A.	MYU	554	0 ou nul.
BJG	059	A.	JGZ	340	1 ou premier.
JDF	326	B.	PFT	677	2
KUM	420	C.	LPX	473	3
NWB	597	D.	BKO	061	4
RGA	835	E.	EXM	192	5
DY	207	E.	NFJ	565	6
AF	667	E.	OJL	626	7
RWQ	863	F.	QMU	790	8
MRB	543	G.	RQG	855	9
JWP	368	H.	FKC	219	10
FSZ	228	I.	AGR	012	11
BYK	093	I.	IYA	313	12
KEV	387	J.	MUR	546	13
QBN	746	K.	QXI	811	14
OVK	653	L.	MFR	514	15
PMC	707	M.	FKH	212	16
LUB	484	N.	DFG	139	17
AQU	026	N.	CLN	111	18
HAP	298	O.	FZK	239	19
NAB	558	P.	KNO	406	20
CMR	112	Q.	NXP	598	30
DXA	180	R.	PNY	710	40
OAU	607	S.	QAL	742	50
QVL	808	T.	NOR	582	60
SPY	872	U.	DPV	161	70
GUB	279	V.	AUQ	030	80
AXG	036	W.	BSO	076	90
POR	715	X.	GLB	267	100
FAB	196	Y.	BZD	094	1000
HZK	306	Z.	JLR	353	....ième.
			QFK	759	....ième.
LEF	447	à.	LFQ	449	leur.
PTV	728	à la.	FBW	200	leurs.
BDK	047	au.	AKX	016	ma.
DCM	136	aux.	DVQ	173	mon.
KRD	417	de.	CPD	115	mes.
QLB	786	de la.	MJW	525	nos.
FUA	231	des.	NSC	591	notre.
CJL	108	du.	QRV	798	vos.
KLF	400	et.	KYN	428	votre.
PJU	697	la.	DZJ	186	nous.
MDQ	509	le.	BGV	052	vous.
GBF	242	les.	NJX	572	il (s).
HXA	304	lui.	PXN	737	pour.

VERBES et quelques Substantifs dérivés de ces Verbes

GJY	262	Abandonner ou Abandon.
EPX	189	Accepter.
CBP	097	Achever.
LIP	456	Adresser.
NKP	573	Ajourner.
JIP	396	Aller.
PVA	730	Apercevoir.
RUN	859	Appuyer.
DLZ	151	Arrêter ou Arrêt.
BVN	085	Atteindre.
MAZ	499	Attendre ou Attente.
ODK	614	Avancer ou Avance.
FIP	214	Avoir.
IBM	307	Bombarder.
GPL	274	Cesser.
ADF	006	Commencer.
MUW	548	Compléter.
LSY	480	Conduire.
QOP	795	Conserver.
RWZ	864	Continuer.
AZM	040	Déborder.
UZR	900	Déboucher.
WZP	934	Décider.
JEP	331	Demander.
FKQ	220	Détruire ou Destruction.
BLC	062	Diriger ou Direction.
NGK	569	Echouer.
FMK	225	Entendre.
QSD	799	Envoyer.
TZU	884	Etre.
GLK	269	Exécuter ou Exécution.
AYN	037	Faire.
WDF	920	Faire connaitre.
PGH	685	Guider ou Guide.
KAM	373	Laisser.
UFC	889	Manquer ou Manquant.
CRA	118	Mettre.
PDV	673	Occuper ou Occupation.
UPA	894	Opposer ou Opposition.
ZLO	987	Ordonner.
PCN	669	Organiser ou Organisation.
VNP	909	Paraitre.
LGH	452	Placer ou Place.
AFQ	010	Préparer ou Préparation.
LWD	489	Recevoir.
WRZ	928	Réduire.
BWL	086	Rentrer.
FWR	233	Repousser.
KUB	418	Résister ou Résistance.
PQD	716	Rétablir.
ZTV	991	Réussir.
LXK	492	Sortir.
ONP	634	Surprendre ou Surprise.
JMA	356	Téléphoner ou Téléphone.
CQA	117	Trouver.
RNP	850	Utiliser ou Utilisation.
RAL	821	Voir.
UAR	885	Faut-il.
ZFL	975	Transmettez.

Temps de Verbes

PKN	699	Présent.
KOX	411	Passé.
BPF	069	Futur.
MZD	556	Impératif.

MESURES

NZC	955	Coordonnées.
ACP	004	Demi.
QHR	768	Grand, important.
LAX	436	Heure.
VWD	916	Jour.
TPA	876	Kilomètre.
RHM	840	Minute.
GFM	254	Mètre.
MVK	549	Petit, faible.
DNY	155	Quart.

ORIENTATION

QCX	748	
VFI	904	à.
XQR	944	Allant vers.
RBX	823	Au centre.
LMX	461	Dans.
ALC	018	Derrière.
JAG	317	En arrière (de).
YMS	963	Devant.
PRS	718	En avant (de).
OGV	621	Direction (de).
GXJ	287	(à) Droite.
ZKN	983	Est.

BHA	053	Obus lacrymogènes.
GHO	258	Obus à balles.
URB	895	Obus explosifs.
QKN	780	Pièce.
PIL	603	Réglage.
OEP	617	Tir trop court.
KBV	377	Tir trop long.
CDK	099	Tir trop à droite.
KFQ	391	Tir trop à gauche.
JKD	348	Tir de barrage (sur).
RJV	843	Tir de représailles (sur).
QA	912	Tir de contre-préparation (sur).
DAK	132	Tir de surprise (sur).
ARC	029	Tir d'interdiction.
KVJ	423	Tir de harcèlement.
DWB	178	Tir sur artillerie (en).
LJM	459	Tir sur minenwerfer (en).
RVD	861	Tir sur mitrailleuses (en).
QWP	810	Tir de réglage.
YXA	968	Tir d'efficacité.

MOTS USUELS

NKW	575	Accumulateurs.
FCA	201	Aile.
PLO	700	Agent de liaison.
GKZ	263	Ami.
BIZ	057	Artifices.
YDA	956	Assortiment.
PZF	740	Attaque ou Attaquer.
DTX	170	Attention.
LTZ	481	Aujourd'hui.
JKO	349	Avion.
FRC	227	Blessé.
CIX	105	Bon, Bonne.
ROU	851	Brancardier.
QTV	803	Capitaine.
OYR	660	Cartouches 86.
MQN	541	Cartouches D.A.M.
LYA	496	Cavalerie.
VRM	913	Certain (ement).
ORF	641	Char d'assaut.
KQA	416	Colonel.
BRJ	301	Combat.
CVH	123	Commandant.
AEV	009	Contre-attaque.
GYS	290	Corps d'Armée.
DGW	140	Coup de main.
JXC	369	Coureur.
NDR	562	Critique.
UVO	896	Cuisine.
ZDF	972	Défense, Défensif ou Défendre.
LOU	465	Demain.
MXI	553	Demande ou Demander.
QGD	766	Disparu.
JOW	361	Distance.
DLA	150	Division.
QDI	752	Douteux.
WXA	931	Eau.
RFA	829	Ennemi.
XUR	948	Fatigue ou Fatigué.
NQF	586	Français.
JDG	328	Fumée.
DBU	133	Fusil.
FVB	232	Gaz.
SDV	868	Général.
PUR	729	Génie.
GVO	283	Grade.
WPK	927	Hier.
QYM	816	Homme.
MEJ	513	Immédiat (ement).
OWB	657	Intact.
NZA	604	Liaison.
XLB	940	Lieutenant.
RFN	833	Ligne.
MLR	532	Masque.
DYF	183	Matin.
KCO	380	Mauvais, mal.
VDO	903	Médecin.
YJN	961	Menace (sur).
RSP	856	Mine.
NRV	588	Minenwerfer.
DXL	182	Nombre, Nombreux.
AMD	021	Nuit.
EQW	191	Offensif ou Offensive.
IJQ	308	Officier.
LVM	488	Ordre.
OPG	635	Outils.
OCB	611	Pigeons-voyageurs.
RCZ	824	Poste d'écoute.
WBK	919	Poste optique.
UBK	888	Pots Ruggieri.
YPN	964	Prisonnier.
OKW	628	Progression.
MGU	519	Projecteur.
JVN	367	Rassemblement ennemi (vers...).
GMZ	270	Ravitaillement.
DMR	152	Relève ou Relever.

TABLEAU DE DÉCHIFFREMENT

ABJ	003	Attaque ennemie paraît avoir échoué.	CBP	097	Achever.
ACP	004	Demi.	CDK	099	Tir trop à droite.
ADF	006	Commencer.	CFA	101	Canal.
AEV	009	Contre-attaque.	CGU	102	Barrage.
AFQ	010	Préparer ou Préparation.	CIX	105	Bon, bonne.
AGR	012	11.	CJL	108	Du.
AB	013	Mortier de 75.	CKS	109	B. C. P.
AKX	016	Ma.	CLN	111	18.
ALC	018	Derrière.	CMR	112	Q.
AMD	021	Nuit.	CPD	115	Mes.
AOY	022	Entrée.	CQA	117	Trouver.
APK	023	Renfort.	CRA	118	Mettre.
AQU	026	N.	CSQ	119	Demandons.
ARC	029	Tir d'interdiction.	CUM	122	Carrefour.
AUQ	030	80.	CVH	123	Commandant.
AVJ	034	Fusee (s) fusante (s).	CWJ	125	Prière de vérifier ou de faire vérifier le chiffrement du télégramme N°
AWO	035	Secteur.			
AXG	036	W.	CXG	127	Abritez tout le monde sauf les guetteurs.
AYN	037	Faire.			
AZM	040	Déborder.	CYK	128	Nord.
BAJ	043	Artillerie de campagne.	CZO	131	Abatis.
BCF	044	Antenne.	DAK	132	Tir de surprise (sur...)
BDK	047	Au.	DBU	133	Fusil.
BEZ	048	I. D. ou Brigade.	DCM	136	Aux.
BFL	049	Réseau.	DFG	139	17.
BGV	052	Vous.	DGW	140	Coup de main.
BHA	053	Obus lacrymogènes.	DHJ	144	Crête.
BIZ	057	Artifices.	DKP	146	Char d'assaut ennemi.
BJG	059	A.	DLA	150	Division.
BKO	061	4.	DLZ	151	Arrêter ou arrêt.
BLC	062	Diriger.	DMR	152	Relève ou relever.
BMN	064	Relève aura lieu.	DNY	155	Quart.
BOR	068	Nettoyeurs.	DOF	158	Alerte.
BPF	069	Futur.	DPV	161	70.
BQY	072	Régiment.	DQA	162	A.
BRZ	073	Attaque partie.	DRY	167	Grenade.
BSO	076	90.	DSW	169	Artillerie ennemie tire(sur)
BTV	077	Soutien.	DTX	170	Attention.
BUA	082	Artillerie.	DUK	171	Impossible augmenter énergie.
BVN	085	Atteindre.			
BWL	086	Rentrer.	DVQ	173	Mon.
BXG	089	Rivière, ruisseau.	DVW	175	Nous progressons (vers..)
BXW	091	Vague.	DWB	178	Tir sur artillerie (en...)
BYK	093	I.	DXA	180	R.
BZD	094	1000.	DXL	182	Nombre, nombreux.
CAW	096	Contre-chars d'assaut.	DYF	183	Matin.

Appendix 6.—EXTRACTS FROM A TWO-PART FRENCH FIELD CODE OF APPROXIMATELY 2,300 GROUPS

SECRET

EXEMPLAIRE

N° [redacted]

Tout militaire qui reçoit ou qui trouve ce Code est prié de lire les recommandations importantes figurant à la page V des Instructions.

CODE CHIFFRÉ

SÉRIE 65

Veillez sur ce Code.

Tâchez de le brûler s'il court le risque d'être pris.

MINISTÈRE
DE LA GUERRE.

CABINET
DU MINISTRE.

SECTION DU CHIFFRE.

SECRET

INSTRUCTION

SUR L'EMPLOI

DU CODE CHIFFRÉ.

Chaque mot ou expression se chiffre par un groupe de quatre chiffres.

Exemples : **SOIXANTE** se chiffre par **9518** ;
TERRAIN se chiffre par **3739**.

Si un mot se présente plusieurs fois, on le chiffre chaque fois différemment, soit en utilisant successivement les groupes placés en regard dans la table de chiffrement, soit en le décomposant au moyen de radicaux.

Exemples : **PATROUILLE** peut se chiffrer par **8749, 6884, 7311.**

ou : **PA TR OU ILLE.**
4620 7663 8817 0773

Il est expressément interdit de laisser, dans un même message, des parties en clair et des parties chiffrées.

Un message téléphoné, ou transmis par T. P. S., T. S. F. ou par télégraphie optique, doit être entièrement chiffré.

Exceptionnellement, si on n'a pas le temps de le chiffrer entièrement, on le transmettra en clair.

Tous les messages transmis par T. S. F. et aussi tout autre message particulièrement secret ou important doivent subir un **DOUBLE CHIFFREMENT** fait au moyen du tableau de concordance joint au Code.

Pour le double chiffrement, substituer un bigramme de lettres, *au premier chiffre* du premier groupe, et continuer à constituer un bigramme de lettres à toutes les tranches de deux chiffres qui suivent :

Exemple : **0|75|0 8|75|0 8|39|9 2|73|7.**

Les groupes de quatre chiffres se trouvent ainsi enchaînés dans les bigrammes de substitution.

Faire emploi des groupes nuls qui sont à la fin des radicaux pour commencer ou finir les télégrammes, pour encadrer les noms propres syllabés, pour indiquer une séparation de mots syllabés, etc.

Utiliser, le plus possible, les phrases toutes faites.

RECOMMANDATIONS IMPORTANTES.

Ce Code doit être l'objet d'une surveillance constante.

Éviter de l'emporter dans les missions dangereuses.

Le détruire, sans hésitation, s'il est en danger d'être pris.

Si un Code a disparu, en aviser l'autorité supérieure.

TEMPS DE VERBE.

0009	Présent.
3717	
9673	
6015	
0999	
7158	Passé.
3003	
1170	
4806	
5106	
8562	Futur.
4531	
2538	
2606	
5079	
8773	Conditionnel présent.
3323	
4253	
2662	
6328	
8000	Impératif.
4737	
8061	
7580	
9921	
6309	Participe présent.
1950	
9996	
8210	
7574	
3317	Participe passé.
1571	
5769	
3500	
7563	
1176	

PONCTUATION.

5609	Point (.).
2365	
7165	
5241	Point (.).
3667	
2139	Point d'interrogation (?).
8500	
5391	
6100	
4817	
8271	Deux points (:).
3191	
6470	
1907	
8711	
5980	Virgule (,).
9991	
3376	
4342	
0067	
1500	Parenthèse ( ).
7424	
8173	
1014	
9264	

NOMBRES (numéraux et ordinaux).

5360	un.
2032	
7419	
3171	deux.
0721	
5216	
9358	trois.
2599	
1050	
7021	quatre.
3849	
7862	
6267	cinq.
1314	
7414	
5634	six.
0228	
4650	
2250	sept.

3213	sept.
4269	
8650	huit.
6618	
4079	
0250	neuf.
3391	
9049	
5514	dix.
4594	
1261	onze.
9950	
7505	douze.
1356	
7649	treize.
6129	
2206	quatorze.
8573	
6071	quinze.
9216	
0838	seize.
8986	
3759	dix-sept.
5222	
8812	dix-huit.
1684	
0516	dix-neuf.
2341	
4114	vingt.
4876	
8348	vingt et un.
5028	— — deux.
7032	— — trois.
3560	— — quatre.
5376	— — cinq.
8407	— — six.
6033	— — sept.
9580	— — huit.
6356	— — neuf.
4122	trente.
7330	——— et un.
5681	——— deux.
9281	——— trois.
3236	——— quatre.
2010	——— cinq.
4509	——— six
7892	——— sept.
2235	——— huit.
6565	——— neuf.
4228	quarante.

8648	quarante et un.
3639	——— deux.
9500	——— trois.
5099	——— quatre.
1949	——— cinq.
7259	——— six.
2120	——— sept.
0077	——— huit.
8761	——— neuf.
3512	cinquante.
4442	——— et un.
2936	——— deux.
9131	——— trois.
1549	——— quatre.
3950	——— cinq.
3219	——— six.
9420	——— sept.
0049	——— huit.
3862	——— neuf.
9518	soixante.
4971	——— et un.
2579	——— deux.
5542	——— trois.
4314	——— quatre.
5800	——— cinq.
8385	——— six.
6290	——— sept.
1145	——— huit.
8328	——— neuf.
0596	soixante dix.
2113	——— et onze.
6636	——— douze.
4957	——— treize.
5579	——— quatorze.
1607	——— quinze.
0000	——— seize.
7765	——— dix-sept.
3204	——— dix-huit.
6760	——— dix-neuf.
1750	quatre-vingts.
7617	——— un.
5860	——— deux.
7700	——— trois.
8617	——— quatre.
0667	——— cinq.
9741	——— six.
5668	——— sept.
3569	——— huit.
9044	——— neuf.
1250	quatre-vingt-dix.

N° 65.

4212	quatre-vingt-onze.
8950	quatre-vingt-douze.
2761	quatre-vingt-treize.
6829	quatre-vingt-quatorze.
7776	quatre-vingt-quinze.
8350	quatre-vingt-seize.
2319	quatre-vingt-dix-sept.
3414	quatre-vingt-dix-huit.
6963	quatre-vingt-dix-neuf.
4011	cent.
2380	——
5399	——
3831	——
2023	deux cents.
1280	——
1209	trois cents.
0632	quatre cents.
4574	cinq cents.
0383	mille.
5188	dix mille.
1971	vingt mille.
7222	quatre-vingt mille.
9750	deux cent mille.
8983	premier.
4037	première.
0570	ième.
9842	ieme.
5123	ieme.
7141	ième.

9031	heure 1/4.
1369	heure 1/4.
6278	heure 1/2.
8083	heure 1/2.
7519	heure 3/4.
2567	heure 3/4.
3823	heure H.
6668	heure H.
8144	heure H.
4999	janvier.
6500	février.
7093	mars.
8899	avril.
9949	mai.
0265	juin.
3047	juillet.
7245	août.
9864	septembre.
8970	octobre.
6923	novembre.
9141	décembre.
1193	lundi
1778	mardi.
5012	mercredi.
7871	jeudi.
9608	vendredi.
9689	samedi.
1992	dimanche.
3637	1915.
7049	1916.
0500	1917.
8239	1918.
2950	1919.
3800	1920.

DIVISIONS DU TEMPS.

6522	heure.
0700	heure.

RADICAUX.

1412	A.
6548	—
0370	—
4612	—
5280	ab.
1923	able.
5250	ablement.
0757	ac.
9053	ache.
8877	act.
2750	action.
9066	ad.
8050	af.
2483	ag.
3733	age.
6094	agi.
1030	ai.
7689	aie.

3077	aient.	7228	ber.	7283	cle.
8856	air.	5878	berg.	5656	co.
5233	aire.	2249	bi.	5155	com.
2832	ais.	4245	bien.	1362	comb.
1760	aison.	6234	bil.	6486	comp.
6729	ait.	7679	bl.	8476	con.
0039	aite.	1003	bla.	7190	cons.
4374	al.	0031	ble.	6373	consi.
2174	alt.	8724	blement.	3612	contre.
0917	ale.	4700	bo.	6882	cor.
4182	alement.	7750	bon.	8110	cou.
0555	am.	1733	bor.	7275	court.
3650	amment.	3686	bou.	5321	cr.
5727	an.	2850	bourg.	2619	cra.
7950	ance.	9545	br.	2150	cre.
5480	ans.	4028	bra.	3312	cro.
6450	ant.	8278	bre.	7605	ct.
1720	ante.	5899	burg.	3127	ction.
9600	anti.	8556	by.	1811	cu.
3335	ap.			4425	cul.
4630	ar.			5132	cur.
2709	art.			4717	cy.
8421	as.	7178	C.		
6600	asse.	5500	—		
8978	at.	9179	—		
1787	ate.	6446	ca.	0374	D.
4100	ateur.	3984	cal.	9999	—
9376	ati.	7980	can.	3520	—
7667	ation.	0978	car.	4918	da.
0865	au.	6889	cas.	9235	dan.
5790	aus.	7004	cat.	5309	dant.
3149	aut.	9015	cation.	6369	dar.
2737	aux.	4839	ce.	3540	dd.
5913	av.	3815	cen.	9968	de.
0950	ave.	8517	ces.	4006	—
3178	ay,	2868	cet.	5220	—
6851	az.	5461	cette.	4172	dec.
		4856	ceux.	5568	del.
		2773	ch.	3279	den.
		1450	cha.	5274	dens.
3029	B.	0357	champ.	0327	dent.
0800	—	6339	char.	8467	der.
9100	—	9964	che.	8515	des.
8999	ba.	1117	cher.	3300	——
4137	bach.	7316	chr.	4778	——
1625	bad.	2958	ci.	0474	deur.
1391	ban.	5527	cie.	7851	deux.
8900	bant.	0058	cien.	0536	di.
2964	bat.	7400	cl.	3854	dis.
6998	be.	4050	cla.	3960	dit.

0707	une.	6378	vice.	3694	X.
9704	uni.	5850	vie.	9152	—
2954	up.	8212	vient.	6737	xe.
8904	ur.	4714	viller.	9009	xel.
5840	ure.	6704	villers.	9270	xer.
3776	ury.	3431	villiers.	8612	xi.
9753	us.	2592	vo.		
8354	ut.	1959	von.		
4615	ux.	1770	vons.		
		0954	vont.	8653	Y.
		2861	vou.	8159	ya.
		2900	vous.	5611	yais.
6661	V.	4367	vr.	7715	yait.
8399	—	2224	vre.	2002	yant.
3302	va.	5265	vri.	6560	ye.
7327	vai.	8263	vu.	0023	yeni.
0508	vais.			5259	yer.
6388	vait			3344	yo.
2290	val.				
7386	vant.	8507	W.		
5828	ve.	7781	—		
7367	veau	5318	wa.	6900	Z.
6400	ven.	2729	we.	9952	za.
8850	vent.	7772	wei.	3679	ze.
7013	ver.	8979	wo.	9368	zo.
4731	ves.				
9855	vi.				

GROUPES NULS.

2684	groupe nul.
5450	———
1437	———
0532	———
4471	———
8989	———
1643	———
3700	———
1961	———
4308	———
3868	———
9338	———
3259	———
2914	———
9831	———
4758	———
1665	———
6533	———

VOCABULAIRE.

8112	**à.**
5261	–
0213	–
7567	à quelle heure.
6909	A. C.
1184	à cause.
6363	à ce.
7104	à ce sujet.
2194	à cette.
7286	à destination de.
5715	à fond.
8510	à l'.
3792	à la.
4320	à la date du.
9307	à la tête de.
4688	à l'effectif de.
5894	à leur.
3659	à ma disposition.
8302	à temps.
6249	à titre de.
5277	à tout prix.
2156	abandon (ner .
7154	**abatis.**
4520	abord.
1008	**abri.**
6657	absence.
7787	**absolu.**
0614	absolument.
5354	**accélérer.**
8497	accepter.
3041	**accident.**
1708	accomplir.
4014	accord.
9982	accord avec (d').
2557	accrochage.
2512	**accumulateur.**
3407	accuser réception.
8042	action.
1416	**activité.**
0267	actuellement.
6616	A. D.
1672	**adjudant.**
5575	adresser.
5414	**aéronautique.**
6982	**aéroplane.**
0763	**aérostiers.**
1169	afin de.
4215	**agricole.**
7172	**aile.**
1916	**ailerons.**
2561	**ainsi que.**
3718	A. L.
8313	A. L. G. P.
2621	**alerte.**
6230	**allemand.**
3176	alternateur.
2169	altitude.
9811	**ambulance.**
3331	**américain.**
4680	**ami.**
1656	amplificateur.
8605	ancien.
4769	**anglais.**
5672	**angle.**
0130	annamite.
7160	**antenne.**
5339	août.
9995	apercevoir.
1527	**appareil.**
6211	appartenir.
6788	approcher.
7962	**approvisionnement.**
2276	appui.
5558	appuyer.
7926	après.
8706	**après-demain.**
3772	après-midi.
4380	**armée.**
8317	**arrêter.**
9538	**arrivée.**
9415	**artifices.**
4682	**artillerie.**
3284	———— de campagne.
8030	**asphyxiant.**
8267	**assaut.**
5384	assurer.
2769	**attaque.**
7139	**attaquer.**
5517	**atteindre.**
7064	**attendre.**
7319	atterrissage.
3230	**au.**
9804	au cas où.
5967	au lieu de.

8564	au recu de.
7379	aucun.
6550	augmentation.
3530	aujourd'hui.
9574	aussitot.
6250	aussitot que possible.
4256	autocamions.
5623	autocanon.
2271	automobile.
7300	autre.
2825	aux.
0271	aux abords.
5712	aux environs.
1978	avance.
1928	avant.
3809	avant (en.)
1266	avec.
5111	avez-vous.
3524	aviation.
1726	avion.
5235	—— d'artillerie.
2724	—— de bombardement.
7674	—— de chasse.
0818	—— de commandement.
3702	—— de destruction.
9912	—— d'infanterie.
0600	—— de jalonnement.
6304	—— de réglage.
8223	—— de surveillance.
4850	—— de patrouille.
6862	—— brisé.
9463	avoir.
8104	——
7854	——
3906	B.
9058	–
1154	–
5400	balle.
8984	ballon.
6261	bande.
8800	baraque.
7800	bataillè.
5714	bataillon.
8755	—— infanterie.
4335	—— chasseurs.
9255	—— sénégalais.
9110	batterie.
6733	beaucoup.
4150	belge.
7170	béquille.
5164	besoin.
5307	bicycliste.
8338	bientôt.
6017	bivouac.
3550	blanc.
9155	blessé.
1560	bois.
8550	bombardement.
8459	bombe.
0852	bon, bonne.
7009	bon terrain.
2977	bord.
4675	bordure.
0300	bougie.
4128	boyau.
0286	brancard.
6825	brancardier.
2706	brigade.
8866	britannique.
9640	brouillard.
9118	brume.
4600	C.
3105	–
2466	–
7672	C. A.
1542	câble.
8536	—— de campagne.
7996	—— léger.
2338	cadavre.
4300	calibre.
3900	calme.
2800	camion.
4362	—— automobile.

1956	**canal.**
5367	**canevas de tir.**
0564	**canon.**
7350	**canon de tranchée.**
6300	**——— de 75.**
2350	**cantonnement.**
1616	**capitaine.**
3250	carburateur.
8253	carlingue.
9976	**cavalerie.**
1984	**cavalier.**
7762	ce.
2334	**centaine.**
3491	**certain** (ement).
6773	**ces.**
1349	**chaîne.**
5344	**changement.**
1876	**chasseur.**
0400	**cheddite.**
5750	**chef de bataillon.**
7250	**chemin.**
4329	——— de fer.
4686	**cheval.**
9189	chiffre.
0770	cimetière.
3574	clair.
8720	classe.
1784	code chiffré.
6721	**colonel.**
2440	combat.
6609	**commandant.**
3526	**commandement.**
4131	**commencer.**
4417	**compagnie.**
9169	comprendre.
5466	**compte rendu.**
2655	connaître.
6833	contact.
7989	**contre-attaque.**
0547	contre.
9956	**coordonnées.**
1938	———————
7612	———————
9384	**corde à piano.**
3340	**corps.**
5550	——— -d'armée.
5295	**cote.**
8842	**coureur.**
3670	couvert.
7739	**créneau.**
9584	crete.
2446	cycliste.
0108	D.
2819	—
5619	—
1772	danger.
4800	**dans.**
2943	— —
0877	— — —
0281	**de.**
4936	—
7218	—
8012	**déborder.**
7086	décembre.
6346	déchiffrer.
2433	décision.
6273	défaut.
8955	défense.
3387	**dégâts matériels.**
8691	délai.
9650	—— (sans).
5953	**demain.**
7353	——— **matin.**
7719	——— **soir.**
9062	——— (après-).
7432	demande.
9684	**demander.**
5663	**demi.**
8290	**démolition.**
6743	**dépannage.**
3706	**dépanner.**
9776	**dépanneurs.**
5536	**départ.**
1288	dernier.
3951	**derrière.**
0223	**des.**
8621	——
8231	——
2899	**déserteur.**
4353	destination.
9990	**destruction.**
4789	**devant.**
2265	**difficulté.**
6752	direct.
4234	**direction.**

PHRASES TOUTES FAITES.

4909	Abritez tout le monde sauf les guetteurs.
3827	Alerte.
1691	Alerte aux gaz.
5717	Allongez le tir de barrage.
2133	Artillerie ennemie nous cause de grandes pertes.
8727	Attaque dans conditions convenues.
6838	——— ennemie paraît avoir échoué.
2586	——— ennemie repoussée.
0784	Avez-vous besoin de...
7489	Avons besoin de...
4673	Brancardiers nécessaires pour blessés.
1178	Bruits faisant présumer travailleurs ennemis.
3467	Cessez le tir sur...
8187	Char d'assaut ami.
0831	——————— ennemi.
4693	Circulation anormale d'isolés.
9435	Compte rendu écrit va être envoyé.
5521	Contre-attaque ennemie sur.
7313	Déclenchez attaque.
8634	Demande (je) autorisation de...
6481	——————— ravitaillement en munitions...
9994	Dispositif d'alerte.
7524	Donnez-moi des renseignements sur...
8472	Demandons contre-batterie sur...
5230	——————— tir de réprésailles sur...
6421	——————— tir de barrage sur.
7945	——————— renforts.
4699	Diminuez la cadence du tir.
7531	En panne.
3032	Évacuez les premières lignes.
6792	——— les deuxièmes lignes.
8432	Front actuel passe par...
6783	Indices d'attaque ennemie en.
2984	——— de relève ennemie en.
9417	Infanterie doit être vigilante.
1837	——————— ennemie attaque.
0484	——————————— a atteint.
8671	——————————— progresse dans boyaux.
1282	——————————— se replie.
2741	Je n'ai pas de renseignements sur.
7477	Je ne comprends pas votre télégramme.
3496	Je vous envoie matériel demandé.
4737	Liaison assurée avec.
6830	——— perdue à gauche.
5882	——————— à droite.
1089	——————————— à droite et à gauche.
5970	N'envoyez plus de messages chiffrés.

1830	Nombreuses pertes résultant de notre artillerie.
0325	Nos troupes ont évacué.
3592	———— se sont repliées sur...
5407	—— premières lignes sont bouleversées.
7521	Notre attaque progresse.
1577	Nous avons occupé.
4722	———— réoccupé.
8135	—— nous replions (sur).
0808	—— occupons sûrement.
6134	—— paraissons occuper.
2926	—— progressons vers.
9515	—— sommes arrêtés (en).
3479	Objectif atteint.
7035	——— non atteint.
5685	Ordres en voie d'exécution.
4461	On passe la 1re ligne.
8379	Patrouille rentrée.
4623	———— sortie.
2979	———— va sortir.
6983	Placez (ou complétez) la chaîne de coureurs.
3409	Préparation d'artillerie paraît suffisante.
7983	———————— insuffisante.
9239	Quel est le secteur bombardé ?
3637	Que se passe-t-il sur votre front ?
5779	Rassemblements ennemis en...
7132	Relève aura lieu.
8325	—— n'aura pas lieu.
6935	—— commencée.
8322	—— en cours.
4892	—— terminée.
2535	Renforts ennemis arrivent par.
8454	Situation rétablie.
6454	——— critique.
1777	Sommes débordés à notre droite.
5639	———————— gauche.
0043	———————— des deux côtés.
3939	———— encerclés.
9533	Sur quoi tire l'ennemi.
7618	Suspendez exécution de l'opération.

Artillerie.

2570	Artillerie de campagne (A. C.).
1364	———— lourde (A. L.)
5183	———— de tranchée (A. T.).
1539	———— d'assaut (A. S.).
6528	———— amie va tirer (sur).
8587	———————— tire (sur).
4487	———————— a fini de tirer (sur).

0000	Soixante-seize.
0001	str.
0005	i.
0009	Présent.
0012	nage.
0014	rre.
0016	leu.
0023	yeni.
0024	ns.
0028	oux.
0031	ble.
0035	e.
0039	aite.
0043	Sommes débordés des deux côtés.
0046	Accusez réception de.
0049	cinquante-huit.
0050	part.
0056	millier.
0058	cien.
0067	virgule (,).
0070	q.
0077	quarante-huit.
0086	g.
0096	fie.
0100	dirigeable.
0102	donnée.
0109	ent.
0111	marquer.
0119	mb.
0124	gil.
0130	annamite.
0134	fer.
0139	photographe.
0144	parachute.
0149	sau.
0201	m.
0208	d.
0213	à.
0223	des.
0228	six.
0231	tir de harcèlement.
0233	panique.
0235	ordre de mouvement.
0240	excepté.
0244	point de rassemblement.
0249	nombreux.
0250	neuf.
0256	gradé.
0265	Juin.
0267	actuellement.
0271	aux abords.
0274	moindre.
0276	rouge.
0277	reculer.
0280	tir de contre-préparation.
0281	de.
0283	raccordement.
0286	brancard.
0290	ens.
0300	bougie.
0303	na.
0310	observez le tir sur.
0315	marche.
0321	ssion.
0325	Nos troupes ont évacué.
0327	dent.
0330	front.
0338	ture.
0343	prise.
0349	hôpital.
0350	quent.
0357	champ.
0361	sse.
0370	a.
0374	d'.
0375	ing.
0379	sondage.
0383	mille.
0389	r.
0393	u.
0400	cheddite.
0409	euse.
0418	ieur.
0424	tir indirect.
0426	etr.
0430	sénégalais.
0436	pièce.
0440	parvenir.
0470	recevoir.
0472	obliquer.
0474	deur.
0484	Infanterie ennemie a atteint.
0494	flo.
0500	1917.
0508	vais.
0510	mort.
0516	dix-neuf.
0519	sie.
0527	hussards.
0532	groupe nul.

0536	di.
0539	général.
0547	contre.
0550	ku.
0555	am.
0561	ligne téléphonique.
0564	canon.
0570	ième.
0577	ja.
0580	organique.
0586	ten.
0596	Soixante-dix.
0600	avion de jalonnement.
0602	menaçant.
0607	ennemi.
0610	os.
0614	absolument.
0616	lot.
0622	parc d'artillerie.
0625	jo.
0632	Quatre cents.
0638	prière de.
0642	ition.
0652	sp.
0666	gou.
0667	quatre-vingt-cinq.
0679	iers.
0691	ordonner.
0700	heure.
0707	une.
0711	ne.
0714	italien.
0717	moins vite.
0721	deux.
0726	je.
0731	grand parc.
0734	pre.
0737	le plus tôt possible.
0744	préparatif.
0750	t.
0757	ac.
0759	tué.
0763	aérostiers.
0770	cimetière.
0773	ille.
0778	objet.
0782	ier.
0784	Avez-vous besoin de...
0787	travailleurs.
0790	ess.
0795	vétérinaire.
0799	note.
0800	b.
0804	es.
0808	Nous occupons sûrement.
0818	avion de commandement.
0825	tout.
0827	division.
0831	char d'assaut ennemi.
0834	retard.
0838	seize.
0842	radiogoniométrique.
0848	proportion.
0852	bon, bonne.
0860	E. N. E.
0862	en panne.
0865	au.
0869	qu'.
0877	dans.
0880	tir trop à droite.
0881	jusqu'à nouvel ordre.
0886	sopwith.
0889	vous.
0899	en plus.
0902	poste radiogoniométrique.
0909	é.
0917	ale.
0924	pioche.
0929	ter.
0933	prochain.
0937	quelque.
0941	placer.
0948	régiment d'artillerie.
0950	ave.
0954	vont.
0963	part.
0978	car.
0980	ette.
0989	non.
0991	sous-lieutenant.
0992	secteur.
0994	qu'y a-t-il.
0999	Présent.

Appendix 7.—AN EXAMPLE OF THE ENCIPHERING TABLE FOR FRENCH FIELD CODE

TABLEAU DE CONCORDANCE

SÉRIE 65

Veillez sur ce tableau.
Brûlez-le s'il risque d'être pris.

CHIFFREMENT.		
0 – GS	30 – HR	70 – AN
1 – RH	31 – IA	71 – RB
2 – AM	32 – VS	72 – HN
3 – SI	33 – GU	73 – MH
4 – BH	34 – NH	74 – GD
5 – NS	35 – IS	75 – BU
6 – DA	36 – HD	76 – IE
7 – TD	37 – TA	77 – DM
8 – EA	38 – IB	78 – AI
9 – UG	39 – AE	79 – RN
00 – AT	40 – HT	80 – UH
01 – GA	41 – SD	81 – NR
02 – IM	42 – US	82 – AD
03 – DN	43 – DI	83 – BM
04 – GH	44 – EI	84 – GI
05 – MN	45 – BS	85 – ED
06 – HI	46 – GR	86 – HB
07 – VG	47 – MD	87 – NA
08 – UR	48 – IR	88 – ER
09 – AB	49 – EM	89 – HG
10 – BT	50 – AU	90 – SN
11 – BA	51 – SM	91 – AS
12 – RD	52 – DB	92 – MS
13 – ND	53 – HS	93 – BD
14 – AG	54 – GB	94 – IN
15 – TS	55 – UA	95 – DS
16 – EG	56 – DR	96 – HM
17 – AR	57 – BI	97 – EH
18 – SB	58 – TR	98 – GT
19 – BN	59 – EB	99 – GN
20 – ES	60 – AH	
21 – RT	61 – VN	
22 – HA	62 – TN	
23 – DG	63 – BG	
24 – SR	64 – MU	
25 – BE	65 – BR	
26 – DT	66 – NG	
27 – NU	67 – SH	
28 – GM	68 – UM	
29 – NB	69 – DH	

DÉCHIFFREMENT.		
AB – 09	EM – 49	ND – 13
AD – 82	ER – 88	NG – 66
AE – 39	ES – 20	NH – 34
AG – 14		NR – 81
AH – 60	GA – 01	NS – 5
AI – 78	GB – 54	NU – 27
AM – 2	GD – 74	
AN – 70	GH – 04	RB – 71
AR – 17	GI – 84	RD – 12
AS – 91	GM – 28	RH – 1
AT – 00	GN – 99	RN – 79
AU – 50	GR – 46	RT – 21
	GS – 0	
BA – 11	GT – 98	SB – 18
BD – 93	GU – 33	SD – 41
BE – 25		SH – 67
BG – 63	HA – 22	SI – 3
BH – 4	HB – 86	SM – 51
BI – 57	HD – 36	SN – 90
BM – 83	HG – 89	SR – 24
BN – 19	HI – 06	
BR – 65	HM – 96	TA – 37
BS – 45	HN – 72	TD – 7
BT – 10	HR – 30	TN – 62
BU – 75	HS – 53	TR – 58
	HT – 40	TS – 15
DA – 6		
DB – 52	IA – 31	UA – 55
DG – 23	IB – 38	UG – 9
DH – 69	IE – 76	UH – 80
DI – 43	IM – 02	UM – 68
DM – 77	IN – 94	UR – 08
DN – 03	IR – 48	US – 42
DR – 56	IS – 35	
DS – 95		VG – 07
DT – 26	MD – 47	VN – 61
	MH – 73	VS – 32
EA – 8	MN – 05	
EB – 59	MS – 92	
ED – 85	MU – 64	
EG – 16		
EH – 97	NA – 87	
EI – 44	NB – 29	

CONCORDANCE N° 65.

Le tableau ci-contre a pour objet de permettre, à défaut de communication par fil, la transmission par T. S. F. de tous messages chiffrés avec le Code chiffré, sans que soit mise en danger la sécurité de ce Code.

On doit faire emploi de ce double chiffrement pour les messages téléphonés qui seraient particulièrement secrets ou importants.

Exemple de double chiffrement :

TEXTE :		La		relève		au	-	ra		lieu		demain	matin.
CODE :	1	65	1 4	27	5 0	86	5 8	75	0 1	06	5 7	35	3
TABLEAU :	RH	BR	AG	NU	AU	HB	TR	BU	GA	HI	BI	IS	SI

(Le premier chiffre du premier groupe doit constituer *seul* la première tranche.)

Pour le déchiffrement, remplacer chaque groupe de deux lettres par le nombre qui correspond à ce groupe dans le tableau de chiffrement.

On retrouve les groupes du Code en rétablissant les nombres de quatre chiffres à partir du commencement.

Ne jamais transmettre deux fois un même texte dans des chiffrements différents.

Appendix 8.—EXTRACTS FROM GERMAN FIELD CODES

CONTENTS OF APPENDIX 8

Appendix 8A.—THE *SCHLUESSELHEFT*

Geheim!

Schlüsselheft

1. Ausgabe.

Nicht in Feindes Hand fallen lassen.

I. Morsezeichen und Buchstabiertafel.

a	Adolf	·—
b	Berta	—···
c	Cäsar	—·—·
d	David	—··
e	Emil	·
é	französ. e	··—··
f	Friedrich	··—·
g	Gustav	——·
h	Heinrich	····
i	Isidor	··
j	Jakob	·———
k	Karl	—·—
l	Ludwig	·—··
m	Moritz	——
n	Nathan	—·
o	Otto	———
p	Paula	·——·
q	Quelle	——·—
r	Richard	·—·
s	Siegfried	···
t	Theodor	—
u	Ursula	··—
v	Viktor	···—
w	Willi	·——
x	Xantippe	—··—
y	Ypsilon	—·——
z	Zacharias	——··
ä	Adolfemil	·—·—
ö	Ottoemil	———·
ü	Ursulaemil	··——
ch	Cäsarheinrich	————

Morsezeichen und Buchstabiertafel.

(Fortsetzung.)

	Ziffern:	gekürzt:
0	— — — — —	—
1	·— — — —	·—
2	··— — —	··—
3	···— —	···—
4	····—	·—·
5	·····	·
6	—····	···
7	— —···	—···
8	— — —··	—··
9	— — — —·	—·

Satz- und Hilfszeichen.

Punkt	·· ·· ··
Komma	·—·—·—
Fragezeichen	··— —··
Binde- oder Gedankenstrich	—····—
Klammer	—·— —·—
Bruchstrich	—··—·
Trennungszeichen	—···—
Irrungszeichen	·····
Wartezeichen	·—···

II. Buchstabenzeichen.

a) Allgemeine Verkehrszeichen.

lg	**L**icht **g**ut
ls	**L**icht **s**chlecht
wp	**W**ie dort Em**p**fang?
eg	**E**mpfang **g**ut
es	**E**mpfang **s**chlecht
wt	**W**ie dort **T**on?
tg	**T**on **g**ut
ts	**T**on **s**chlecht
th	Nehmt **h**ohen **T**on
tm	Nehmt **m**ittleren **T**on
ti	Nehmt **t**ieferen **T**on
mg	**M**ehr Ener**g**ie
wg	**W**eniger Ener**g**ie
gl	**G**ebt **l**angsamer
chi	**Chi**ffrierte Nachricht
zi	Stationsnachricht
kr	Dringende Nachricht
nf	Hier liegt kein Spruch mehr vor
fö	**F**unkspruch gelö**s**t
os	Das Empfangene ist **o**hne **S**inn
ve	**V**erstanden
nv	**N**icht **v**erstanden
us	Störung im Funkerbetrieb
mr	**M**otorstö**r**ung
fs	Hier **f**remder **S**törer
wh	**W**iederholen
wa	(5) **W**arten (Minutenzahl), ich rufe wieder an
bp	**B**leibe auf Em**p**fang
fa	**F**olgt **A**ntwort
kü	**K**annst Du **ü**bermitteln
üm	Ich **ü**ber**m**ittele an
nü	Ich kann **n**icht **ü**bermitteln
hh	**H**auptwelle
nn	**N**ebenwelle
um	**Um**schaltezeichen
xx	Ich muß sofort marschieren
ng	**N**otlandun**g**
dd	Station scheidet aus dem Verkehr aus
gr	**G**ruppe
pü	S**p**ruch **ü**berholt
ru	Sie werden **ge**rufen von Station

b) Zeichen für Fliegerdienst.

1. Allgemeine Zeichen.

p a	Planquadrat
w o	Wolken
d u	Dunst
n l	Nördlich
s l	Südlich
o l	Östlich
w l	Westlich
g b	Graben
p t	Punkt
e d	Eisenbahndamm
w d	Wald
s t	Straße
i m	Infanterie in Marschkolonne
i v	Infanterie in Versammlung
a m	Artillerie in Marschkolonne
a f	Artillerie feuernd
m w	Marschkolonne aller Waffen
b v	Bagagen in Versammlung
a t	Ausladen von Truppen
e v	Eisenbahnverkehr
t b	Tank in Bereitschaft
t n	Tank naht
s f	Vorschlag für Störungsfeuer
a l	Allg. Schußlage eigenen oder feindl. Feuers

III. Zahlenzeichen.

a) Militärische- und Ortsnamen.

Achill	000	000
Ackermann	001	001
Adam	002	002
Adele	003	003
Adler	004	004
Admiral	005	005
Adonis	006	006
Albert	007	007
Alexis	008	008
Altwater	009	009
Amsel	010	010
Anhalt	011	011
Ansbach	012	012
Anton	013	013
Bauer	014	014
Bär	015	015
Blücher	016	016
Bocksberg	017	017
Börse	018	018
Bremen	019	019
Brocken	020	020
Brunnen	021	021
Bürger	022	022
Capitth	023	023
Cardinal	024	024

Militärische- und Ortsnamen.

(Forsetzung.)

Caspar	025	025
Caviar	026	026
Cäcilie	027	027
Ceder	028	028
Cement	029	029
Cerberus	030	030
Cigarre	031	031
Cicero	032	032
Cypresse	033	033
Collin	034	034
Damaskus	035	035
Damsdorf	036	036
Daniel	037	037
Danzig	038	038
Dattel	039	039
Delphin	040	040
Delta	041	041
Diamant	042	042
Dichter	043	043
Dido	044	044
Dietrich	045	045
Direktor	046	046
Domherr	047	047
Donau	048	048
Drache	049	049

b) Gefechtsmeldungen.

Vom Gegner:

Gegner bereitet Angriff vor	150
„ greift an	151
„ verstärkt sich	152
„ geht zurück	153
„ in vordere Linie eingedrungen	154
„ links von uns eingedrungen	155
„ rechts „ „ „	156
„ r. u. l. eingedrungen, Mitte hält	157
„ in der Mitte eingedrungen	158
„ in der Mitte u. r. eingedrungen	159
„ in der Mitte u. l. „	160
„ durch vorderste Linie durchgebrochen	161
„ hat starke Verluste	162
„ zwischen seiner und unserer Stellung liegen geblieben	163
Feindl. Angriff abgeschlagen	164
Gegner schießt mit Gasgranaten	165
Feindl. Stellung ist noch nicht sturmreif	166
Gegner schanzt bei	167
Gegner schießt mit Fliegerbeobachtung ein auf	168
	169
	170
	171
	172
	173
	174

Gefechtsmeldungen.

(Fortsetzung.)

Eigene Truppe:

Wir gehen zurück	175
Wir gehen vor (sind zum Angriff fertig)	176
Wir haben starke Verluste	177
Wir halten die Linie	178
Wir werden von der eig. Inf. beschossen	179
Wir werden von der eig. Art. „	180
Anschluß vorhanden	181
Anschluß fehlt	182
Eigener Sturm steht bevor	183
Gegenangriff im Gange	184
Gegenangriff gelungen	185
Gegenangriff nicht geglückt	186
Unterstützung auf dem rechten Flügel nötig	187
„ „ „ linken „ „	188
Unser Ziel ist erreicht	189
	190
	191
	192
	193
	194
	195
	196
	197
	198
	199

c) Buchstaben und Silben.

Buchstaben und Silben.

(Fortsetzung.)

nach	306	st	328
nd	307	t	329
ne	308	tel	330
nen	309	ten	331
ns	310	u	332
nu	311	ü	333
o	312	um	334
ö	313	un	335
ob	314	ung	336
p	315	uns	337
q	316	v	338
qu	317	ver	339
r	318	vor	340
re	319	w	341
rück	320	weg	342
s	321	wie	343
sch	322	wir	344
se	323	wo	345
seit	324	x	346
sen	325	y	347
sich	326	z	348
so	327	zer	349

d) Zahlen und Uhrzeiten.

0	350	12	Uhr nachts	379
1	351	1	„ vorm.	380
2	352	2	„ „	381
3	353	3	„ „	382
4	354	4	„ „	383
5	355	5	„ „	384
6	356	6	„ „	385
7	357	7	„ „	386
8	358	8	„ „	387
9	359	9	„ „	388
10	360	10	„ „	389
11	361	11	„ „	390
12	362	12	„ mittags	391
15	363	1	„ nachm.	392
20	364	2	„ „	393
25	365	3	„ „	394
30	366	4	„ „	395
40	367	5	„ „	396
45	368	6	„ „	397
50	369	7	„ „	398
60	370	8	„ „	399
70	371	9	„ „	400
80	372	10	„ „	401
90	373	11	„ „	402
hundert	374			
tausend	375			

mal	376
ter, te, tes	377
römisch	378

e) Alphabetisches Wörterverzeichnis.

A

Appendix 8B.—AN EXAMPLE OF THE ENCIPHERING AND DECIPHERING TABLES FOR THE SCHLUESSELHEFT

Verschlüsselungstafel.

	0	1	2	3	4	5	6	7	8	9
0	23	48	60	05	78	35	58	64	29	52
1	20	77	33	59	21	70	02	40	63	08
2	11	49	01	69	47	41	79	74	22	42
3	32	76	39	18	75	30	09	51	80	65
4	61	19	43	81	06	56	73	62	10	28
5	85	50	24	88	31	84	27	90	55	57
5	03	91	96	53	68	16	44	89	15	87
7	97	25	71	04	95	34	14	37	93	38
8	26	72	54	92	13	83	45	00	66	67
9	86	12	98	36	99	46	82	17	94	07

Entschlüsselungstafel.

	0	1	2	3	4	5	6	7	8	9
0	87	22	16	60	73	03	44	99	19	36
1	48	20	91	84	76	68	65	97	33	41
2	10	14	28	00	52	71	80	56	49	08
3	35	54	30	12	75	05	93	77	79	32
4	17	25	29	42	66	86	95	24	01	21
5	51	37	09	63	82	58	45	59	06	13
6	02	40	47	18	07	39	88	89	64	23
7	15	72	81	46	27	34	31	11	04	26
8	38	43	96	85	55	50	90	69	53	67
9	57	61	83	78	98	74	62	70	92	94

Appendix 8C.—THE *SATZBUCH*

Geheim!

Satzbuch 140

Teil:
Schlüsseln

Nicht in Feindeshand fallen lassen!

Register-Erklärungen

nebst

Inhaltsverzeichnis.

Wörterbuch:

Buchstabierverfahren:

460519 O—42——7

Vor dem Gebrauch des Buches zu lesen!

Vorbemerkungen.

1. Alle Meldungen und Befehle müssen mit Hilfe des Satzbuches geschlüsselt werden. Klartexte dürfen nur im äußersten Notfalle gefunkt werden.

   Mischung von Klartext und geschlüsseltem Text, sowie Einstreuen von **ungeschlüsselten Zahlen, Zeitgruppen, Trennungs-** oder **Satzzeichen** in den geschlüsselten Text ist verboten.

   Redewendungen und Sätze, die nach dem Satzbuch durch **ein** Signal wiedergegeben werden können, **dürfen nicht** durch ihre Einzelbestandteile ausgedrückt werden, z. B. „in unserer Hand" durch „in" — „unser" — „Hand".

   Worte und Wortendungen, die zum Verständnis nicht unbedingt erforderlich sind, sind beim Schlüsseln wegzulassen, z. B. schlüssele statt „bei-m Feind-e" „bei Feind" usw.

2. Das Satzbuch besteht aus dem Teil „Schlüsseln" und dem Teil „Entschlüsseln" und enthält dreistellige Buchstabengruppen, deren erster Buchstabe **a, k, r, s** oder **u** ist.

   a) Der Teil „**Schlüsseln**" gliedert sich in folgende Abschnitte:

   Wichtige Meldungen,
   Allgemeine Meldungen,
   Stations- und Betriebsmeldungen,
   Wettermeldungen,
   Ortsnamen,
   Militärische Decknamen,
   Zahlen,
   Uhrzeiten,
   Buchstaben und Silben,
   Hilfssignale,
   Satzzeichen,
   Wörterbuch und blinde Signale,
   Buchstabierverfahren.

   Hinter den einzelnen Abschnitten sowie im Wörterbuch ist für handschriftliche Ergänzungen Raum gelassen.

   Die militärischen Namen (Stäbe, Formationen) und Ortsnamen müssen von den Funker-Abteilungen selbst nach Bedarf eingetragen und mit Signalen versehen werden.

140 L

Die für diese Ergänzungen zur Verfügung stehenden Signale sind aus dem Teil „Entschlüsseln" zu ersehen.

Bei Ausfüllung des Satzbuches nicht vorgesehene militärische Namen und Ortsnamen werden mit Hilfe des am Schlusse des Teiles „Schlüsseln" befindlichen „Buchstabierverfahrens" wiedergegeben.

Die Hilfssignale werden hinter die Gruppen gesetzt, deren Bedeutung geändert werden soll. Soll z. B. „angefordert" geschlüsselt werden, so setzt man hinter das Signal für „anfordern" das Signal „Mittelwort der Vergangenheit", also: kax. sav

Die Hilfssignale werden nur angewandt, wenn sie zur Vermeidung eines Irrtums erforderlich sind.

Blinde Signale sind am Fußende jeder Seite aufgenommen. Von ihnen ist ausgiebig Gebrauch zu machen. Vor allem müssen sie in häufig wiederkehrende, ähnlich oder gleichlautende Meldungen und Befehle an beliebigen Stellen eingeschaltet werden.

Kurze Meldungen, die aus nur einem oder sehr wenig Signalen bestehen, sind durch Zusatz mehrerer blinder Signale zu verschleiern.

Beim Entschlüsseln werden die blinden Signale einfach übergangen.

Das Wörterbuch ist alphabetisch angelegt; ä, ö und ü sind als a, o und u behandelt. Bei Eigenschaftswörtern gilt das Signal der Grundform auch für die abgeleiteten Formen, z. B. das Signal für „groß" zugleich für große, großer, großes usw.; das Signal für „dieser" auch für diese, dieses, diesem, diesen. Das Signal für die Nennform gilt auch für die Formen der Gegenwart, z. B. „abflauen" für „flaut ab", „nehmen" für „nimmt". Rückbezügliche Zeitwörter sind unter dem Zeitwort zu suchen, z. B. „sich ausdehnen" unter „ausdehnen, sich", „sich eingraben" unter „eingraben, sich". Wortgruppen wie: „auf dem rechten Flügel", „unter Feuer nehmen", „eigene Artillerie", „hat aufgehört", „zu spät" sind im Alphabet einmal unter ihrem ersten Wort eingefügt (auf, unter, eigene, hat, zu), dann aber auch unter dem nachfolgenden Hauptwort, Zeitwort usw. (Flügel, Feuer, Artillerie, aufhören, spät). In gleicher Weise sind häufig vorkommende Formen von Hilfszeitwörtern und Zeitwörtern wie: ist, war, wird, kann, genommen einmal

unter dieser Form und dann auch unter der zugehörigen Nennform (sein, werden, können, nehmen) zu finden.

Zum Zusammenstellen von Wörtern, die nicht im Satzbuch enthalten sind, sind Einzel-, Doppelbuchstaben und Silben unter „Buchstaben und Silben" aufgeführt.

Das Buchstabieren von Worten, die im Satzbuch enthalten sind, ist verboten.

Sind für ein Wort oder eine Wörtergruppe mehrere Signale angegeben, so müssen diese Signale abwechselnd gebraucht werden, z. B. auch wenn das Wort nur einmal im Funkspruch vorkommt, ist dafür nicht immer das an erster Stelle im Satzbuch stehende Signal zu wählen.

b) Der Teil „Entschlüsseln" enthält zunächst die Signale mit dem Anfangsbuchstaben **a**, hierauf die mit den Anfangsbuchstaben **k**, **r** und **s** und schließlich die mit dem Anfangsbuchstaben **u**.

Am Schlusse des Teiles „Entschlüsseln" befindet sich die **Entschlüsselungstabelle** des „Buchstabierverfahrens".

3 Bei einer

Änderung von Signalen

ist streng darauf zu achten:

1. daß die Änderung im Teil „Schlüsseln" und im Teil „Entschlüsseln" vorgenommen wird,
2. daß diejenigen Signale, deren Bedeutung im Teil Schlüsseln an mehreren Stellen vorkommt (siehe oben: auf dem rechten Flügel, unter Feuer nehmen, zu spät, ist, war, kann usw.), an allen Stellen geändert werden.

   Zur Erleichterung dieser Arbeit sind diese Signale, soweit sie mehrmals vorkommen, mit einem Sternchen bezeichnet.

Wichtige Meldungen.

a) vom Gegner:

Feind bereitet Angriff vor	kks, rlj, ssk
Feind greift an bei	aok, kvj, ufz
Feind verstärkt sich	reh, kni, scd
Feindliche Gräben sind stark besetzt . .	sde, ate, kcu
Feindliche Gräben sind schwach besetzt .	kfa, rhh, sxs
Feindliche Gräben füllen sich	rqa, rmr, ada
Feind in die vordere Linie eingedrungen .	ujl, krt, skz
Feind links eingedrungen	suk, rza, kok
Feind rechts eingedrungen	afp, raa, sbz
Feind links und rechts eingedrungen, Mitte hält	kwe, aji, riz
Feind in die Mitte eingedrungen	ugl, aka, syx
Feind durch vordere Linie durchgebrochen	uya, ahj, rwy
Feind zwischen seinen und unseren Stellungen liegen geblieben	rwk, agl, ube
Feindlicher Angriff abgeschlagen	set, kse, rpg
Feind hat starke Verluste	uvi, kkd, ald
Feind schießt mit Gasgranaten	kjl, uca, urk
Feindliche Stellung ist noch nicht sturmreif	rye, auy, kbi
Feindliches Trommelfeuer liegt auf . . .	apa, una, ajt
Feindliches Sperrfeuer liegt auf	rdl, smv, suh
Feind löst ab	asl, kzo, upx
Feindliche Truppen unbeschossen bei . . .	sgq, rxf, uzd
Feindlicher Flieger unbeschossen über .	axz, rup, spp
Feindliche Kavalleriepatrouille gesichtet bei	rtc, kgo, ukw

.....

.....

.....

.....

.....

Blinde Signale . . . . . arq, kye, uzh, sqv, rif

Wichtige Meldungen
(Fortsetzung).

b) von den eigenen Truppen:

Wir gehen vor	kzj, uei, rwe
Wir gehen zurück	sca, kma, all
Wir halten die Linie	are, kyp, sda
Wir greifen an	kcn, azf, rga
Wir haben starke Verluste	rfz, uqq, swi
Wir können uns nicht halten	klb, acl, rry
Wir werden von der eigenen Infanterie beschossen	rxp, kqa, uae
Wir werden von der eigenen Artillerie beschossen	uzn, sly, ryw
Eigener Sturm steht bevor	anx, uvs, kpy
Gegenangriff im Gange	rnb, aio, sac
Gegenangriff gelungen	uia, avu, kae
Gegenangriff nicht gelungen	svn, rja, ump
Anschluß vorhanden	aek, szo, ktt
Anschluß fehlt	kxl, roq, udz
Erhöhte Gefechtsbereitschaft	rso, kda, agu

c) **Artillerie:**

Sofort Sperrfeuer erbeten	uhz, rbz, sio
Sperrfeuer kann aufhören	snk, rxx, uzy
Feuer vorverlegen	rzl, klk, ame
Feuer zurückverlegen	uue, rea, sea
Feuer mehr nach links verlegen	kil, atf, rha
Feuer mehr nach rechts verlegen	aqh, rqz, uho
Feuerwalze erbeten	rcj, sma, rzh
Feuerwalze weiter vorlegen	rvl, sqn, uyp
Halten der Feuerwalze erbeten	shl, aqd, rbp
Sprengpunkte heben	awb, sba, kar
Sprengpunkte senken	khu, avz, rjz
Abwehrfeuer erbeten	rkh, uua, kiz
Einbruchstelle verriegeln!	umt, sua, afu
d) Erbitten Nachschub von	sra, upp, kwk
Erbitten sofort Verstärkung	aha, utn, kcf
Tankwagen im Anmarsch	kua, uct, stz

Stations- und Betriebsmeldungen.

Erhöhte F.T.-Bereitschaft	knw
Erhöhte F.T.-Bereitschaft aufgehoben	akq
Verstärkter Empfang	sfl
Station betriebsfertig	ayo
Station baut ab	kef
Ich zerstöre die Station	rhf
Ich habe die Geheimpapiere vernichtet	upj
Sende mit Erdkabel	sxg
Fernsprechverbindung unterbrochen mit	ace
Treffer nach Station	kro
Langsamer und deutlicher geben	rqk
Sende mit Hochantenne	uba
Schlechter Empfang	skq
Habt ihr unsere sämtlichen Meldungen gehört?	usm
Eure sämtlichen Meldungen sind gehört	koa
Quittung folgt nicht	uxj
Antwort wegen Bestellungsschwierigkeiten verzögert	rag
Sofort nach hier senden	sbn, klq
Dies ist ein Übungsfunkspruch ohne Sinn	aul, res, sfi
Wo ist Akkumulator-Ladestelle?	kbq, aop, rmw
Sind Akkumulatoren fertig?	rib, aya, kfz
Blinde Signale	rzi, akp, sur, kst, uuv

Stations- und Betriebsmeldungen

(Fortsetzung).

Akkumulatoren abholen	uoz, suw, afg
Wo steht ihr?	sym, kwp, rtg
Wir stehen bei	abe, kjf, rdb
Station soll auf Empfang stehen um	ksh, egy, axa
Station wird vorgezogen nach	rpn, kgf, uka
Station marschiert	ucg, ruj, ufl, spj
Station marschiert	sjl, uxa, rlu, kvv
Meldekopf befindet sich bei	utj, ssb, abu
Kopf des Funkspruchs	kkm, snx, api
*Antwort dringend erforderlich	avn, ujz, ugb

*Ablösung	kns, akz	*Draht	shz
*Akkumulator (Sammler)	rfj	Dunkelfeinde	awq
Amperemeter	sdd, kdi	Eierketten	khm
Anoden-Batterie	rgj	Eisenvorschalt-widerstand	rkb
Antenne	uqa	Edison-Akkumulatoren	ulq
Antennendraht	svz	Empfänger	szg
Antennenkabel	aed	Erdantenne	agd
*Beleuchtungsmaterial	kqq	Funker	kun
*Benzin	rra	*Funkspruch	rug, uda
Benzol	ubz	*F.T.-Verbindung	sqh, rwb
Blei-Batterie	slp	*Getränke	urw
Bosch-Aggregat	kpi	g-Fukgerät	xmn
Detektor	aia	*Gleichstrommaschine	amr
*destilliertes Wasser	uwg, raz	Hörer	rex

Blinde Signale . . . . . snd, roe, abt, uaw, kdg

Wettermeldungen

(Fortsetzung).

darüber	axf	in 200 m Höhe . .	rel, aes
diesig	kmi	„ 300 „ „ . .	ukf, ush
drehend	rkf	„ 500 „ „ . .	sai, kla
durchschnittlich	sxa	„ 750 „ „ . .	ape, ucp
etwa	kvo	„ 1000 „ „ . .	seu, kut
etwas	uqw	„ 1500 „ „ . .	ueh, sen
Feuchtigkeit . . .	sdk, kav	„ 2000 „ „ . .	sue, rya
Fortdauer	aoa	„ 2500 „ „ . .	ktn, swt
Fortdauer bestehender Wetterlage wahrscheinl.	uut	„ 3000 „ „ . .	rsf, ajw
Frost	rfa	„ 3500 „ „ . .	upd, shg
Gebiet	kzm	„ 4000 „ „ . .	scu, ume
Gefrierpunkt	ase	„ 4500 „ „ . .	aau, reg
geschlossen	rnh	„ 5000 „ „ . .	kki, syr
Gewitter	szd	„ 6000 „ „ . .	skr, rma
starke Gewittertätigkeit	kej	„ 7000 „ „ . .	utg, azb
gleichbleibend	axn	„ 8000 „ „ . .	afa, uxz
gleichmäßig	skd	kalt	sel
heiter	rco	kühl	rsn
heute	apu, urs	langsam	kba
hoch	sgd	leicht	ans
Höhenwind	kix	linksdrehend	uxo
in der Höhe . . .	rze, aku	Luftgewicht	ref, asx
in größeren Höhen	uul, ren	mäßig	sqq
in Höhe von	arv, sjo	mild	kjj
in 100 m Höhe . .	srs, kxu	Mittag(s)	rno

Blinde Signale . . . . . aep, krn, sbr, uof, rxm

Wettermeldungen

(Fortsetzung).

morgen	koo	sehr	ass
nach	sia	Sicht	rnu
Nachmittag(s)	arj	sichtig	krm
nach oben	uwd	später	sfr
Nacht(s)	akf	stark	aos
nahe	sfa	Stärke	uvg
Nebel	rzt	stärker	sii
nebelig	uqe	stellenweise	rud
Niederschläge	ahw	Sturm	aql
Niederschläge in Schauern	udj	stürmisch	ral
Norden	rla	Süden	ayf
nördlich	saq	südlich	kte
normal	ulm	Südosten	rts
Nordosten	kwa	südöstlich	kia
nordöstlich	ssw	Südwesten	sjk
Nordwesten	ubp	südwestlich	agh
nordwestlich	kjv	Temperatur	rkp
Osten	als	tief	kka
östlich	kbn	trocken	rdg
rechtsdrehend	ryj	über	uyo
Regen	uja	überwiegend	aqr
Richtung	rdg	unsichtig	kfr
ruhig	ufr	verbreitet	uku
Schnee	rxt	vereinzelt	afi
schwach	ssi	Verschlechterung des Wetters	rus

Blinde Signale . . . . . kcb, ami, rif, sch, uhl

Militärische Decknamen
(Fortsetzung).

Abschnitt „G"

Militärische Namen:

Division „G"	aav
Inf. Brig. „	aax
Regt. G I.	aay
„ „ II.	abs
„ „ III.	abv
K. I. W. G I rechts	abx
„ „ links	acs
„ G II. rechts	act
„ „ links	acy
„ G III. rechts	add
„ „ links	adε
Art. Kdeur. G.	aεc
„ Hauptgruppe G	aεv
Fernkampfgruppe G	afε
Art. U. Gruppe Ost	aff
„ „ Mitte	afv
„ „ West	agt
Div. Beob. Kontseo	agv
Divfunka G	agy
Diverna G.	[illegible]
Gruppe Gorz	aiv

Zahlen.

Zahlen, für die keine besonderen Signale gegeben sind, z. B. 7069, werden in der Weise geschlüsselt, daß die Signale der einzelnen Ziffern: sieben, null, sechs, neun, einfach nacheinander gegeben werden; hierbei dürfen nur die Ziffern null bis neun benutzt werden. Runde Hunderte und Tausende, z. B. 200, 300 usw. und 2000, 3000 usw., in der Weise, daß die Signale für zwei, drei usw. und hundert bzw. tausend nebeneinander gesetzt werden.

Die Signale der Silbe „te" am Ende der Ordnungszahlen dienen zum Schlüsseln der Ordnungszahlen 13te, 14te usw.

Das Signal der Silbe „mal" am Ende der Multiplikationszahlen dient in gleicher Weise zum Schlüsseln der Zahlen 6 mal, 7 mal usw.

Beispiele: 7069: ukz, ayi, kgs, rxc; 200: adr, uza; 8000: rte, uub; 13te: slh, rmg; 6mal: sga, uma.

null . . .	anm, kyw, sfd, ayi	15	ajc, sgg
1	kez, rne, ujd	16	rkz, uoj
2	swa, adr, krg	17	szr, aaa
3	rte, ugz, snz	18	ktm, rpz
4	rys, uxd, kod	19	udm, sir
5	kjs, apz, rdz	20	kin, amx
6	sga, axv, kgs	30	sch, azc
7	rlz, ukz, srz	40	kdb, rhg
8	ahz, roc, uep	45	upa, swk
9	spw, rxc, uyk	50	zid, kwb
10	knl, akc, rfw	60	rrr, slz
11	sej, art, kem	70	kpz, apv
12	uju, swx, aem	80	rbx, saz
13	uaq, slh	90	khy, avy
14	uwu, kiv	hundert . . .	avh, uza, kzw
		tausend . . .	uam, rzz, uub

Blinde Signale . . . . . rxu, kps, ukr, kmv, aqi

Buchstaben und Silben.

a . . . alv, ulz, kra
ä . . . . . rqu
*ab . . ubm, şkv
age . . . . aoz
agne . . . soz
ai . . . . . ryl
ain . . . . uwy
air . . . . kjd
aire . . . . aim
*am . . . . rcg
*an . . shc, axt, kgb
ance . . . . rkt
ang . . . . umn
ar . . . . sza
au . . . . aab
*auf . kud, rpu, ucz
*aus . . . . siw
aux . . . . rwc
ay . . . . uzz
b . . ath, kmz, rec
bar . . . . ayb
bas . . . . aol
be . . . . kdd
*bei . sfq, rnc, uqe
ben . . . . swb
ber . . . . alv
*bis . kwc, rsm, uhy
bl . . . . snb
bois . . . . uvb
br . . . . . rzm
butte . . . uww
c . . . kjk, apb, rcf
ch . . . shn, ava
château . . kaj
che . . . rku, umf
chen . . . szz
cher . . . . agb
cht . . . kth, rpa
ck . . . . ucb
côte . . . . sqb
cours . . . rxk
court . . . uym
croix . . . kmh
d . . . anf, rfc, kzy
*da . . . . sdh
*das . . . . ars
de . . . . keh
*dem . . . rnd
*den . . uit, swq
*der . . ads, kxq
dern . . . rsp
*des . . uht, sok
*die . . rzy, uud
dr . . . . . kpw
*durch . ain, rbm
e . . sax, avx, kay
é . . . . . rjy
eau . . . . unb
eh . . . . srx
ei . . . ahy, kux
*ein . . rve, uec
el . . . . . aqz
elle . . . . rxz
em . . . . kko
en . . alp, kyx
end . . . . sdi
eng . . . . azu
ent . . . . kee
*er . . rnx, uqt
*es . . swv, adc
et . . . . . kqo
ette . . . . rrf
eu . . . . uaz
eux . . . . slb
ey . . . . . ryc
f . . . uyz, kpj, aqf
*fach . . . akm
ff . . . . . rdq
fe . . . . . shw
fl . . . . . avr
fontaine . . kgd
forêt . . . rkq
fort . . . . uly
fr . . . . syp
*für . . ahn, kta
g . . rvf, udx, spy
ge . . uyl, kml

Blinde Signale . . . . . aep, rpp, uml, kst, sye

Buchstaben und Silben

(Fortsetzung).

*gegen . amd, rfr
gen . . sdm, azr
ger . . . . kch
ges . . . . rnf
gl . . . . ujw
gne . . . . svj
gny . . . . acv
gr . . . . . kxh
grand . . . rrh
h . . . uar, sli, ryb
haft . . . . uvm
haut . . . . kjm
he . . . . apc
heit . . . . rcb
her . . . . shb
hin . . . . axy
*hinter . . kgc
ht . . . . rki
i . . ukd, syc, aar
*ich . . . ktf, rpl
icht . . . . ucf
ie . . . sih, rwn
ien . . . . uzp
ier . . . . kky
ière . . . . amw
iers . . . . reb
ies . . . . kyj
ig . . . . . scf
il . . . . . azh
illy . . . . kcg

*im . . rhq, uph
*in . . . swf, adi
ion . . . . rye
isch . . . . uuw
*ist . . . utb, klz
j . . kxm, rsk, uhh
*ja . . . . sml
*je . . . . uui
k . . apl, rbi, shx
keit . . . . avm
ken . . . . khv
kl . . . . . rjk
kr . . . . . umj
l . . agf, kvu, ruy
la . . . . . syv
le . . . . . kib
les . . . . arp
ler . . . . sde
lich . . . . kzf
ll . . . . . rfk
lles . . . . anp
los . . . . uyu
ly . . . . . rxl
m . udw, sjw, klo
maison . . rok
*mal . . . . uma
*man . . . ali
me . . . . ksf
men . . . . abl
mer . . . . szf

*mit . . rly, unk
mm . . . . khx
mon . . . . awx
mons . . . sgc
mont . . . rdp
mpf . . . . aqe
n . . rzn, uuf, kig
*nach . ubt, skh
nd . . . . rsh
ne . . adp, kqk
nen . . uix, swl
nes . . . . rqp
*neu . . . rwz
ng . . . . kdv
*nie . . . . aru
nk . . . . . sep
nn . . ane, red
ns . . . . . klc
nt . . . . . uze
ny . . . . . sqk
o . kue, roe, neu
ö . . . . . auk
*ob . . . . szi
oire . . . . ukn
ois . . . . rlr
oix . . . . khw
on . . . . aww
ons . . . . saf
ont . . . . rcm

Blinde Signale . . . . . ard, kye, ukl, rrk, sqv

*an Stelle von	rzd	antreten	kwy
andauern	aic	Antwort	rtr
andere	rdn	anwesend	ugc
Änderung	sgr	Anzahl	snv
anfangen	awy	*Anzuge, im	ryd
anfordern	kax	Apparat	uvd
Anforderung	rlf	Arbeit	kjy
Anfrage	ukt	arbeiten	apm
Angabe	sze	Armee	rdm
angeblich	aho	Armeeoberkommando (A.O.K.)	sgt
angegriffen	kuc	Artillerie	awv, kho
angreifen	uev	*eigene —	rji, uln
Angriff	rtk	*feindliche —	ste, agg
Angriffsstreifen	sqf	*Kommandeur d.—	rvj
Angriffsvorbereitung	rxg	*leichte —	rpq
anhalten	uyb	*schwere —	sgx
anlegen	knx	Artillerie-Beobachter	kjn
*Anmarsch, im	ake	Artillerie-Feuer	rvi, ksi
Anmarschweg	kyy	*eigenes —	uct, sjn
Annäherungsgraben	sdl	*feindliches —	uyc, kke
Annäherungsweg	azs	Artillerie-Flieger	aot
anrufen	kdw	Artillerie-Meßtrupp	rei
Ansammlung	rgq	Artillerie-Stellung	kzu
anscheinend	uiy	Artillerie-Tätigkeit	scg
Anschluß	svl	Art.-Unterstützung	asr
ansetzen	afj	Artillerie-Verbindungsoffizier	kce, rhm

Blinde Signale . . . . . ugr, rif, seh, kqx, avd

Art.-Vorbereitung	upy	auflösen	kzk
*ohne —	sxq	Aufmarsch	scl
Arzt	ach	aufnehmen	azj
auch	krk	aufrecht erhalten	kci
*auf	kud, rpu, ucz	aufreiben	rnn
Aufbaumeldung	rwl	*aufgerieben	sjf
aufbrechen	uhm, slr	Aufsatzschieber	uik
Aufbruch	kpl, uuk	Aufschlag	svb
*auf d. rechten Flügel	kjp	Aufschlagzünder	aeq
*auf d. linken Flügel	apd	Aufstellung	kxl
*auf der ganzen Linie	rdu	Augenblick	rsq
*auf Hintergelände	sgp, khn	*aus	siw
*auf Stellung	aad	*aus Richtung	rqh, axj
*auf Vorgelände	rjj, umq	ausbleiben	uhp
auffällig	syd	ausdehnen, sich	snq
auffahren	abb	ausführlich	ryg
*Aufforderung z. Schuß	ayd	ausfallen	uwr
*Aufforderung z. Salve	agq	Ausgang	kip
*Aufforderung zum Wirkungsschießen	ksk	ausgenommen	aqs
Aufgabe	rpm	ausheben	rcp
aufgeben	ucq	Auslade-	sar
*aufgerieben	sjf	ausladen	axq
aufhören	rwh	ausreichend	kgi
*hat aufgehört	uyj	aussagen	rlk
Aufklärung	kkg	ausschließlich	ukg
Aufklärungseskadron	aoh, rej	ausschwärmen	stg

Blinde Signale . . . . . abt, uuv, rfu, sbr, khc

Appendix 8D.—AN EXAMPLE OF THE FIRST THREE PAGES OF INSTRUCTIONS AND TABLES FOR ENCIPHERING WORDS NOT IN THE *SATZBUCH*

Buchstabierverfahren.

Das Schlüsseln.

1. Ersetze in dem zu buchstabierenden Worte ä durch ae, ö durch oe, ü durch ue (z. B. Düsseldorf = Duesseldorf) und zerteile das Wort in Buchstabenpaare. Bleibt dabei ein einzelner Buchstabe übrig, so hänge an ihn einen als wertlos erkennbaren Buchstaben, z. B. j, x, y oder q an.

Beispiel: Das Wort „Duesseldorf" ergäbe:

du — es — se — ld — or — fx

2. Schlüssele die so gebildeten Buchstabenpaare mittels der „Schlüsselungstabelle". Dies geschieht, indem man die Buchstabenpaare aufsucht und sie durch die in der Tabelle neben ihnen stehenden Buchstabenpaare ersetzt.

Beispiel: du = lz, es = jt, se = ch, ld = se, or = bv, fx = wd.

3. Vor jedes so gefundene Geheimbuchstabenpaar setze je als dritten Buchstaben a, k, r, s oder u.

Beispiel: klz ajt chu sse rbv swd.

4. Zähle die auf diese Weise gebildeten dreisteiligen Signale, suche das ihrer Anzahl entsprechende **„Buchstabiersignal"** auf und setze es vor diese Signale. (Die Buchstabiersignale befinden sich auf der folgenden Seite.)

Das Buchstabiersignal gibt dem Entschlüsselnden an, wieviele hinter ihm folgende Signale nicht im Satzbuch aufzusuchen, sondern mittels des Buchstabierverfahrens entstanden sind.

Beispiel: klz ajt uch sse rbv swd.

Es sind 6 Signale. Das Buchstabiersignal für „es folgen 6 geschlüsselte Buchstabenpaare" lautet: upf.

Es wird vor die Signale gesetzt

upf klz ajt uch sse rbv swd.

Buchstabiersignale.

Es folgt 1 geschl. Buchstabenpaar	—	uty	ala
Es folgen 2 geschl. Buchstabenpaare	—	ata	sle
„ „ 3 „ „	uso	kmd	rsa
„ „ 4 „ „	aua	rik	uoa
„ „ 5 „ „	kti	sie	uzu
„ „ 6 „ „	rtw	upf	kdc
„ „ 7 „ „	awj	rir	snu
„ „ 8 „ „	svr	asu	kze
„ „ 9 „ „	rce	ajm	uvc
„ „ 10 „ „	uli	stj	amz
„ „ 11 „ „	—	kqe	uup
„ „ 12 „ „	—	rau	apo
„ „ 13 „ „	—	kpu	ugi
„ „ 14 „ „	—	adz	rhn
„ „ 15 „ „	—	sck	klw
„ „ 16 „ „	—	rvp	ufu
„ „ 17 „ „	—	aaq	syz
„ „ 18 „ „	—	sam	kbz
„ „ 19 „ „	—	uaa	soe
„ „ 20 „ „	—	asa	kxz

a		b		c		d	
aa	nu	ba	ku	ca	ez	da	sv
ab	ha	bb	ah	cb	ir	db	hl
ac	oe	bc	vo	cc	zg	dc	rx
ad	hc	bd	ft	cd	ba	dd	ge
ae	xf	be	sm	ce	up	de	vh
af	gs	bf	ev	cf	lp	df	la
ag	bf	bg	no	cg	tb	dg	ob
ah	qa	bh	nf	ch	ar	dh	lf
ai	kb	bi	gq	ci	rn	di	fr
aj	is	bj	qr	cj	er	dj	qt
ak	vz	bk	kw	ck	st	dk	aj
al	wt	bl	oy	cl	dt	dl	uc
am	fi	bm	jx	cm	kg	dm	sz
an	nk	bn	tx	cn	ye	dn	fx
ao	gh	bo	fl	co	ke	do	nm
ap	sc	bp	xz	cp	vt	dp	wl
aq	id	bq	kk	cq	yy	dq	ac
ar	yi	br	rt	cr	qm	dr	eh
as	fv	bs	ue	cs	hj	ds	yw
at	zk	bt	ik	ct	pn	dt	sr
au	ed	bu	fa	cu	gj	du	lz
av	rh	bv	xk	cv	ni	dv	jk
aw	jn	bw	he	cw	ot	dw	zi
ax	to	bx	ys	cx	jm	dx	kn
ay	mm	by	zu	cy	xq	dy	cv
az	vb	bz	jd	cz	dn	dz	pi

e		f		g		h	
ea	pq	fa	dj	ga	fn	ha	rv
eb	pl	fb	da	gb	el	hb	tq
ec	zp	fc	xi	gc	kd	hc	mi
ed	iw	fd	vw	gd	ww	hd	qg
ee	zs	fe	bi	ge	et	he	zd
ef	wh	ff	so	gf	ut	hf	an
eg	hr	fg	aa	gg	ji	hg	nq
eh	oj	fh	pe	gh	zq	hh	af
ei	gv	fi	kl	gi	hf	hi	ze
ej	tv	fj	ph	gj	xp	hj	lc
ek	ia	fk	av	gk	vp	hk	kt
el	qh	fl	xx	gl	ja	hl	ui
em	sy	fm	gt	gm	nc	hm	fo
en	az	fn	jr	gn	qv	hn	pd
eo	fc	fo	ov	go	iy	ho	fe
ep	nt	fp	ht	gp	si	hp	ll
eq	bs	fq	th	gq	fu	hq	ol
er	ky	fr	gd	gr	wj	hr	eb
es	jt	fs	ql	gs	pb	hs	sd
et	ao	ft	ei	gt	hw	ht	gk
eu	dg	fu	un	gu	sk	hu	qz
ev	vu	fv	na	gv	ee	hv	yn
ew	fk	fw	ig	gw	rp	hw	di
ex	ug	fx	wd	gx	cn	hx	vj
ey	zn	fy	go	gy	or	hy	kp
ez	ga	fz	zw	gz	ak	hz	jw

Schlüsselungstabelle 140 (a—h)

Appendix 9.—EXTRACTS FROM A BRITISH ARMY FIELD CODE*

SECRET

This Document is the property of H. B. M. Government, and is intended only for the personal information of _____ _____ and of those officers under him whose duties it affects. He is personally responsible for its safe custody and that its contents are disclosed to those officers and to them only

SECOND ARMY TRENCH CODE

COMMON WORDS AND PHRASES

046	About	060	In front (of)	074	Position
047	Against	061	Left	075	Quarter
048	Back line	062	" flank	076	Quickly
049	Behind	063	Line	077	Rear
050	By	064	Located (at)	078	Rendezvous
051	Can	065	No, not	079	Return
052	Centre	066	North	080	Right
053	East	067	Now	081	" flank
054	Enemy	068	Officer (s)	082	Sentry (ies)
055	Flank	069	On	083	Since
056	From	070	Other ranks	084	Slowly
057	Front	071	Our	085	South
058	On front from	072	Parapet		
059	Front line	073	Point		

GAS AND GAS ATTACK

OUR FORCES

153	Conditions are favourable for release of gas	165	Gas alert on
154	What is approximate velocity of wind?	166	" " off
155	Approximate velocity of wind is ____ miles	167	All ready for gas attack
156	Wind dangerous	168	Gas will be released at ____ (time)
157	" safe	169	Gas has begun to be released
158	" has dropped	170	" " ceased " " "
159	Gas	171	" " blown back
160	Are we to use gas?	173	Require (number) ____ gas cylinders
161	You will make gas attack	174	Gas cylinders will be carried up to trenches
162	Am / (____) is/ are/ going to make gas attack	175	" " have arrived
163	This retards release of gas ____ hours from original zero	176	Our gas cylinders damaged by enemy's fire
164	Warn gas personnel to have all ready by ____ (time)	177	" " " leaking
		179	
		180	

*I never saw an original of a British Army field code. The extract here shown has been set up in type from a typewritten copy (of the original) found in a historical file among Major Barnes' papers.—*W. F. F.*

Artillery

Our Forces

Artillery support

314 I (____) require artillery support from (nature of guns)
315 I (____) cannot advance without artillery support
316 I (____) " consolidate (____) without artillery support

Barrage

318 Barrage with (nature guns) required
319 " " " " will begin at ____
320 " " " " " cease " ____
321 " " " " " lift " ____
322 Increase barrage
323 Renew "
324 Stop "
325 Lift barrage to ____
326 Creeping barrage
327 Stationary "
328 Barrage effective
329 Am/ (____) is/are going to advance and artillery should lift
330 Am/ (____) is/are going to advance and artillery should lift to supports
331 Am/ (____) is/are going to advance and artillery should lift to point ____
332 Am/ (____) is/are going to advance and artillery should lift to line
333

Reinforcements

Our Forces

564 Do you require reinforcements?
565 Reinforcements required
566 Require following to make good casualties ____
567 Am/ (____) is/are sending up reinforcements
568 Reinforcements are on the way
569 " have arrived
570 No reinforcements available
571 Unable to get up reinforcements owing to barrage
572 Have reinforcements ready
573 Reinforce front line trenches
574 " support line
575 " troops at ____
578 Am/ (____) is/are being reinforced by ____
579 " (____) is/are moving up in support of ____
580 Reserves at point ____
582

Enemy Forces

583 Enemy is being reinforced at ____
584 " has been " " ____
585 " reinforcements moving up to ____
586 " " " " from ____
587
588

Spelling

841 Commence spelling
014 A
017 B
844 C
021 D
213 E
229 F
848 G
285 H
410 I, J
665 K
852 L
679 M
730 N
741 O
856 P
771 Q
873 R
877 S
T
882 U
894 V
897 W
865 X
905 Y
867 Z
868 Cease spelling

Appendix 10.—REPORT OF 1ST LT. J. RIVES CHILDS *

*I have added the paragraph numbers, for reference purposes. The notation (at the end) "Parker Hitt's initials" is also mine. Otherwise this appendix is a faithful reproduction of the original, errors, insertions, deletions, etc., included.—*W. F. F.*

May 17, 1918.

MEMORANDUM FOR MAJOR MOORMAN.

EXPERIMENTATION WITH OUR CODE.

(1) A. Time. The recording of the frequency of groups, on attached chart, occupied 3-1/2 hours.

(2) One hour and a half after the receipt of the messages, the first letters were identified and the word k-i-l-l-e-d, was solved at the end of the third hour.

(3) The solution of the cipher alphabet was complete at the end of the fifth hour, and the messages were completely decoded and set up on the typewriter at the end of the tenth hour.

(4) A cursory examination of the messages indicated that the behavior of the group TKG offered the most likely point of entry. This group was isolated in the following manner, attention being paid solely to its repetition as a doublet.

	BCN	TKG	TKG	BCN
	BCN	TKG	TKG	GRO
TWS	BCN	TKG	TKG	GWY
TWS	BCN	TKG	TKG	GWY

Around TKG was noted the repeated appearance of BCN, GRO, GWY, etc., Inspection was made for the repetition of these groups throughout the forty-four messages. Other groups such as DCA, ACZ, FKA, TWS, were also noted as tending to appear in the vicinity of TKG.

(5) TKG was immediately assumed to be a single letter, and resort was had to the frequency of occurence of double letters in English. T and S were assumed for the value of TKG, and immediately discarded, not appearing to fit. L, third in point of frequency as double letter in English was next assumed. The spelling group ED, was the most natural to assume as following the LL. It will be noted that in two cases after the repetition of TKG there is a group whose initial letter is in two instances G, i.e., GWO and GWY. The group representing L ends in G in the cipher, therefore, this letter constitutes a check on our assumption. Reference was had to the book, and the result of assuming TKG to represent the code-word MIH, (L) and GWY to represent HEG (ED), was confirmed. Meanwhile the groups which surrounded TKG, as noted above, had been identified as single letters, not only because of their appearance, coincident with TKG, but also because of their appearance as a double, i.e.,

SCU	DCA	DCA	BCN
ACZ	GRO	GRO	BCN
GRO	ACZ	ACZ	FKA

The fact that these groups appeared in this manner and at the same time were the most frequent groups appearing in the forty-four messages, identified them as letters or spelling groups. The doublets could certainly be identified as letters.

(6) In the part which had been deciphered L-L-ED, it was next assumed that the group preceding must naturally be a vowel. The letter "I" was assumed giving "I-L-L-ED", K as preceeding "I" following as an inevitable assumption. These results were then checked up by the means of the code book, and confirmed. The fact the such a word, as "K-I-L-L-ED", does not appear as a code-word, when it must necessarily form constantly a part of messages in the vocabulary of the Army, illustrates one of the defects of the code. There are certain words such as this, for example, INSTRUCTION, ADVISED, YOUR, SNIPERS, FORCING, TRANSFERRED, SENT, BAVARIAN, AUSTRIAN, ENTANGLEMENTS DURING, which when employed any number of times, as they are certainly likely to be, without alternative readings for the common letters of the alphabet and for the common spelling groups, will make the decipherment and decoding of any considerable number of messages received by the enemy, a simple task. It might be suggested for example, that where the groups, ED, ING, LY, MENT, are represented by the same values on every page, as many different values might be given them, as they occur. If the verb "WORK" is encoded on page 35, and the past participle "WORKED", is to be used, it would be no more difficult, and would result in no more confusion, for the operator to make use of the value given ED, on that particular page, as distinctive from the other values that might be given ED on the other pages. In receiving the message the operator would naturally decode the message by the use of the value of ED, to be found on the page on which he found himself. This would also result in a check on the two groups in case a mistake had been made.

(7) Upon tabulating results, it was found that in every instance save one every premise which we had made was confirmed. Following is the frequency of the groups which we had isolated originally and assumed to be letters or spelling groups

Enciphered code group	Frequency	Code Group	Value
TKG	23	MIH	L
FKA	30	SIK	S
DCA	23	ROK	R
YCI	24	GOF	D

AVA	10	KYK	H
BCN	[illegible]	LOP	I
GRO	18	HAW	E
GWY	19	HED	ED
DRF	20	RAS	. (period)
SWZ	16	VEN	TO
BVO N	14	lyw	ING
HVL	11	TYD	T
SCU	9	VOZ	U

Seventy perdent of these prove themselves to be letters, twenty-two percent spelling-groups. Group for period was the only one we had miscalculated, out of thirteen.

(8) The fact that the code is enciphered [illegible] not complicate it, nor does it appear, that it would long succeed in puzzling the enemy. If a group TKG, is a code group, representing a single letter, and it is the only code group representing the letter, it might be enciphered and re-enciphered, to the nth power, without altering in the least, its behavior and its positive identification as a letter, when observed throughout any number of messages. The fact that TKG, is represented by MIH, which in turn represents L, is of no concern to the enemy, and is a matter about which he will be little troubled. He is satisfied to know that TKG, represents L, and all the twistings and turnings in the world will not alter its identification as L, as the code stands in its present form.

(9) Of course the use of code-groups to represent letters and spelling groups is, in a code, inevitable, but the worse feature of this evil, may be avoided by the employment of [illegible] alternative groups, to represent the letters and spelling groups, which must appear most frequently. Otherwise it would always be possible for the enemy to identify the cipher portion, (that is, the groups representing letters and spelling groups) at a glance, and from this point, to isolate these groups, and by the use of simple frequencies employed with ciphers, to decipher and decode them, will be a matter of small moment. To illustrate by example: AVA, was identified almost immediately after the code was in our hands, as a group representing a letter. The initial and final letters were identical. What letter was there in the code whose initial and final letters were the same? There was only one-H-, we were not even under the necessity of trying and fitting from among several.

(10) From this it would appear, that if the code is to be enciphered at all, as it stands now, three different alphabets should be employed, one for the initial letters of the code group, one for the final letters and one for the middle letters.

(11) Attached to this report is a chart, showing the frequency, of the groups, as made up immediately upon receipt of the messages. This chart illustrates quite accurately, as we have previously noted, the means by which simple cipher frequencies may be employed, and will be employed by the enemy, to arrive at the solution of the code.

(12) Furthermore, it will be noted that there are certain columns of the chart, column G for example, which stands out prominently from the remainder. Suppose we turn to page 14 and 15 of the code book, which contains the code groups for E and its spelling groups, ER, EN, the most frequently occuring letter and the most frequently occuring spelling groups, in our language, contained on the same page, with a long entry of code groups, relating to the "ENEMY ADVANCE STOPPED" and etc., The natural supposition is, that the initial letter "H", by whatever means it may be enciphered, will always be identified, in any considerable body of messages, since it is seen to be the initialed letter of a series of code groups, representing, letters, spelling groups, and phrases, which are bound to occur most frequently in messages passing in the army. This fact illustrates the glaring fault of permitting the contents of the code, to be encoded, with groups, whose initial as well as whose final letters run in alphabetical sequence. Most often the initial letter of the code, coincides with the initialed letter of the matter to be encoded. This, while not so marked at the beginning of the book, gradually increases, so that towards the end the letters run practically parallel. Thus, the initial code-letter, "S" constitutes, the initialed code letter of subject matter which begins almost exclusively with "S". The initial code letter "N" on page 23 embraces the code groups from "N NORTHEASTERLY". Certainly the enemy would eventually determine it, and if the code groups after decipherment, began in E, he would not look for its translation, in a word beginning with Z. Take in message "No.28." for example and assuming the beginning, "SHORT OF" as solved, the fact that the next group is RUB, will at once warrant the assumption that "MUNITIONS" is an erroneous hypothesis and that "RATIONS" in alliteration with that group, is a quite probable solution.

(13) And again, it might be further added that the fact that there exists no blind groups or nulls, anywhere in the code, materially simplifies the work of the decipherer and decoder.

(14) Lastly, the option for the use of words as singular or plural, without any qualifying mark, gives rise to a multitude of misinterpretations, To quote further by example, in the message "Aeroplane(s) coming out" the receiver of the message would not be able to determine whether a single plane was approaching, or a squadron. Also, in the message "Rush rifle(s) ammunition" it is not clear whether rifle ammunition is to be rushed, or rifles and ammunition.

(15) To summarize, therefore, the weaknesses of the present code as revealed in our attack.

1. The absence of
   (a) Alternative groups, to represent letters and
   (b) Nulls or blind groups, [illegible] makes the cipher portion of the code, stand out in sharp relief, and makes the solution of it by simple frequencies a mathematical certainty.

2. The employment of a simple substitution system to encipher the code, the initial letters of whose groups, coincides most frequently, with the initial letter of the text encoded, affords the best sort of check to the work of the enemy decoder, and offers no security.

3. The Employment of an alphabetical sequence, to distinguish the code groups, through-out the book, gives a frequency, to certain initial letters which cover the portion of the book most used, as pages 14 and 15, for example, already noted, as to enable them to be identified by the frequency of their occurence.

4. Omission of very common military words, which necessitates, there being spelled out, when it is necessary to employ them, thereby facilitating and practically insuring the decipherment of the text by the enemy.

5. The fact that there is no distinction made between the singular and plural forms of nouns is certain to give rise to grave misunderstandings.

Note: In the forty-four messages, given us, to be deciphered and decoded, errors amounted to about 1 per message.

Every point above noted is well taken and can be corrected in a new code. P. H.

(122) Parker Hitt's initials

NO. 1. OR ZCM FRT MRL MKZ ZWI DKL MRY HRA TWS BCN
TKG TKG GWY MRL UES

NO. 2. OR SWZ PEM YRD SRI DVD UKF HVI DWI NKL MWT
HVL AVA IRM MWB PVF MRM PWS UKH TVM PWO YCI
GRO IKG DWG NRL BCN GVO FWN PVF TCP AWH

NO. 3. OR PCY YRM NCF YVD TRZ ICP YVF HVL BVO SCU
BCH FKA AVA UKI GWS NCL NRL

NO. 4. OR DCA SCU FKA AVA FWB PVY MWZ DWH MCY

NO. 5. OR LRO BRI SWA UEM NCF UCF ICP AEI URI TCL
SEP SWZ DEZ GWS ZWG

NO. 6. OR MWY HCS ZEN GWY SWZ GEO UES HKU MVL UGA
SCL

NO. 7. OR ICA YCI UKF FRT SRZ BWO NKL MWZ SRM LKB
MRH PWS UKD DKZ SWZ AEP BWO NRL BCO BKD

NO. 8. OR YRS FKA BCN YCI GEN PKL YCA SWZ NCF LEN
NKZ MRB BVG FWB TCP ZEA GRO GWY PVY PVF DVZ

NO. 9. OR YVI MWY ZWI UVY DCA YRD MWZ NCB LEM GWD
HVW PVH ZWY FKA BEG ACL NWA FCB YKT GWY IKG
UVY DCA DEU PWO YCI SVP TRS GRO UWO IVF NVF
TCA GWY HET LES BVO DCA SCU FKA AVA GWY

NO.10. OR YEL TWB PVY DCA SCY FKA AVA GVO DEP FKA
AVK HET IWG GVH YCI MRI ZWI TWS BCN TKG TKG
GWY SVD DCA TWG BYO ACY TKG FRT

NO. 11. OR BVA DCH NEB

NO.12. OR DVN YRS DKP YCI AKB LKH DEM BRO YVU YCI
FKA NVF TRD TWG NWA ZWI BKT GVP SRS NRD TWS

NO.13. OR UWN TRS SRI ZRA HVL GRO DCA UEM TWS UKZ
YCI NRD GRO FKA BWH NRL AEG SES SRI LEP
LKY GWY AKB FRB LKN

NO.14. OR BWT DEZ YCI YVS FKA GWD HVL IKG DWL NVF
DEP MVP ZRD SWZ FRI NWA TEL FKA GWD HVL
LKB MWB MKO PWS DKH TWP FKA PWO HVL TRS
GVO BCH

NO. 15. OR UEM LEP BWI DEZ YCI BVZ TRZ FKA FWZ LKN
ZEP BCN HCN

NO.16. OR SRF LEP LKN GWS FEG ZRY GWY AKB ZRA TRZ

NO.17. OR AVA SCU DCA DCA BCN ICP BKS SRB UEM FWB
AWG

NO.18. OR AWZ UKH AKY GWY MWY UEO IKG MRB SCL IKT
TKG GRO PVN GEN FKA BWN ACD AES FWB PVD
TKI FCL URI MCM LVA

NO.19. OR PWO YCI SVP TRS GWY AEL LWT UKF NKF NWO
TKG TVM FCB BRH SRI ZWI HVI SWZ FVD LKN TWO
NKN ZET TEN NVY FKA GRO TVM HVL

NO.20. AR ACZ GRO GRO BCN SVD BCN FKA AVA BCN AVB
HWS LES PVN FKA DRF NRD AVA AKB AVA PED
PVF GRO ACZ ACZ FKA DRF

NO.21. OR LEP SVS GWY FCB DKH

NO.22. AR BWT DCA FRT DEY DRF UKZ YCI NWO HVL UVY
LRM DKU LRS TEL YCP

NO.23. OR GWS AWG LCF TEU YCA YCI ACZ TKG LKM FKA
UET LKB LCN PKG LRH DCA LKB YCI SCU DCA
BVO ZVP IEU GRB

NO.24. OR BEG FKA NVF GRO IKT SWZ DCA AEP UKF BEG
FKA NVF GRO IKT HVL MRP MEP SRM DEU LKB
LCF NIO SVP BCN TKG TKG BCN GEN SWO AEY

NO.25. OR NWM TET GWY LKB TVM BCN ACZ ZEA GRO SVP
BCN TKG TKG GRO FRT ZRY BRO GEP DVY ACI SCL
DEM LVT FKA GWD HVL

NO.26. OR SCL LCF TEU YCA GWY IKG GWS FVT UCL PKL
DVS ZCH TEZ GCO DCA BEG HKS DCA SCU IKT SWT
FKA SVS GWY SVD SCU AVA

NO.27. OR UES YRL BRH HVL DCA PVN FKA GVO GEN DCA
DCA GWY YRI YRD SWZ AWB FEN FCD NWN SWZ
HVI ZEY DWI

NO.28. OR FVS NWA DEM DRF ZWI AVA SEM ALZ FKG DRF
UWN TRO SRI ZRA HVL GEN UEM SRI DVD

NO.29. OR BCA DRF GEG DRF DET DEM UET BVO SWS GVO
DEG GRO

NO.30. OR GWD VKG UEN GWS DRB YCI SCU DCA BVO ZVP
MRL DKG DRF LCN PWO SVP PWO DCA BCN PVN
FKA DRF MRL TWS BCN TKG TKG GWY MRY UES
UKP FVM URA FCD SRB

NO.31. OR MRL YRD UKF LKH GCN IRM BCN PVN YCI HKS
TEL LKB MWA PWS HRZ AKB LKH NKZ DES DRF
AKY LEP

NO.32. OR MRI TWS BCN TKG GWY YRL MWM UES YCI
SCU DCA BVO LKH DRF MWZ MRM ZWF AEL SCL
ICT YCI DKG HVY SCL NCB YCI DRF GVP SRS
DCI NRB

NO.33. OR HWD DCA FKA YCI NRD BVO AEZ UET PVU
BVO GWS AKB IKT BVO SRB SWZ TWO SEY YKT

NO.34. OR FCD LCA SWZ DEF DWN GKT TET YCI TEL
NRP NIA BWH TKG TKG NRD SVP BCN TKG TKG
GRO

NO.35. OR LES TKG BCN GRO SVP GIY SWA AKB HVG
SWZ AED BEG PKD YRL ZEN SRA HED DRF LKH
UKH HED ACH TKG UEM SRA BKA

NO.36. OR SEA DRF AEI BVL LCN DRD TCT ZET BVA
YCL UCF PKH

NO.37. OR BCM SEZ DEB NWA LCN FCB IRZ GWY IKG
PCY DRF LRI AVL IWF TWG GRB

NO.38. OR AEL DKP BVO ACH DRF AEY LWT NRL BCO
BCN GWY FRT

NO.39. OR UWL DWZ DCA PWO BEG GWY PEM ZVP SVP
TRS BCN LCN BCN TKG BCN SCS DWZ

NO.40. OR ARZ IKY UCT ZEN GWY NKZ ZKP DRF MRY
SWZ FRI TEL

NO.41. OR MRL ZWI UKF AEH NVY SWZ GWS TEL SKM
PVF DWI SKH AEU FKA ZEB LEM GET PVH ZWY
FKA

NO.42. OR TCL GWD DCH GVP MRD ZKA ACM MRU PWS
SED DEZ HRZ

NO.43. AR PEM HKU LCP SRI NVF LWO BCN ZRY HVL
GEN TRS IVQ BVO HKM URP AKB BRD UEM PWO
DRH

NO.44. OR TKF FKA LKH TVB IKG SRI NEU PKG IVF NVF
TKG TRS BWH YCI FWP FKA FRZ GWY UEM GVZ TRZ
NWA HWA FKZ NKI UCB DRF AVB HVZ DCA NRD SCU
LCN TKG GRO UEM TCT UEM SRI AKF IKI UWI GES
GWY LKB DKL DRF BRH HVY HCB FKA AKB SRI LKH
NWI FKZ YKM DRF HCU MEP YCH MWA ZKB BVO MRP
MEB UES YWB BVO ICT YCI SCL LCB BVO ACB NCI
FCD DEM LKN DRF IKT NRD TKG

MESSAGE NO. 1.

MORNING REPORT 242 MEN PRESENT 4 SICK KILLED 2 WOUNDED

MESSAGE NO. 2.

TO ALL COMPANIES THE RELIEF WILL TAKE PLACE ON THE 24TH BETWEEB 23 AND ZERO O'CLOCK WILL BE MADE BY PLATOON(S) NOT IF (probably means NOTIFY) RIGHT LEFT FLANK.

MESSAGE NO 3.

AEROPLANE(S) COMING OUT OPPOSITE DIRECTION CANNOT DISTINGUISH WHETHER ENEMY OR NOT.

MESSAGE NO.4.

RUSH RIFLE(S) AMMUNITION 25 POST(S) 54.

MESSAGE NO.5.

ARE HAVING HARD TIME WITH OUR WIRELESS CANNOT GET WAVE(S) LENGTH UNABLE TO RECEIVE ENEMY MESSAGES.

MESSAGE NO.6.

TWENTY STRETCHER BEARERS NEEDED TO EVACUATE WOUNDED STATION(S) 85 --- (probably Z) TRENCH(ES)

MESSAGE NO.7.

CAPTAIN D., WILL REPORT THESE HEADQUARTERS ON THE 25TH AT TWELVE O'CLOCK WIDTH (probably WILL) PROCEED TO GENERAL HEADQUARTERS NOTIFY HIM.

MESSAGE NO.8.

CONSIDER ABANDON SECOND LINE DAMAGE TO OUR BATTERY ON TIME 6 INCH RIFLE(S) LEFT NEED AMMUNITION AND REINFORCEMENTS.

MESSAGE NO 9.

DETAIL 4 MEN YOUR COMPANY 25 ORGANIZE BARBED WIRE ENTANGLEMENT IN FRONT OF SECTOR(S) COVERED BY YOUR REGIMENT ADVISE WHEN COMPLETED SUPPLIES BEING RUSHED.

MESSAGE NO 10.

DEFECTIVE AMMUNITION RAPID TRENCH MORTAR AMMUNITION SH FRESH SUPPLIES BREACH EXPLODED 3 MEN KILLED. WRITING --- REPORT.

MESSAGE NO. 11.

INCREASE RANGE OUR ARTILLERY SHELLING US.

MESSAGE NO. 12.

REINFORCEMENTS HAVE ARRIVED CON PREPARED FOR ATTACK (probably means COME PREPARED FOR ATTACK) RATIONS HAVE BEEN DISTRIBUTED SPIRIT OF MEN HIGH EVERYTHING O.K.

MESSAGE NO. 13.

WHAT IS THE MATTER WITH K. WHY DOES HE NOT GIVE US BARRAGE ASKED FOR REPLY AT ONCE

MESSAGE NO. 14.

HAVE YOU RECEIVED DISPATCH SENT BY PISTOL PRE 84 MAY HAVE TO REPAIR LINE(S) SENT AT 23:38 O'CLOCK ? IS NOT S T IS EVERYWHERE IED

MESSAGE NO. 15.

WITH BARRAGE HAVE NOT RECEIVED INDICATIONS RIFLE(S) PIT(S) AT ONCE MUST I STOP

MESSAGE NO. 16.

THICKEN BARRAGE BARRAGE AT ONCE ENEMY SENDING MASSED FORMATION

MESSAGE NO. 17.

HURRY CANNOT HOLD THEM WITH RIFLE(S) FIRE

MESSAGE NO. 18.

FIRST LINE WILL BE FOLLOWED 20 YARDS BY 6 TRENCH(ES) CLEANERS HAVING GAS GRENADE(S) RIFLE(S) AND KNIFE(VES) SECOND(S) WAVE(S) 50BEHIND

MESSAGE NO.19.

ADVISED GERMAN(S) ARTILLERY WILL OPEN FIRE ON L M SECTOR HAVE THE MEN TAKE TO SHELTER AT ONCE KEEP ONLY NECESSARY LOOK OUT SENT

MESSAGE NO.20.

GEE I WISH I HAD SOME BEANS. OF FOR H ALSO AND EGGS.

MESSAGE NO.21.

BARRAGE WANTED SECTOR ?.

MESSAGE NO. 22.

HAVE YOUR REPORT READY. WHY DONT YOU ANSWER QUESTION ARE LINE(S) CUT.

MESSAGE NO. 23.

ENEMY FIRE(S) BADLY DAMAGES GLASS WORK(S) AT BACARRAT DURING NIGHT CHURCH STEEPLE(S) DOWN.

MESSAGE NO. 24.

INSPECTOR GENERAL WILL INSPECT 167 REGIMENT AT BADONVILLIER TOMORROW, GET READY.

MESSAGE NO. 25.

OBSERVATION POST(S) LOCATED AT MILLE REPORT(S) MASS HAVE KEEN ENEMY TROOPS REINFORCE FRONT LINE TRENCH(ES) RATION(S) BEING SENT

MESSAGE NO. 26.

TRENCH(ES) BADLY DAMAGED BY ENEMY SHELL(S) WILL NOT BE ABLE (TO) REMAIN MUCH LONGER INSTRUCTIONS WANTED.

MESSAGE NO. 27.

WOUNDED, HAVE TRANSFERRED COMMAND COMPANY TO FIRST SERGEANT SEND OFFICER TO TAKE MY PLACE

MESSAGE NO. 28.

SHORT OF RATIONS. MEN HUNGRY. WHAT IS BEING THE MATTER WITH THE RELIEF

MESSAGE NO. 29.

HOUSE. ENGINEER. REARGUARD RATION WORKING TOGETHER F READY (TO) E.

MESSAGE NO. 30.

ENCOUNTER WITH ENEMY PATROL DURING NIGHT 2 PRISONERS. BAVARIANS. 2 KILLED 4 WOUNDED WHERE SHALL WE SEND THEM

MESSAGE NO. 31.

TWO COMPANIES WILL ATTACK ENEMY POSITION BETWEEN I AND ST LINE AT TWENTY-TWO O'CLOCK SIGNAL FOR ATTACK ONE RED STAR SHELL. FOLLOW BARRAGE

MESSAGE NO. 32.

THREE KILLED, 16 WOUNDED DURING ATTACK. 250 METERS GERMAN TRENCH(ES) CAPTURE(D) PRISIONER(S) TAKEN TRENCH(ES) ORGANIZE(D). EVERYTHING QUIET NOW.

MESSAGE NO. 33.

SNIPERS DOING GOOD WORK ANNOYING ENEMY FORCING THEM TO KEEP UNDER COVER.

MESSAGE NO. 34.

SEND AVIATOR TO RECONNOITER POSITION ENEMY FIELD ARTILLERY LOCATED LINE(S) N.W.OF HELLOVILLE.

MESSAGE NO. 35.

BELIEVED TIME FOR TANK(S) TO GO IN ACTION, NEED THEIR SUPPORT. ATTACK WILL BE SUCESS GAS ATTACK SOUTHWEST WITH THEIR HELP.

MESSAGE NO. 36.

UNDERSTOOD. GET IN TOUCH WITH B PERFECT LIAISON NECESSARY INCREASED WIRELESS ACTIVITY.

MESSAGE NO. 37.

HOSPITAL(S) UNIT REAR OF B SECTOR BOMBED BY AEROPLANE(S) ANTI-AIR-CRAFT GUN BROUGHT IT DOWN.

MESSAGE NO. 38.

GERMAN PREPARING GAS ATTACK. GET READY ARTILLERY NOTIFIED REPORT.

MESSAGE NO. 39.

WEATHER CONDITIONS POOR RAINED ALL NIGHT VISIBILITY POOR

MESSAGE NO. 40.

FIELD BUZZER WIRE NEEDED one 4 TO REPAIR LINE(S)

MESSAGE NO. 41.

TWO MEN WILL GREEN (probably mean GO) OUT TO ENEMY LINE(s) TONIGHT AND PLACE T.P.S. GROUND S (s probably abb. for SET.) NEAR BARBED WIRE ENTANGLEMENTS.

MESSAGE NO. 42.

LENGTHEN RANGE EVERY 10 MINUTE(S) FROM 15 O'CLOCK UNTIL RECEIVE SIGNAL(S)

MESSAGE NO. 43.

ALL STATION(S) ATTENTION THE P ARTILLERY SUPPORT I MASS TER IS COMING SOON WATCH FOR HAS STOPPED WITH A PERISCOPE.

MESSAGE NO. 44.

LAST NIGHTS ATTACK MADE BY THE OUR LIGHT ARTILLERY ACCOMPLISHED RESULTS REQUESTED WITH EXCEPTION OF SMALL SALIENT ON THE LEFT WING. HAD TEARROUBLE (probably TROUBLE) WITH LIAISON WITH THE FRENCH BUT WELL ESTABLISHED ASSEMBLE PRESENT HAVE TAKEN STEPS FOR THE ATTACK(S) OBSERVE SALIENT CORRESPOND. STRIP 67 DEAD 22 MISSING 173 WOUNDED CONSOLIDATING CAPTURED TRENCHE(ES) AWAITING FURTHER ORDER(S) SEND RATION(S) AT ONCE COL

Appendix 11.—THE FIRST AEF FIELD CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY FORCES

Confidential

The American Trench Code

No. 768

This Code Book has been issued to

for official use under his direction only.

By Command of General Pershing:

JAMES G. HARBORD,
Brigadier General,
Chief of Staff.

Official:
BENJ. ALVORD,
Adjutant General.

A. G. PRINTING OFFICE
1918

INSTRUCTIONS FOR USE OF CODE.

1. This code book will be used, in connection with secret instructions, in transmitting all messages by radio and earth telegraphy, and in all other cases where the message might by any chance fall into the hands of the enemy.

2. To cover a number of possible methods of sending, a four-figure code group and a three-letter code group have been provided for each word or phrase.

3. The first two figures of each figure group and the first letter of each letter group will be found at the top of the page.

4. Throughout the book will be found a number of prefixes and suffixes arranged in alphabetical order. Those most commonly used are repeated in the margin of each page.

5. To code a message, substitute for the word, phrase or sentence to be sent the figure group or the letter group corresponding to it. The code message should never contain mixed figure groups and letter groups, but should be made up exclusively of one or the other.

Example: "Patrol reports indication attack preparation."

Code either	RAL	SAM	LYN	MAN	DIT	RIB
or	2307	2408	1993	2009	1447	2334

6. If a phrase is used several times in the same message, code it differently each time, if possible, by breaking it up into separate words.

Example: "Gas attack" KOT
(Gas) (Attack) KOR DIT

7. Numbers may be sent in code or in the clear, but if sent in the clear they must always be preceeded by the figures 2370 or the letters RUF.

8. If a code book is lost, it must be reported by number at once through military channels to G. H. Q. A. E. F.

9. Destroy at once by burning all scraps of paper on which coding or decoding memoranda have been made.

10. Your secret instructions for this code must *always* be used in connection with it.

11. Inform your subordinates where you carry this code, and of the importance of saving it if you become a casualty.

12. **THIS CODE MUST NOT FALL INTO THE HANDS OF THE ENEMY.**

12-B

01 AB..... 0
02 AC..... 1
03 AD..... 2
04 AF..... 3
05 AG..... 4
06 AK..... 5
07 AL..... 6
08 AM..... 7
09 AN..... 8
10 AP..... 9
11 AR.....10
12 AS.....11
13 AT.....12
14 AV.....13
15 AW.....14
16 AZ.....15
17 EB.....16
18 EC.....17
19 ED.....18
20 EF.....19
21 EG.....20
22 EH.....21
23 EK.....22
24 EL.....23
25 EM.....24
26 EN.....25
27 EP.....26
28 ER.....27
29 ES.....28
30 ET.....29
31 EV.....30
32 EW.....31
33 EZ.....32
34 IB.....33
35 IC.....34
36 ID.....35
37 IF.....36
38 IG.....37
39 IH.....38
40 IK.....39
41 IL.....40
42 IM.....41
43 IN.....42
44 IP.....43
45 IR.....44
46 IS.....45
47 IT.....46
48 IV.....47
49 IW.....48
50 IZ.....49

51 OB.....50
52 OC.....51
53 OD.....52
54 OF.....53
55 OG.....54
56 OK.....55
57 OL.....56
58 OM.....57
59 ON.....58
60 OP.....59
61 OR.....60
62 OS.....61
63 OT.....62
64 OV.....63
65 OW.....64
66 OZ.....65
67 UB.....66
68 UC..... 67
69 UD.....68
70 UF.....69
71 UG.....70
72 UH.....71
73 UK.....72
74 UL.....73
75 UM.....74
76 UN.....75
77 UP.....76
78 UR.....77
79 US.....78
80 UT.....79
81 UV.....80
82 UW.....81
83 UZ.....82
84 YB..... 83
85 YC.....84
86 YD.....85
87 YF..... 86
88 YG.....87
89 YH.....88
90 YK.....89
91 YL.....90
92 YM.....91
93 YN.....92
94 YP.....93
95 YR..... 94
96 YS.....95
97 YT..... 96
98 YV.....97
99 YW.....98
00 YZ.....99

13-C

01 AB.....Decimal Point
02 AC.....4.2
03 AD.....5.9
04 AF.....9.2
05 AG.....9.45
06 AK.....9.5
07 AL.....100
08 AM.....155
09 AN.....240
10 AP.....Sunday
11 AR.....Monday
12 AS.....Tuesday
13 AT.....Wednesday
14 AV.....Thursday
15 AW.....Friday
16 AZ.....Saturday
17 EB.....January
18 EC.....February
19 ED.....March
20 EF.....April
21 EG.....May
22 EH.....June
23 EK.....July
24 EL.....August
25 EM.....September
26 EN.....October
27 EP.....November
28 ER.....December
29 ES.....A. M.
30 ET.....P. M.
31 EV.....o'clock

32 EW.....A
33 EZ.....Abandon
34 IB.....Abandon first line
35 IC.....Abandon second line
36 ID.....Able (to)
37 IF.....About
38 IG.....Above
39 IH.....-Ac
40 IK.....Accident
41 IL.....According (to)
42 IM.....Accurate
43 IN.....Acknowledge
44 IP.....Act
45 IR.....Action
46 IS.....Active
47 IT.....Activity
48 IV.....Activity of artillery
49 IW.....Adjust
50 IZ.....Adjutant

51 OB.....Advance
52 OC.....Advance guard
53 OD.....Advancing
54 OF.....Advantage
55 OG.....Aeroplane (s)
56 OK.....Aeroplane observation
57 OL.....Aeroplane wireless
58 OM.....After
59 ON.....Afternoon
60 OP.....Again
61 OR.....Against
62 OS.....Age
63 OT.....Aim
64 OV.....Air
65 OW.....-Al
66 OZ.....Alert
67 UB.....All
68 UC..... All clear
69 UD.....All communication has been cut (with)
70 UF.....All is well
71 UG.....All of your messages have been received
72 UH.....All ready
73 UK.....All returned
74 UL.....All right
75 UM.....Alone
76 UN.....Along
77 UP..... Already
78 UR.....Also
79 US.....Alter
80 UT..... Altogether
81 UV.....Always
82 UW..... Am
83 UZ.....Am having
84 YB.....Am I
85 YC.....Am not
86 YD.....Ambulance (s)
87 YF.....Ambush
88 YG..... Ammunition
89 YH.....Ammunition depot (s)
90 YK.....Ammunition exhausted
91 YL.....Ammunition for 75 m.m. Field Gun, reduced
92 YM.....Among [charge, explosive projectile
93 YN.....Amplifier
94 YP.....An
95 YR.....-Ance
96 YS.....And
97 YT.....Angle
98 YV.....Annihilate
99 YW.....Announce
00 YZ.....Annoy

—ed—1721—HEG
—ing—1999—LYW
—ly—2083—MUZ
—ment—2121—NEG

27-Z

01 AB.....Was not
02 AC.....Watch
03 AD.....Water
04 AF.....Wave (s)
05 AG.....Way
06 AK.....We
07 AL.....We are about to advance, lengthen range
08 AM.....We are held up
09 AN.....We are in need of
10 AP.....We are losing heavily
11 AR.....We are surrounded
12 AS.....We attack
13 AT.....We cannot
14 AV.....We have withdrawn
15 AW.....We hold the line
16 AZ.....Weak
17 EB.....Wear
18 EC.....Weather
19 ED.....Weather conditions
20 EF.....Well
21 EG.....Went
22 EH.....Were
23 EK.....Were not
24 EL.....West
25 EM.....Westerly
26 EN.....Wet
27 EP.....What
28 ER.....What is the approximate velocity of wind?
29 ES.....What is exact range of objective?
30 ET.....What is position (of)?
31 EV.....What is the situation (at)?
32 EW.....When
33 EZ.....When shall we be relieved?
34 IB.....When will barrage begin?
35 IC.....Where
36 ID.....Where is your headquarters?
37 IF.....Whether
38 IG.....Which
39 IH.....While
40 IK.....White
41 IL.....Who
42 IM.....Whole
43 IN.....Why
44 IP.....Wide
45 IR.....Width
46 IS.....Will
47 IT.....Will be
48 IV.....Will have
49 IW.....Will he
50 IZ.....Will I

51 OB.....Will it
52 OC.....Will not
53 OD.....Will not be
54 OF.....Will signal by
55 OG.....Wind
56 OK.....Wind favorable
57 OL.....Wing
58 OM.....Wire
59 ON.....Wire cutters
60 OP.....Wire entanglement (s)
61 OR.....Wire reel (s)
62 OS.....Wireless
63 OT.....Wireless message (s)
64 OV.....Wireless out of commission
65 OW.....Wireless station (s)
66 OZ.....Wiring party (ies)
67 UB.....With
68 UC.....Withdraw
69 UD.....Within
70 UF.....Within range
71 UG.....Without
72 UH.....Without artillery preparation
73 UK.....Without delay
74 UL.....Wood (s)
75 UM.....Work (s)
76 UN.....Working party (ies)
77 UP.....Worm
78 UR.....Would
79 US.....Would be
80 UT.....Would not
81 UV.....Wounded
82 UW.....Yard (s)
83 UZ.....Yellow
84 YB.....Yes
85 YC.....Yesterday
86 YD.....Yet
87 YF.....Yield
88 YG.....You
89 YH.....You will be relieved (on) (at)
90 YK.....Z
91 YL.....Zeppelin (s)
92 YM.....Zero hour
93 YN.....Zero hour has been postponed
94 YP.....Zero postponed——hours from original zero
95 YR.....Zone (s)
96 YS.....X
97 YT.....Y
98 YV.....
99 YW.....
00 YZ.....

ed—1721—HEG
ing—1999—LYW
ly—2083—MUZ
ment—2121—NEG

Appendix 12.—ENCIPHERING CARD FOR FIRST AEF FIELD CODE

SECRET

2-a

THIS TABLE MUST NOT FALL INTO THE HANDS OF THE ENEMY.

1. If destroyed to prevent capture, report will be made to the office to which its return is ordered.

2. This table will be used from 3 a. m.....

to 5 a. m....., after which it will be returned in sealed envelope to .....

ENCIPHER

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	U	V	W	Y	Z
h	o	m	s	v	a	r	e	c	z	k	n	f	l	u	w	y	i	t	b	d	p	g

DECIPHER

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	r	s	t	u	v	w	y	z
F	V	I	W	H	N	Z	A	T	L	O	C	M	B	Y	G	D	U	P	E	R	S	K

Key word .....

Service message .....

Private message .....

Appendix 13.—TEST MESSAGES SUBMITTED TO BRITISH IN CONNECTION WITH TESTING OF FIRST A. E. F. TWO-PART FIELD CODE

(1)	CUP	GWY	PYV	XYP	POF	BKY	MEF	SNP	WBO	NGF	PJA	SGR	LPU	YMP	AFR	GPA	LGS
	YOU	YXM	VOY	BYP	BXK	VEK	DXB	MUW	CFW	LGW	DWM	ANW	RMB	OKB	DCA	GXS	GMJ
	VBX	QYO	OBW	MXF	WOY												
(2)	DIT	MOP	PSJ	FMV	OGN	BWJ	JPY	QOP	DUN	PCO	YJS	FMY	LOB	CUP	GOD	BUN	YOL
	GUM	BFC	FPL	PCX	NBC	BYN	RWS	SNY	WJS	ONG	RYP	VMB	SGR	JEW	VCJ	NFW	RMS
	PUG																
(3)	NOV	JOR	MXF	BUT	VPA	COX	NEF	WAP	POF	MBY	SXG	JFB	LBW	BEW	SUB	RAN	MSO
	CBS	XYF	WCA	XOW	PJY	XMO											
(4)	YAP	CAT	YBJ	VSY	MXG	KSM	NXV	QVK	RYP	LUK	DXA	BXK	REK	XMP	XYS	PBU	FPY
	GPV	MUW	YOU	XYM	MCO	XAV	SAR	NXG	QYM	BWA	GMS	GSM	YPS				
(5)	GOT	GNY	AND	FMB	DYM	KPN	SYP	KVB	MPL	WEG	RUK	SAC	LAD	SMX	OWE	ORK	DSB
	FPS	JWP	YUX	XOW	WYS	JOV	BXK										
(6)	BKO	FAD	DWB	LGS	RYB	WJG	NAC	RWK	BOM	GFY	BAG	NES	QAM	DWM	WOY	VMS	NAT
	XUN	YBP	DCA	BYS	SOF												
(7)	JWO	ABG	YUW	NOT	RKV	XWS	SAW	GWM	MXO	WYK	XYF	KSB	AGF	WBC	XBN	XBO	KGO
	JYB	XSP	SKX	GWP	ONG	BPS											
(8)	COS	CFO	CFV	RMS	XPL	POW	AFY	BNU	FWX	WOS	RWK	NBC	PJY	JEW	VCA	JPO	LGW
	YFO	BPY	MOP														
(9)	MJO	SAT	POB	DIS	PLJ	MGI	SUG	BFX	NES	FWP	GXP	SYK	MSG	POB	JAB	GUM	RAC
	WBC	APW	VSY	WPA	XFY	GFM	MCS	SOB	GUM	NOB	PSJ	BXL	AUM	RMS	AFY	XYP	SCP
(10)	BGL	MGP	JXW	JYM	VNK	LYM	GOV	JMP	CSV	VOY	BPY	OBP	FPB	WPN	FPL	XYF	LGF
	QYW	MUW	MPB	JYM	JWU	RMS	RWK	BOM	YOU	XUN	VEB	SGP	KBS				
(11)	GPS	CUF	SXB	BSO	DIS	MAV	LGX	VEB	QOP	DSV	AXY	PEG	JEW	DPB	FBY	OCF	NWJ
	OCX	NES	COS	GNU	LES	SKX	GFM										
(12)	GBK	DAR	KSA	DEL	BUT	SYP	OWL	RAN	MSY	FMU	MJB	XYF	GBK	LPU	LUP	OCU	BEP
	GNU	ASV	NOV	PYB	YUX	XYP	GSP	KXG	MBY	WMX	LOS	DWJ					
(13)	OXW	GAV	FMS	VOK	LGS	KVA	JWY	NEF	CFV	FEM	SXG	JFB	LBW	FWX	COP	YOU	OCD
	OCF	OBP	OXM	MXF	WOY	XOW	BXS	WYK	JEW	XJU	JAP	OPL	BAP	MJP	FCM	BMY	
(14)	NOW	MGI	YPA	RMS	DSY	FWC	VOY	WAP	APW	WEG	YAK	GWM	BGP	BYM	JSP	WCF	DCJ
	WBY	FPL	DAB	GMS	NAP	ABK	AWY	RGW	OBX	GAY	FGK						
(15)	GPJ	MAR	QXJ	PLJ	YPO	MJO	SAT	XYF	PXS	RYB	BUK	WNV	RAT	BUN	DXB	SPU	SWU
	FED	DMO	CUT	FPY	YAK	BPS	KGB	ABK	YJA	NYW							
(16)	ANY	MOP	XJU	FCM	FOG	WXY	MBS	LAS	COX	NEF	PNY	BOW	PWU	YOU	ABO	QSO	DCA
	FPG	BEW	RMS	MBY	JYG	XOG	MSB										
(17)	XOW	CMU	YXM	LPN	NOV	LPU	BUG	PJA	BUT	LOW	KSM	NXV	QAG	JEW	FGN	VPA	RYP
	NUM	YJC															
(18)	OSD	YFO	CUF	WMX	XPO	OPL	VAS	VOD	GFY	VXF	LAW	DGA	MUD	GSX	XPL	LPU	YWC
	NES	KMA	SCW	SYP	GNU	BXU	LYK	OPL	SAW	BPS							
(19)	XJU	KXM	PNY	NPO	WSC	RMS	FYN	MES	QYW	BEW	DUN	XGP	GUP	YJC	JEW	KGB	WJG
	RUG	JYM	VNK	LYM	XSP	JWO	XWB										
(20)	VCA	FCM	XGP	BWC	VEG	ASY	ABO	XYF	LEP	MUT	LOR	NBC	OWU	ASY	MUW	DSY	NBP
	XMO	NES	JOB	OCJ	YSO	BYG	DCJ	JGA	ROB								
(21)	POV	NOV	BOW	MOP	YOU	QMJ	NSV	MCP	OSA	XYF	KSM	OSV	DCJ	NAP	WEV	RKY	NAY
	LES	PXK	VYM	WBC	NBC	JOC	GEB	VEB	JXO	GNB	GUM	XYF	BOX	XAV			

(22)	BYW	BNC	MXO	XUJ	XSP	RFB	FPL	JEW	DIS	AUB	BLX	PLY	SAC	WNB	MGD	MEK	OWG
	CUP	RYP	FPY	CWP													
(23)	FEW	DSY	PFW	FSV	REF	WNG	SUP	GFM	RYL	MCP	GXA	MEK	XFH	RAN	VSD	WNO	DYM
	QJP	COX	VAN	RGW	DXS	XMW											
(24)	FCS	RMS	FCM	FYL	YPX	PSJ	AFO	QSB	RYB	XON	NES	OWG	SWU	WPY	GMS	BXK	SGP
	FMO	JEW	PYW	PUS	WBC	GFY	BPY	XYS	VMJ	JSK	WOG	SUY	XBY	GXA	JGM	SXB	VPX
	YOW	NET	AMS	WEV	FPL												
(25)	NOW	GFA	DCA	RGW	JSP	MEK	XJU	PFY	YXM	YSO	JYB	DCA	DWJ	FES	OBX	BFY	BAD
	YBP	MOP	NPA	XOG	LOR	OWU	DUN	XYF	FGR	JXW	WEG	QSB	SKB	VCS	MSG		
(26)	OMB	XPL	GBM	NFW	LGS	SAR	YSO	XPN	YUX	BOK	WOY	DCA	RPJ	WPA	DXV	SXW	YXG
	KBM	YOU	WYM	JAP	BES	LGS	SKX	NBC	XMP	GOD	LGV	BOW	MOP	OWA	JEW	REF	OPL
	MCS	KGU	GMJ	YPO	RKV	FMS	RMS	BNC	REG	LOB	GYN	RBL	WOY	XSP	MOP	BEP	OWA
	GMB	FCV	NWJ	FAC	VOY	JGM	GUN	XYF	OBP	BYS	FGK	RYP	VSD	AWG	MGI	YFP	FPL
	YAB	BAM	BEW	WCS	KVA	JAB	JBX	GYS	NOV	MPL	SOM	FLX	NES	OPV	MBS	ABO	RUG
	JXW	BGX	BEV	PWU	WPA	BAK	VNK	FAC	BSX	DCA	PNR	NOM	WEG	CJW	NSO		
(27)	BKJ	DSY	COT	BOM	BFY	GFY	YUM	OWE	VCS	FPL	NES	YUB	JAP	XFS	GMJ	FBU	JEW
	XJU	NAC															
(28)	VYL	XYB	FEM	VBC	MEK	YJV	GBM	NFW	RMS	YSO	JSX	NSV	WNX	JOV	PCU	PCM	DSY
	LEB	YOU	XFM	SNA													
(29)	FAD	MOP	MSK	WOS	MYS	ASY	GPA	FPL	LUM	VMJ	FJW	XYF	NCP	SMC	LPU	VSG	COX
	BAD	JEW	JMP	FES	MPL	AXG	VBA	XFY	MUD	LPN	BYN	YOU	NUV	KPY			
(30)	DSK	ABF	DCJ	XYF	ROF	SCO	KGB	WPX	BPS	NES	DMG	LGW	QOJ	BUN	MJB	VJB	OBY
	BAT	POB	AND	XYM	BXK	RMS	GFY	MES	MPB	SXV	CBW						
(31)	FEW	AUX	BMV	MEK	LBV	MPB	NGF	SYP	NXV	RGN	RYS	YOU	NGK	XAM	YFP	FCM	OCU
	LGB																
(32)	CBN	NSV	MCP	DSK	YJV	BXU	MUW	KMD	COP	PJB	GAL	XJS	PEK	MOG	RKO	NFY	MEV
	WBO	XSP	XYF	NEW	YAW	SYK	WEG	LGS	FRU	JYB	JFC						
(33)	FOG	NET	LOP	SYK	SCO	SWO	NWA	NES	DIT	FPL	WXY	SYK	WEG	ONV	NFB	JXW	NBJ
	JEW	GOC	YAM	NPY													
(34)	MPB	POV	DOB	BAK	REK	FRP	XYF	NAM	WJY	XWB	SGP	FMV	MPL	XON	YOU	SNP	YUX
	BFC	BEW	RMS	FED	YXM	JSK	RKB	GWY									
(35)	GNU	FPS	SCO	DUM	YON	GXB	DSY	LEB	OBP	XYP	JYM	SUP	PXS	FPY	GNC		
(36)	MJC	MXG	VXK	QXJ	XSA	LOB	JGX	YWS	DWM	VXW	NES	SWP	BYS	JSP	QOF	GUM	YPO
	LBY	AGU	MAV	VYN	MUD	BFU	DUK	FRB	YAL	XYF	JUW	WJB	MSG	VOM	RYB	MOP	GLP
	XMP	XOW	LGW														
(37)	NWY	YSO	DXO	PXB	LAS	JOB	KVY	RWS	COX	BAN	YPO	MCP	MJO	LOB	WJG	LGB	KVA
	YUM	JPO	YUX	BYP	CMX	YFO	DCA										
(38)	NBL	BNX	XAM	RGW	CAK	XUN	BEV	YOU	JOP	PUG	AFO	AFM	MOP	FYM	WMX	FPC	MOK
	JEW	SOF	POS	YBP	LGS	NUM	BED	RMS	NGF	WBO	DMS	NEF	DCA				
(39)	AMK	GNU	XOG	YFA	KGB	BYW	NES	XMD	JOC	CFG							
(40)	BNY	BFY	XYF	WCX	SGP	BYG	CUF	APU	LOB	FPY	WOV	RMS	JEW	LBV	SUP	GXA	NEF
	NXA	BKO	ROB	OWA	YSO	MOP											
(41)	JXW	FAD	QXJ	MPB	YWS	NES	XUN	GXO	VAF	AFR	DYM	MCP	XBN	FPL	GWM	NBC	PLU
	WOY	JEW	LGF	SMC	JAP	LPU	BAG	YOU	YFO	DUN	PYL	JOV	PCX	OBR	BYS	GPA	RMS

Appendix 14.—REPORT OF MAJOR HAY, OF BRITISH GENERAL STAFF (CODE SECTION)

M. I. 1. B/889/Cy.

MAJOR MOORMAN.

The four specimen pages of the code adopted for wireless signalling purposes by the American Expeditionary Force have been examined in this office and, in deference to your wishes, the following observations are submitted.

1. The trigrams employed in the four pages under consideration are composed of any three letters of the alphabet except H, I, and Z, with the further restrictions that E, T and U do not occur as a first component, D, Q, and T as a second or Q as a final component of any group.

2. No letter is repeated in any one trigram, so that groups like AGA, BBM, XPP do not occur.

3. If these conditions hold throughout, there are thus 20 different initial letters, 20 medial, and 22 final, making, when all the remaining combinations are used, a possible aggregate of 7,600 groups. Perhaps, however, the number should be 20, 21, and 22 respectively. This would provide a round total of 8,000 groups and a symmetrical arrangement of columns in the code book.

4. Six hundred and twenty-one different trigrams are used in the total of 1,151 contained in the 41 messages submitted. Of these 621 trigrams 371 occur only once and 135 only twice. The average frequency for each group is less than 2. The deduction is that many alternatives are employed.

5. The most frequent groups are XYF (16), RMS (15), JEW (15), NES (13), MOP (11), FPL (10), DCA (9), YOU (13), LGS (7).

6. The statement above that many alternatives are employed is borne out by the fact that there are hardly any recurrences of the same trigrams in juxtaposition or even in proximity to one another. JEW+XJU occur twice; BEW+RMS twice; NFW+RMS twice. MOP tends to occur near the beginning and end of messages, and suggests therefore, an address or signature, or it might be a stop. Other groups that strike one as worth watching are: DCA, FCM, RMS, XJU, XOW, YFO, YOU.

7. If spelling is used to any extent, it has not been detected (for the reason given in par. 6).

8. Both the code as a whole and the messages in particular would seem to have been composed with great precautions for safety; but from only 41 messages one is unable to form a definite opinion as to the possibility of solution. Appearances are certainly in favor of safety, but much would depend on the amount of traffic and the frequency with which the code was changed. Also information under the following headings might prove of great value to anyone attempting its solution. Moreover most of this information would presumably be available to the enemy.

(*a*) The date and time of day when the messages were sent.

(*b*) The approximate positions of the sending and receiving stations.

(*c*) The system of call signs, general wireless procedure, etc.

(*d*) The organization and disposition of the forces under the American command.

(*e*) Names of commanders and designations of units (unless special code groups are used for these in every case).

(*f*) Intelligence derived from inferences based on actions which seem to follow the reception of certain messages or vice versa.

(*g*) Chance information gained through carelessness on the part of a subordinate officer or N. C. O., such as the interception by the enemy of the substance of a code message repeated in clear by telephone or power buzzer. This is no doubt strictly prohibited, but in the stress of battle such things may occur.

I am of the opinion that this code when used with care could not be read by the enemy until he had collected a very large amount of material.

One of the principal safeguards against discovery lies in the use of alternatives, and in practice this safeguard loses something of its value owing to the fact that encoders soon get into the habit of using the same common groups and of neglecting to use the alternatives. In fact the user of a code can only with great difficulty be prevented from clothing his meaning always in the same manner both with regard to the language used and the selection of groups for encoding. The length of time for which this code can be considered secure is therefore mainly dependent on the way in which it is handled.

Under favorable conditions this code would be safe for at least 2 months; but having regard to the probability of accidents, I think it would be advisable to make a more frequent change and not at regular, but rather at irregular intervals.

M. V. HAY,
Major, General Staff.

M. I. 1. B.
24th June 1918.

Appendix 15.—REPORT OF CAPTAIN HITCHINGS, OF BRITISH ARMY CODE SOLVING SECTION

SECRET

AMERICAN THREE-LETTER CODE

SURVEY BY

GENERAL STAFF, B. E. F.

Section Intelligence E (c)

June 30th, 1918 1500

SURVEY OF AMERICAN THREE-LETTER CODE

Before entering into a detailed examination of the 41 messages submitted, it should be noted that a code is often rendered insecure by agitated operators failing to comply with instructions to make the fullest use of every alternative group.

There is a tendency on the part of operators to send certain stereotyped messages at stated hours daily, containing, for the most part, the same words, on different sectors of the front. These operators may have obeyed instructions to the letter. Yet a comparison of the messages by the enemy may result in showing that several code groups are the alternatives for the same "clear" letter, word, or phrase.

These are the insecurities caused by modern conditions. They compromise codes and ciphers which may be theoretically insoluble.

PECULIARITIES

1. No letter is repeated in the same group. This might infer that the code groups are indexed in alphabetical order and also that there is only one group containing the same letters, and that the operator has the option of transmitting the letters of any group in any of the six possible ways.

For example in message 12, groups 14 and 15, we have LPU^{6} LUP which if arranged alphabetically would be LPU^{7} LPU^{7}. (The index number refers to the number of times a group occurs in the 41 messages.)

Likewise in message 14, groups 8 and 9, we have WAP^{3} APW^{2}, rearranged alphabetically they are APW^{5} APW^{5}.

However, this is ruled out by the fact that certain letters which occur frequently as second and third letters are not found as initial letters. It is therefore assumed that repetitions have been avoided with a view to ensuring against operator's mistakes.

This also appears to be the case with the omission of the letter H, which is often mistaken for S.

It is consequently observed that groups have been very successfully selected to avoid Morse errors occurring in the transmission of the message.

2. E, H, I, T, U, and Z do not occur as initial letters.
3. D, H, Q, T, and Z do not occur as second letters.
4. H, Q, and Z do not occur as final letters.
5. About 600 groups appear in the 41 messages.
6. The frequent groups are:

XYF occurs 16 times	FPL occurs 9 times
RMS occurs 15 times	MOP occurs 9 times
JEW occurs 14 times	DSY occurs 6 times
NES occurs 13 times	YSO occurs 6 times
YOU occurs 13 times	

7. The following result is arrived at by indexing the groups according to their final letter. It is noticed that there is a tendency for certain initial letters, coming before the same bigram, to be near each other in the normal alphabet, e. g.—

Initial letters	*Bigrams*	*Initial letters*	*Bigrams*
G N V W Y	PA	J K L M Q Y	OP
K L	GB	B R S X	YP
J L M N P R S	OB	B F L M N	ES
K L W X	PN	B N M P X Y	OW
J N X Y	PO	A B G	FV

8. Repetitions are:

jym[4]	vnk[3]	lym[2]	in messages 10 and 19
sxg[2]	jfb[2]	lbw[2]	in messages 3 and 13
	nfw[3]	rms[15]	in messages 2 and 28
	bew[4]	rms[15]	in messages 16 and 34
	gbm[5]	nfw[3]	in messages 26 and 28

9. The following are passages of groups which occur more than once:

In message														
1	snp	wbo	ngf	pja	agr	lpu								
1	gpa	lgs	you	yxm	voy	byp	bxk							
2	gum	bfc	fpl	pcx	nbc	byn	rws							
6	lgs	ryb	wjg	nac	rwk	bom	gfy	bag	nes					
6	xun	ybp	dca	bys	sof									
7	saw	gwm	mxo	wyk	xyf									
8	fwx	wos	rwk	nbc	pjy	jew								
8	jpo	lgw	yfo	bpy	mop									
9	mjo	sat	pob	dis	plj	mgi								
9	syk	msg	pob	jab	gum									
9	wbc	apw	vsy	wpa	xfy									
10	jmp	osv	voy	bpy	obp									
10	fpl	xyf	lgf	qyw	muw	mpb	jym							
10	rms	rwk	bom	you	xun	veb	sgp							
11	nes	cos	gnu	les	skx	gfm								
13	nef	cfv	fem	sxg	jfb	lbw	fwx							
14	voy	wap	apw	weg	yak	gwm								
15	qxj	plj	ypo	mjo	sat	xyf	pxs	ryb						
16	mbs	las	cox	nef	pny	bow	pwu	you	abo					
19	yjc	jew	kgb	wjg	rug	jym	vnk	lym	xsp	jwo	xwb			
22	mek	owg	cup	ryp	fpy									
24	psj	afo	qsb	ryb	xon	nes	owg	swu						
25	dca	rgw	jsp	mek	xju									
25	yxm	yso	jyb	dca	dwj	fes	obx	bfy	bad	ybp	mop			
26	bow	mop	owa	jew	ref	opl	mcs							
26	gmj	ypo	rkv	fms	rms	bnc								
28	mek	yjv	gbm	nfw	rms	yso								
29	cox	bad	jew	jmp	fes	mpl								
29	xfy	mud	lpn	byn	you									
30	pob	and	xym	bxk	rms	gfy	mes	mpb						
34	xwb	sgp	fmv	mpl	xon	you	snp	yux	bfc	bew	rms	fed	yxm	jsk
37	ypo	mcp	mjo	lob	wjg	lgb	kva	yum	jpo	yux	byp			
41	jxw	fad	qxj	mpb	yws	nes	xun							
41	dym	mcp	xbn	fpl	gwm	nbc	plu	woy	jew	lgf	smc	jap	lpu	bag
	yfo	dun												you

CONCLUSIONS

From the peculiarities as they stand, we cannot infer anything with any great degree of certainty, because there may be others besides those enumerated, and this possibility forbids the general conclusion from being anything but tentative. The conclusions arrived at are:

(*a*) The code is a complex one; i. e., arranged in two parts for encoding and decoding.

(*b*) It abounds in alternative equivalents.

(*c*) The code groups seem to have been chosen with the object in view of assisting transmission by avoiding the combination of letters whose Morse equivalents might lead to mistakes.

(*d*) Solution cannot be effected on the 41 messages; however, it would not be safe to assume that the code is insoluble. From the fact that in 30 messages repetitions of 3 groups do recur on 2 different occasions it must be assumed that as each new message is intercepted the chances of getting repetitions increase at a higher progressive ratio.

(*e*) If the test messages submitted are a true representation of the messages which will be sent by different operators on the various sectors of the front, and during uncomfortable circumstances, then the code is an undoubtedly sound one and presents great difficulties to solution on anything under 200 messages. For example in message 32, from the eighth to seventeenth group, inclusive, there are 10 code groups which do not occur anywhere else. It is possible that these could only be discovered after the interception of from 700 to 1,000 messages.

(*f*) Estimating that 75 percent of wireless messages in the field are successfully intercepted, it is doubtful if any leakage of valuable information could take place until after 1,000 messages had been sent.

(*g*) A study of peculiarities (par. 9) suggests that alternatives are governed by a system, not selected at random. Should this be the case the security of the code is considerably impaired.

Appendix 16.—SAMPLE PAGES FROM THE VARIOUS FIELD CODES PREPARED AND USED BY THE A. E. F.

(Appendices 16A to 16G formed "the River Series"; appendices 16H to 16K, "the Lake Series"; appendices 16L to 16N, "the Numbered Series")

CONTENTS OF APPENDIX 16

Appendix 16A.—EXTRACTS FROM THE "POTOMAC" CODE

Secret

MUST NOT FALL
INTO HANDS OF
ENEMY

The
"POTOMAC"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

No. 2027

This book has been issued

to _____

for official use under
his direction
only.

BY COMMAND OF GENERAL PERSHING:

JAMES W. McANDREW,
Chief of Staff.

OFFICIAL:
ROBERT C. DAVIS,
Adjutant General.

A. G. PRINTING DEPT., G. H. Q. A. E. F., 1918.
(155)

Instructions

1. This code book, to be known as the "Potomac" Code, is issued to all combatant troops down to battalions.

It is primarily intended for communication within the division, but may be used for messages to higher headquarters.

Messages encoded by its use may be transmitted by any means at hand, but radio or earth telegraphy should be used only when more secret means are not available.

2. Messages once transmitted in clear or in any other code or cipher must not be repeated in this code.

Messages once transmitted in this code must not be repeated in any other code or cipher or in clear.

Except that number and hour of signature may be in clear when preceding first code group, the use of "clear" in code messages is prohibited.

3. The use of this code for regular routine reports should be limited to actual necessities. Such reports should be transmitted by other means than radio or earth telegraphy.

4. Avoid use of words not in code book when other words with same significance are provided. Words spelled out, letter by letter, not only take time to code, transmit and decode, but they are one of the favorite points of attack by enemy code men.

5. Where two or more code groups are assigned the same letter, syllable, word or phrase, first one and then another should be used so that in a series of messages each occurs about the same number of times. In particular, no group should ever appear twice in the same message.

6. At least one group marked "Null" should be used for every ten code groups in a message. These should be placed at irregular intervals. A "Null" should always occur between double letters; thus the word "boot" would be encoded:

(b)	(o)	(Null)	(o)	(t)
KVG	LOC	MUD	VYN	ASG

Note that different groups are used for the letter "O"

7. Coded and decoded copies of messages must never be filed together. All notes and memoranda used in coding or decoding messages must always be destroyed, by burning, if practicable.

8. Messages must be short. Several short messages will be less likely to be read by the enemy than one long one.

Except in emergency a long message, if it must be sent, will be divided into two or more parts and each sent as a complete message.

Very often the best way to handle a long message is to leave out unnecessary words.

9. Addresses will not be used when context of message indicates for whom intended. When used, they must be in code.

10. Signatures should be sent only when absolutely required. When sent, they must be encoded, letter by letter, if necessary. Usually it will be sufficient to indicate origin by some word in code book previously agreed upon by each commander and his immediate subordinates.

11. The message handed Signal Corps operator should be in the following form, on any suitable paper:

"No. 1. 15:40. KVG LOC MUD VYN ASG

Send this message to First Division.

J. M.

1 June 1918 Capt., 1st Infantry"

Items should always appear in this order, that is:

(a) Number of message.

(b) Hour of signature.

(c) Body of message.

(d) Order directing transmission.

Order directing transmission may also indicate means to be employed when deemed necessary by the Commanding Officer, but this will, in general, be left to the discretion of the Signal Corps.

Number of message and hour of signature should be given only when they will serve some good purpose. They will be in clear.

Body of message must be entirely in code.

12. Blank spaces at end of book are for use of divisions for designation of organizations and local geographical points, or for such other use as may be desired.

Words assigned will be reported to Corps, Army and General Headquarters, and to neighboring divisions.

ENCODING

0...WNO..MXA..OKU
1...FWP..KSA..GOT
2...WBO..WCF..RKV
3...NYF..PJA..NUM
4...VMB..FSO..CMU
5...GYN..MJW..WYS
6...XJM..FEG..MYS
7...RMB..RFS..AFR
8...OXM..GUP..SXM
9...YAW..MSX..FUM
10...MXO..BXS..BGP
11...VCJ..JFW..LUK
12...KGP..OXW..VSD
13...BUW..RWM..SPY
14...DPG..PAR..XJS
15...GBY..OCX..CBY
16...FMB..PBO..OBK
17...BUG..VAB..YOC
18...JOR..AFV..POS
19...VAF..OBW..FLM
20...BXL..SYB..MBO
21...MSO..CMB..OGV
22...LYT..GYM..WBL
23...WSB..FBX..RPA
24...GPX..PNW..VPN
25...KBW..PFO
26...MEW
27...VCW
28...FXS
29...CSO
30...WES..ORK
31...ANO
32...PES
33...VMA
34...FJP
35...OLJ..BLC
36...ANW
37...ROM
38...WXV
39...DAR
40...KMC..REP
41...DOS
42...JMS
43...RUB
44...GMU
45...FSM..AXM
46...PON
47...FAK
48...JWC
49...MOG
50...WAJ..JXB
51...PYM
52...JGO
53...RYG
54...PFR
55...BPU..XJB
56...ONP
57...GSY
58...KBJ
59...NBY
60...FUN..BEN
61...PAW
62...PCF
63...BKS
64...BPN
65...GPW
66...LUN
67...NCX
68...MOB
69...VYB
70...JUM..FPE
71...GYV
72...BSM
73...FGX
74...VXG
75...GKJ..NEW
76...DWU
77...DCS
78...BMC
79...XYV
80...PSU..FAN
81...GKO
82...XAB
83...NFV
84...PSO
85...DGM
86...JGP
87...CBM
88...YSJ
89...FRO
90...PFV..RYW
91...VBP
92...ASB
93...OCW
94...PAK
95...OBL
96...GUS
97...SGB
98...ROW
99...BLP

Null...XSP
Nd...WBJ..XWS
St...CBS..GNY
Th...DYM..MXF

Null...LYS
Nd...QOV..WBJ
St...DEL..CBS
Th...GAV..DYM

DECODING

ABE...Falling back
ABF...Heavy
ABG...Message received
ABK...Supply
ABM...Have you received
ABO...Bombardment
ABP...Barrage
ABS...Battalion
ABV...Automatic
ABW...Must be
ABX...Truck
ABY...Received
AFC...Cannot
AFD...One
AFJ...Turn
AFM...Machine gun emplacement
AFO...Enemy
AFR...7
AFV...18
AFX...Smoke
AFY...Stop
AGE...Diminish
AGF...-en
AGH...Picket
AGK...Stay
AGL...Field buzzer
AGN...In communication with
AGO...Question
AGU...Lieutenant
AGY...Emplacement
AMC...Further
AMG...Wounded
AMK...We are losing heavily
AMO...At close quarters
AMP...Confirm
AMS...Our first line
AMV...-ate
AMX...Might
AMY...Evident
AND...Battalion
ANF...During the night
ANG...Fifth
ANK...All stations
ANP...Observer
ANO...31
ANS...Consider
ANW...36
ANX...Your
ANY...Within
APB...Bombproof
APE...Relief completed
APF...Retire
APJ...Premature
APN...Impossible
APO...Withdraw
APU...Machine gun ammunition
APW...E
APX...Remove
APY...Moving
ASB...92
ASF...Shell
ASG...T
ASK...Has not been
ASM...Gas is being blown back
ASO...Control
ASP...Removed
ASV...Keep
ASX...Surprise
ASY...(Null)
AUB...Runner
AUF...Must have
AUG...Condition
AUK...Safety
AUM...Minute
AUP...Rescue
AUS...Point
AUW...V. B. rocket
AUX...On the right
AWB...Sometime
AWC...Require
AWE...Barricade
AWG...O'clock
AWK...Light signal
AWO...Double
AWP...Still
AWS...Lengthen
AWX...Will signal by
AWY...Will not
AXB...Forcing
AXF...Magazine
AXG...Trenches
AXM...45
AXP...Send
AXS...Moment
AXV...Your
AXW...Last night
AXY...Going
BAD...Advance
BAF...Afternoon
BAG...Division headquarters

Appendix 16B.—EXTRACTS FROM THE "SUWANEE" CODE

Secret

MUST NOT FALL
INTO HANDS OF
ENEMY

The
"SUWANEE"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

ENCODING

0...WPC..GMX..CJP
1...VEF..ANY..CBU
2...AWO..DEL..DOG
3...VAG..WCK..XWS
4...RMO..PBU..DXY
5...AUX..VSP..FAW
6...YUM..SBW..BOD
7...MEG..CMO..BOG
8...SAN..OKM..MAC
9...JOV..VMA..BOM
10...GXS..OSV..AMK
11...SGW..WOK..RUG
12...JVC..DGS..NUB
13...ANK..SNB..MEP
14...BKJ..XYF..BFA
15...LYP..FGR..NWA
16...BUW..JBS..JAV
17...FCM..CAF..DMO
18...KBO..MOB..FLY
19...QAV..WJX..RUN
20...BAN..OSY..GWA
21...NOC..AWE..BYK
22...GNA..VPF..NWJ
23...OMA..BLD..GBL
24...NAC..OBY..FET
25...GNY..MUY
26...WUA
27...PYK
28...WJO
29...AMP
30...WPX..MCK
31...PAM
32...YMV
33...BMD
34...DCJ
35...YJP...GSP
36...YPF
37...DOV
38...KXW
39...XMD
40...CBX..BUD
41...JSO
42...QBF
43...WEP
44...QVG
45...BLY..SWM
46...VND
47...LES
48...FXM
49...PAD

Null...AGF
Nd...ROF..WYK
St...DWB..SGO
Th...FLB..LEM

50...OCD..PFJ
51...DON
52...RAW
53...DYK
54...OSA
55...XMP..SON
56...CPL
57...NBY
58...FXB
59...BGY
60...JMU..RKO
61...MAV
62...JFA
63...AFO
64...MUG
65...SYN
66...SUY
67...MYW
68...VNW
69...SBL
70...PXA..SXB
71...XAM
72...VCJ
73...WNX
74...RYG
75...MBY..XFW
76...GLY
77...DMX
78...KPL
79...GKC
80...BSX..FMY
81...OBC
82...KPX
83...DSP
84...LAV
85...DGK
86...OSD
87...NEW
88...CAR
89...NYK
90...SOV..ANS
91...XGP
92...FBO
93...ONW
94...OPL
95...RFW
96...VYN
97...QOJ
98...VMC
99...PAY

Null...FYN
Nd...ROF..WYK
St...RBS..OGN
Th...JYF..QAF

Approach...BAW
Approved...DPW
Approximate...KVS
Approximately...DXJ..NSO..MCX
-ar...RFP
Are...GNU..XYM..VSJ
Are having...WYO
Are not...CBY
Are they...XUY
Are we...CUK
Are you...PXB
Are you all right...FWX
Arm...PEF
Armored...DSM
Army...VCO
Arrive...DGO
Arrived...PWC..ONC..KGU
Artillery...QXJ..FRA..PCK
Artillery fire...FEV
Artillery observer...PNR
Artillery position...BNK
Artillery preparation...LOV
Artillery support...XMA
-ary...RGU
As...CFK..MSK..PYS
As far as...CJB
As soon as...RMV..BAF
Ascertain...VEB
Ask...BUG
Asphyxiate...YBJ
Assemble...FBX
Assist...VXP
Assistance...FRU
At...NBJ..FGN..KMA..VXY
At close quarters...GFP
At once...PCB
At point...VOR
-ate...XGK
Attack...VJO..GFO..NXV
Attacked...BNO
Attacking...VEL
Attempt...SOR
Attention...XBU
Austrian...YBS
Automatic...KPO
Automatic rifle...YXB
Automatic rifle ammunition...QVK
Available...PAK
Aviator...DAW
Await...WAX
Null...MUS
Ing...PBC..FGA
Ion...QXY..KMD
Ll...YJB
Ly...NXA

Await instructions...BUT
Away...KXA
Axe (s)...SPF
B...RYB..WEF..ABY
Back...LBX
Bad (ly)...LGN
Badly damaged...GLX
Badly wounded...MOG
Bag (s)...NGK
Balloon...GUT
Barbed wire...BGK...QEK
Barrage...SMO..FES..POB
Barrage wanted...MBJ
Barricade...YMB
Battalion...MGX..PAC..GAN
Battalion headquarters...KGO..NPC
Battery...OWB..YSJ..KSO
Battle (s)...XFP
Bavarian...GPX
Bay (s)...VAT
Bayonet...CUM
Be...QEX..JAR
Be ready...YFB
Be released...CSP
Because...XON
Been...OCX..LOM
Before...QEG
Began...JSV
Begin...SOK
Begun...PNO
Behind...KBS
Behind the lines...YUW
Being...FYW..LEV
Being established...GXB
Being held...XPU
Being sent...RMB
Being shelled...MJX
Believe...XAV
Belong...KGW
Below...FBW
Belt (s)...SBY
Bengal lights...GMB
Best...SKP
Better...FPO
Between...PUK..WBO
Beyond...ASV
Billet (s)...NOB
Bivouac...YWU
Black...GVJ
Block...JUP
Null...BNX
Nd...ROF...WYK
Re...AGE..NBL
S...GEW..OXS
St...OGN..RBS
Th...QAF...LEM

DECODING

ABE...Bomb-proof
ABF...Essential
ABG...Of
ABK...V
ABM...Section
ABO...Was not
ABP...Damage
ABS...Slight
ABV...N
ABW...These
ABX...And
ABY...B
AFC...November
AFD...Helmets
AFJ...Does
AFM...Sentry
AFO...63
AFR...Why
AFV...Adjust
AFX...Telephone
AFY...Troops
AGB...Afternoon
AGE...-re
AGF...(Null)
AGK...Our artillery
AGL...Squadron
AGN...Field artillery
AGO...Most
AGU...Commissioned officer
AGY...Least
AMC...(Null)
AMG...Aeroplane
AMK...10
AMO...Hyphen
AMP...29
AMS...Bombarded
AMV...Follow
AMX...Destroyed
AMY...Wagon
AND...Men
ANF...Come
ANG...Observer
ANK...13
ANO...Signal
ANP...Let
ANS...90
ANW...Too far
ANX...Appear
ANY...1
APB...Green
APE...Advance guard
APF...Yesterday
APJ...Or
APN...Without
APO...Could not
APU...Has not arrived
APW...On the
APX...Wire
APY...We are losing heavily
ASB...Relief completed
ASF...Rush
ASG...Exact range
ASK...Communication
ASM...Which
ASO...Rations
ASP...Depth
ASV...Beyond
ASX...He
ASY...Did not
AUB...-ent
AUF...Suspect
AUG...Prussian
AUK...Stokes
AUM...Prepare
AUP...To
AUS...Machine gun fire
AUW...Will
AUX...5
AWB...Instructions
AWC...Have arrived
AWE...21
AWG...-ous
AWK...By platoon (s)
AWO...2
AWP...Will lift
AWS...In enemy's hands
AWX...Longer
AWY...Wounded
AXB...From
AXF...Board
AXG...No
AXM...Poor
AXP...Forcing
AXS...Send by
AXV...Gas attack
AXW...Had
AXY...Reconnoitering
BAD...Mass
BAF...As soon as
BAG...Will begin

Appendix 16C.—EXTRACT FROM THE "WABASH" CODE

SECRET

MUST NOT FALL
INTO HANDS OF
ENEMY

The
"WABASH"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

Appendix 16D.—EXTRACTS FROM THE "MOHAWK" CODE

SECRET

MUST NOT FALL
INTO HANDS OF
ENEMY

The
"MOHAWK"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

Instructions

1. This code book, to be known as the "Mohawk" Code, is issued to all combatant troops down to battalions.

It is primarily intended for communication within the division, but may be used for messages to higher headquarters.

Messages encoded by its use may be transmitted by any means at hand, but radio or earth telegraphy should be used only when more secret means are not available.

2. Messages once transmitted in clear or in any other code or cipher must not be repeated in this code.

Messages once transmitted in this code must not be repeated in any other code or cipher or in clear.

Except that number and hour of signature may be in clear when preceding first code group, the use of "clear" in code messages is prohibited.

3. The use of this code for regular routine reports should be limited to actual necessities. Such reports should be transmitted by other means than radio or earth telegraphy.

4. Avoid use of words not in code book when other words with same significance are provided. Words spelled out, letter by letter, not only take time to code, transmit and decode, but they are one of the favorite points of attack by enemy code men.

5. Where two or more code groups are assigned the same letter, syllable, word or phrase, first one and then another should be used so that in a series of messages each occurs about the same number of times. In particular, no group should ever appear twice in the same message.

6. At least one group marked "Null" should be used for every ten code groups in a message. These should be placed at irregular intervals. A "Null" should always occur between double letters; thus the word "boot" would be encoded:

(b)	(o)	(Null)	(o)	(t)
4212	2976	2627	3460	4704

Note that different groups are used for the letter "O"

7. Coded and decoded copies of messages must never be filed together. All notes and memoranda used in coding or decoding messages must always be destroyed, by burning, if practicable.

8. Messages must be short. Several short messages will be less likely to be read by the enemy than one long one.

Except in emergency a long message, if it must be sent, will be divided into two or more parts and each sent as a complete message.

Very often the best way to handle a long message is to leave out unnecessary words.

9. Addresses will not be used when context of message indicates for whom intended. When used, they must be in code.

10. Signatures should be sent only when absolutely required. When sent, they must be encoded, letter by letter, if necessary. Usually it will be sufficient to indicate origin by some word in code book previously agreed upon by each commander and his immediate subordinates.

11. The message handed Signal Corps operator should be in the following form, on any suitable paper:

"No. 1. 15:40. 4212 2976 2627 3460 4704

Send this message to First Division.

J. M.
1 June, 1918 Capt., 1st Infantry"

ENCODING

0...4616..4585..3524		50...2973..4620	
1...3211..4753..4997		51...3533	
2...3323..4794..3305		52...3920	
3...3657..3517..3188		53...3851	
4...4498..2661..4213		54...4774	
5...3667..2522..4431		55...2714	
6...3272..2875..4900		56...3089	
7...3766..4650..2613		57...3961	
8...4004..3009..2650		58...3498	
9...4550..3137..4313		59...3731	
10...3248..2525..4887		60...2806..4479	
11...3685..2770..4034		61...3824	
12...3203..3755..3613		62...2920	
13...2727..4851..2909		63...2564	
14...4379..3256..4529		64...4680	
15...3047..4271..3251		65...3492	
16...4867..4339..4029		66...3506	
17...2664..4802..3826		67...2847	
18...3267..2800..4059		68...2821	
19...4799..3083..2705		69...4661	
20...3979..2893..3240		70...2544..3200	
21...4210..2717..3579		71...2687	
22...2614..4273..2942		72...2825	
23...3820..2595..4804		73...4521	
24...3710..2778..4026		74...2709	
25...2804..3713..2902		75...4890..4598	
26...3529		76...4916	
27...2788		77...4698	
28...3838		78...2958	
29...4018	Null...3978	79...3243	
30...3653..2749		80...4878..4002	
31...3366		81...4633	
32...4350		82...4984	
33...3171		83...2507	
34...2541		84...4576	Null...3903
35...3155..4816		85...3637	
36...3976		86...4715	
37...2579		87...3221	
38...4830		88...3465	
39...2519		89...4266	
40...2677..4320		90...2684..3173	
41...3281		91...3575	
42...4334		92...3846	
43...2707		93...4778	
44...4487		94...2758	
45...3401..4963		95...4973	
46...3293		96...3899	
47...3079		97...3432	
48...3870		98...4671	
49...2633		99...3349	

DECODING

2500...Go	2550...Leave
2501...Tank	2551...Sign
2502...Not	2552...Request
2503...Compass	2553...Combat train
2504...Has been	2554...Battalion
2505...P	2555...Serious
2506...-ou	2556...On
2507...83	2557...Progress
2508...During	2558...Opposite
2509... (Null)	2559...No casualties
2510...Kill	2560...French 75 mm.
2511...Must	2561...-rd
2512...-qu	2562...E
2513...Too little	2563...Men
2514...Be ready	2564...63
2515...Attacking	2565...Defensive
2516...Favorably	2566...Nothing to report
2517...Reinforcements arrived	2567...Border
2518...Earth	2568...And
2519...39	2569...-es
2520...First	2570...Artillery position
2521...Drop	2571...Small
2522...5	2572...Still
2523...Green	2573...Pair
2524...Commander	2574...By
2525...10	2575...Messenger
2526...Lengthen	2576...-ite
2527...Fog	2577...Relieved
2528...Cross	2578...Increase
2529...Body	2579...37
2530...During	2580...H
2531...Cannot	2581...Our
2532...Parachute	2582...Liquid fire
2533...Postponed	2583...End
2534...Men gassed	2584...Out of
2535...Occupy	2585...Considerable
2536...Advised	2586...Raid will take place
2537...Platoon	2587...Moment
2538...H	2588...R
2539...Have taken	2589...Require
2540...Seventh	2590...-ing
2541...34	2591...Repeat
2542...Do not	2592...100
2543...January	2593...Mile (s)
2544...70	2594...Sending up
2545...Breach	2595...23
2546...Approved	2596...Ought not
2547...Between	2597...No
2548...Observation	2598...On this
2549...Quartermaster	2599...Q

Appendix 16E.—EXTRACTS FROM THE "ALLEGHENY" CODE

SECRET

MUST NOT FALL
INTO HANDS OF
ENEMY

The
"ALLEGHENY"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

ENCODING

0...2896..4901..5200	50...2329..3942
1...1943..5471..3048	51...5343
2...4071..5784..3260	52...1861
3...3749..3485..4130	53...4011
4...4815..5316..2281	54...2276
5...3012..4207..2844	55...1970..3193
6...2277..4599..2124	56...2420
7...5523..2163..2325	57...4738
8...2178..2238..5842	58...1673
9...3189..3882..5218	59...2392
10...3178..1672..2188	60...3501..2267
11...5527..5098..2079	61...3893
12...1921..5302..4791	62...3584
13...2083..1922..4985	63...4044
14...1815..1509..5142	64...5207
15...5011..2475..4457	65...1959..3159
16...1593..2567..1830	66...5886
17...1658..2284..3069	67...1596
18...5660..1676..2410	68...3054
19...4598..5693..1560	69...5103
20...4581..2176..2594	70...4243..3521
21...3824..1610..4082	71...3389
22...1722..4415..2457	72...1845 Null...4060
23...2244..4824..5063	73...4967
24...4424..3610..4780	74...2723
25...5275..2547	75...5389..3582
26...4616	76...3370
27...5746 Null...4267	77...4477
28...4075	78...5392
29...4709	79...2557
30...5186..1786	80...3347..4260
31...3609	81...3229
32...1990	82...2554
33...2400	83...2900
34...2351	84...5018
35...5318..3756	85...3468..3951
36...3292	86...4959
37...3651	87...2667
38...3980	88...5282
39...1704	89...2993
40...2913..4518	90...4148..2426
41...3492	91...3396
42...1809	92...2289
43...5122	93...2663
44...2187	94...3067
45...2496..3965	95...4429..4909
46...5287	96...2972
47...1819	97...1685
48...5637	98...5977
49...2817	99...1645

Appendix 16F.—EXTRACTS FROM THE "HUDSON" CODE

SECRET

MUST NOT FALL
INTO HANDS OF
ENEMY

Memorize this Group:
"2222---Code Lost."

The
"HUDSON"
CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

ENCODING

0...1797..5519..4887
1...1997..2074..3854
2...5527..2953..2738
3...5295..2742..3759
4...1934..4951..2610
5...5838..2623..3967
6...3498..5214..4057
7...5191..2417..3980
8...2283..2946..4400
9...5979..4412..2136
10...4626..3031..5342
11...1591..5025..2044
12...3286..2681..4277
13...2512..5981..5928
14...3088..2633..5367
15...2554..2488..4532
16...3107..5067..3261
17...3569..4644..1884
18...2334..4865..3204
19...5115..1789..3336
20...1538..4655..3876
21...5033..3479..5243
22...4582..5594..4129
23...5407..1742..2259
24...2669..2395..4254
25...2021..5300

Nulls:
4286
2809
2094
4198
5078

26...3738
27...5767
28...4513
29...3022
30...4733..4052
31...2884
32...5895
33...2238
34...2438
35...4893..2837
36...1812
37...2530
38...2182
39...3080
40...2929..4767
41...5004
42...3664
43...2855
44...5142
45...2407..4902
46...1861
47...3951
48...4288
49...1684
50...2155..4423
51...4321
52...5784
53...2172
54...5063
55...4112..2830
56...2478
57...5385
58...3351
59...2650
60...3111..2704
61...3937
62...1992
63...2229
64...1691
65...1752
66...5800
67...3295
68...2420
69...2159
70...1900..2457
71...3118
72...3181
73...1714
74...2715
75...1920..2352
76...2145
77...3190
78...5535
79...3169
80...1527..4305
81...2006
82...3658
83...2547
84...3720
85...2400
86...4801
87...3446
88...4409
89...3301
90...4749..4156
91...2586
92...5739
93...2347
94...2300
95...5501
96...4694
97...5130
98...2049
99...2432
100...2525..5414..1698..4605

Nulls:
5471
4145
4286
1683
4093

Appendix 16G.—EXTRACTS FROM THE "COLORADO" CODE

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

No. 342

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The

"COLORADO" CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

ENCODING

0...FWP..OCM..DMA		51...MPL	
1...KSU..RYV..AGL		52...VJS	
2...NBX..JPS..DSK		53...SXB	
3...YMJ..SPF..PCB		54...GMA	
4...LPW..GKX..QBG		55...MXF..VBX	
5...MCA..FBL..KPW		56...SWA	
6...BFC..MYV..OMJ		57...OGX	
7...RPA..CPS..MSG		58...GYM	
8...PWY..JXW..GSC		59...DXJ	
9...RBJ..QYA..NGW		60...VNO..PBL	
10...FCV..GBL..DCM		61...OSX	
11...JFU..ZBW..XPO		62...DYN	
12...VSY..NYK..CJF		63...FYM	
13...BNA..CFX..DWA		64...ZBA	
14...QJC..PLB..NWJ		65...XMY..VCX	
15...GNU..SGA..XBC		66...OGA	
16...RGS..NSV..GNP		67...DPA	
17...JBK..DGA..KXY		68...BWJ	
18...OXW..RBY..XYM		69...JBY	
19...BGR..DPL..RFY		70...OBX..WSX	
20...YWU..XJM..OWY		71...VYW	
21...NXO..BPG..QPJ		72...DMX	
22...PSA..SCO..FGN		73...KMY	
23...GVJ..KXO..OPB		74...WJX	Nulls:
24...JWC..NFC..MBC		75...GVA..ORF	XWO
25...NPJ..QMX		76...AXW	YXO
26...PFJ		77...XGD	WJS
27...LYW		78...SKC	PNW
28...VPA		79...ONS	LUW
29...SMD		80...CPA..LGJ	
30...GFU..CMX	Nulls:	81...PYW	
31...BKV	SKP	82...GXO	
32...KBV	VBY	83...CFG	
33...YPF	XOB	84...JMS	
34...SNW	AUS	85...WXV	
35...VJC..MGX	GWS	86...RFK	
36...ABW		87...OBL	
37...RWB		88...JFC	
38...NGA		89...CBA	
39...JPL		90...OPW..LYB	
40...DYW..RKC		91...SBN	
41...VSA		92...QPM	
42...JSC		93...GMS	
43...NBL		94...LBX	
44...CUY		95...PWA	
45...XJG..WCA		96...GPC	
46...GNA		97...YBW	
47...RMY		98...QVM	
48...APB		99...GWU	
49...YBM		100...DGX..JUW..RPX..WPA	
50...MGI..DCA			

Are having...PAT
Are not...SXW
Are we...CSA
Are you...DUL
Are you all right...FPA
Arm...PWO
Armored...QOY
Army...DOS..AUF
Army headquarters...BYW..DXS
Arrive...XSO
Arrived...ZOY..CMO..FPC
Artillery...KSM..YJW..XMP
Artillery fire...CJV
Artillery observer...ANK
Artillery position...FON
Artillery preparation...WAV
Artillery support...REL
-ary...FOK
As...GBX..XWC..FLB
As far as...BSY
As soon as...LUM..NUK
Ascertain...ONC
Ask...PNB
Asphyxiate...GLX
Assemble...FUG
Assist...BLU
Assistance...AXF
At...JAC..SYK..YON..COT
At close quarters...DGO
At once...WPX..XSA
At point...YSJ
-ate...DSX
Attack...BXM..YWA..SMP
Attacked...RGK
Attacking...LPY
Attempt...JXM
Attention...WEB
August...ABM
Austrian...DPX..NGP
Automatic...OVX
Automatic rifle...JSM
Automatic rifle ammunition...RPV
Available...JPY
Aviator...BNO
Await...KGM
Await instructions...VNY

Nulls:
LAY
ROB
GNW
PAY
WYS

Away...JWS
Axe (s)...NYB
B...PSJ..DCV..BWA
Back...YFM
Bad (ly)...VYG
Badly damaged...BKM
Badly wounded...DYF
Bag (s)...VEN
Balloon...QYO
Bank...MER
Barbed wire...NPA..GFB
Barrage...NYS..VCP..BGN
Barrage wanted...DOG
Barricade...MUS
Battalion...YAX..WAP..BAR
Battalion headquarters...DMO
Battery...VCA..AFM..GXY [NXB
Battle (s)...VAB
Bavarian...WSM
Bay (s)...FRX
Bayonet...GAL
Be...LGW..SNG
Be ready...VPK
Be released...BES
Because...FMP
Been...JAW..SYM
Before...QXP
Began...PBA
Begin...JOM..FAK
Begun...BMP
Behind...JGF
Behind the lines...MXY
Being...NUW..VMC
Being established...QSM
Being sent...AUX
Being shelled...DAR
Believe...WXG
Belong...VXK
Below...QPX
Belt (s)...JYG
Bengal flares...FUN
Best...RBS
Better...SBC
Between...RAS..LOR
Beyond...AMX
Billet (s)...FRA

Nulls:
PJV
FWY
VSX
GFY
PXM

-ion...NOG..OVA..DAW
-ly...GFP..JFY
-nd...MXA..NWP..ANP
-nt...OPL
-re...RWU..QVC
-s...LYN..ASV..DPG..OMB
-st...PWJ..BPA..SXM..GMC
-th...KMS..NFW..PLX

BPN...Perfect
BPO...Will not
BPS...Renew
BPU...All ready
BPW...Wing
BPX...Reoccupy
BPY...Early
BSA...Wire
BSC...Retire
BSJ...Bombarded
BSM...Rush
BSO...Return
BSP...Decrease
BSU...Troops
BSX...Returned
BSY...As far as
BUD...Has stopped
BUF...Visibility
BUG...Report condition of
BUK...Build | trenches
BUM...Leave
BUN...Communication
BUP...When
BUS...Enemy has lost heavily
BUT...Single
BUW...Relieving
BWA...B
BWC...Several
BWD...Reinforced
BWG.....
BWJ...68
BWM...Urgent
BWO...Revetting
BWP...Division headquarters
BWS...V
BWU...Confident
BWX...Right
BWY...Wire entanglements
BXA...No casualties
BXF...Consolidating
BXG...Were
BXK...Pigeon
BXL...Unchanged
BXM...Attack
BXO...Without delay
BXS...Wireless station
BXU...Extreme
BXW...Too far
BXP...Rifle
BXY...March

BYA...Commissioned officer
BYD...Round
BYF...Was
BYG...Flank
BYK...Work
BYL...Conclude
BYM...Defensive
BYN...Good
BYP...Reinforcements
BYS...Repeat
BYV...West of
BYW...Army headquarters
CAB...Small
CAF...Heavily
CAK...Will be
CAM...Repair
CAN...Coming
CAP.....
CAR...Reply at once
CAT...Correct
CAV...Wagon
CAW...June
CAX...The same
CBA...89
CBF...Top
CBG...Relief completed
CBJ...Trouble
CBM...E
CBN...We
CBO...Can be
CBP...Warning
CBS...Required
CBU...Double
CBW...Brigade
CBX...Too early
CBY...Has not been
CFA...Tomorrow
CFB...Relief will take place
CFG...83
CFK...Thursday
CFM...Lachrymatory
CFO...M
CFP...Confirm
CFS...Will open fire
CFV...Renew
CFW...Wood
CFX...13
CFY...Total
CJA...Slow
CJB...Many

Appendix 16H.—EXTRACTS FROM THE "SENECA" CODE

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

No. 457

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The

"SENECA"

TRENCH CODE

Precede every message in this code by
"SEN"

NOTE: The * indicates new word or phrase.

INSTRUCTIONS

1. This code book, to be known as the "Seneca" Code, is issued to division, brigade, regimental and battalion headquarters of your division. Whether or not it is issued to neighboring divisions must be determined by you before you send them telegrams encoded by its use. (See G. O. No. 172, G. H. Q. American E. F., 1918.)

2. IN CASE OF LOSS OF THIS BOOK, NOTIFY SUPERIOR AUTHORITY AT ONCE. BURN IF IN DANGER OF CAPTURE.

3. Coded messages sent by telephone will be preceded by the word "Seneca." If transmission is difficult, use the following telephone alphabet, authorized by G. O. No. 103, 1918:

A—Able	N—Nan
B—Boy	O—Opal
C—Cast	P—Pup
D—Dock	Q—Quack
E—Easy	R—Rush
F—Fox	S—Sail
G—George	T—Tare
H—Have	U—Unit
I—Item	V—Vice
J—Jig	W—Watch
K—King	X—X-ray
L—Love	Y—Yoke
M—Mike	Z—Zed

Example: If the operator receives "buy" as "vie," and difficulty is experienced in distinguishing "B" from "V," "buy" may be spelled "boy-u-y."

4. Coded messages sent by telegraph or radio will be preceded by the group "SEN."

5. The use of this code for regular routine reports should be limited to actual necessities. Such reports should be transmitted by other means than radio or earth-telegraphy.

6. Avoid use of words not in code book when other words with same significance are provided. Words spelled out, letter by letter, not only take time to code, transmit and decode, but they are one of the favorite points of attack by enemy code men.

7. Where two or more code groups are assigned the same letter, syllable, word or phrase, first one and then another should be used so that in a series of messages each occurs about the same number of times. In particular, no group should ever appear twice in the same message.

8. At least one group marked "Null" should be used for every ten code groups in a message. These should be placed at irregular intervals. A "Null" should always occur between double letters; thus, the word "boot" would be encoded:

(b)	(o)	(Null)	(o)	(t)
RBC	PXB	VAP	COD	VEM

Note that different groups are used for letter "O."

ENCODING

00...BAT..GPL
0...GWO..MEF..BAP
1...VEN..OCM..GAP
2...RGD..FJO..QYW
3...CMB..DGS..NUM
4...PJV..JAK..XMU
5...KSP..PLY..WEF
6...ORB..GPY..YMC
7...ABG..DYL..MOS
8...VPA..SPY..QVK
9...OSC..JUW..XPJ
10...CBP..NXP..PNU
11...NSV..DSK..VSF
12...RKY..GVO..AMY

0'clock:
13...KMD..YFJ..CPB OBK
14...SKX..BUT..NBA GNA
15...VXK..JOP..DUW PNR
16...RWK..DWJ..PAG
17...SCW..MGV..LAM

Minutes:
18...YJA..DOG..KPS DPL
19...PUX..VJB..FPO NCV
20...SON..FEK..OBL XUB
21...GFS..ZVC..QPF
22...LBW..SYP..CSV
23...SNG..JGL..BET
24...RYK..QEP..VMA
25...ZOB..SUC
26...REL

Nulls:
27...BKS BNA
28...YWX NCJ
29...FON NAG
30...POV..JEX DEP
31...MJP REF
32...ZAS
33...VOL
34...JXM

battalion
35...ONV BYG..XAP..JSO
36...OVB
brigade
37...WXO SBN..OPS..CBG
38...CAN
corps
39...LET XJU..RKB
40...MUC..RUW
division
41...GEX WNV..LBY
42...LGN
regiment
43...WCO DWA..OSJ..ABY
44...BJU
45...KVP
46...MXS
47...NOW
48...DPB
49...WOV
50...QMV..JBX
51...VYN
52...JSX
53...PWU
54...XFW
55...MYF
56...GKO
57...XBN
58...BYN
59...KGW
60...DAR..QJW
61...NWU
62...BGR
63...NCS

Nulls:
64...JWA DWS
65...WUP QAM
66...COT BJP
67...FLY YFG
68...MCB XFM
69...OXA
70...SBP..WSO
71...YUJ

first...SPG..KGO
72...RFX
73...JPU

second...YPM..NAK
74...QAX
75...SXJ..APF

third...MGW..PBR
76...SMO
77...XON

fourth...VEF..MAT
78...DMA
79...YXG

fifth...WXM..LOP
80...YOB..FCK
81...XJC

sixth...QPX..DAL
82...LYN
83...YAW

seventh...VXG..KBG
84...AFO
85...JVN

eighth...QBM..SOW
86...QXP
87...LUB

ninth...GOC..BSC
88...MPO
89...NAM

tenth...AWC..PWS
90...KBS..BWD
91...OLU
92...WAX
93...SPK
94...FWP
95...GMA
96...LOM
97...GLX
98...NPS
99...XUN
100...KXF..RMX..RPS..PFY

DECODING

ABE...bombarded.
ABF...notice
ABG...7
ABK...degree (s)
ABM...ridge
ABO...D
ABP...-non
ABS...converge
ABV...take place
ABW...mistake
ABX...are not
ABY...Regiment
AFC...-es
AFD...sometime
AFJ...S
AFM...very
AFO...84
AFR...Boche
AFV...sandbag
AFX...patrol schedule
AFY...emplacement
AGB...we are in need of
AGE...hundred
AGF...situation
AGK...aeroplane
AGL...understand
AGN...question mark
AGO...following
AGU...ward
AGY...send out patrols
AMC...complete
AMG...moving
AMK...permission
AMO...do
AMP.....
AMS...incendiary
AMV...station
AMX...barrage
AMY...12
AND...weather conditions
ANF...enemy infantry
ANG...mask
ANK...open
ANO...H
ANP...British
ANS...when shall we be relieved
ANW...millimeter (s)
ANX...force
ANY...why
APB...an
APE...my
APF...75
APJ...radio message
APN...come
APO...-ty
APU...foot
APW.....
APX...our artillery
APY...all points
ASB...report
ASF...heavy
ASG...was not
ASK...cross-road
ASM...should be
ASO...-im
ASP...regulate
ASV...be released
ASX...Third Corps
ASY...has destroyed
AUB...storm
AUF...A
AUG...large
AUK...were not
AUM...-ate
AUP...on
AUS...missing
AUW...enemy artillery
AUX...until
AWB...general
AWC...tenth
AWE...numbering
AWG...(null)
AWK...October
AWO...working party
AWP...is there any gas
AWS...out of
AWX...comply
AWY...more
AXB...required
AXF...has
AXG...to be
AXM...being sent
AXP...suffocate
AXS...him
AXV...relief
AXW...detachment
AXY.....
BAD...new
BAF...as
BAG...machine gun

Appendix 16I.—EXTRACTS FROM THE "CHAMPLAIN" CODE

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

No. 131

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The "CHAMPLAIN" CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY FORCES

ENCODING

0...SCP..RGX..PSC
1...WPX..FBP..VSD
2...APJ..YOP..KGX
3...FCV..QXA..WEV
4...COM..SOP..WSO
5...RBO..YUX..NAW
6...GLP..QEM..DOS
7...OWL..RGU..JWC
8...RAG..GXJ..SCB
9...BOW..KVS..ZAB
10...BES..GAY..FUP
11...LOK..KBY..GFK
12...BKX..WNX..PBA
13...OXP..CSY..WJO
14...NCW..DMA..FPG
15...CPL..MSY..PUN
16...FWJ..XOG..MYG
17...GMX..AGE..XBA
18...FRM..DXS..CBW
19...NUR..VAX..FSM
20...POV..LEP..JVB
21...KMS..BNM..OBY
22...FEW..AMG..QOS
23...JMY..LGS..AUK
24...QMC..OGP..FYG
25...XFW..OCX
26...GNW
27...YPK
28...KMA
29...DUG
30...ABP..MAN
31...NBA
32...OSA
33...XUF
34...PLG
35...OCJ
36...MGL
37...YJV
38...ZVA
39...RUT
40...FOL..JBO
41...PXS
42...GBW
43...SYN
44...MJX
45...FJV
46...NOR
47...YAX
48...XWP
49...ASG
50...SBJ..CPY

Nulls:
BPF
YAW
FPW
AUM
LGP

51...SNB
52...JOM
53...ZBA
54...DWS
55...DEB
56...DGV
57...VCF
58...BAN
59...WYV
60...SUB..OLJ
61...BXM
62...GSM
63...LAK
64...WOS
65...MAV
66...CAT
67...NUG
68...YFM
69...XJP
70...GEF..SAC
71...QAX
72...DCM
73...NGX
74...WXP
75...GFX..RBX
76...AXB
77...VOY
78...OVX
79...KPL
80...BUD..SWU
81...CMS
82...NPU
83...ROM
84...BYL
85...JYB
86...VYM
87...WAV
88...FAD
89...ONX
90...QYW..JFC
91...BGF
92...GPW
93...SNO
94...PUB
95...DIS
96...PJV
97...YUM
98...XYF
99...RPA
100...SXJ..VXM..SYG..ORF

Nulls:
PAR
CFX
ZVB
DIW
SGM

3

Appendix 16J.—EXTRACTS FROM THE "HURON" CODE

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

№ 1644

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The "HURON" CODE

Precede every message in this code by "HUR"

NOTE: The * indicates new word or phrase.

ENCODING

0...MYB..BMS..JUG		51...JPM	
1...REX..QAP..CUN		52...VPW	
2...NFY..JEB..SKX		53...DWA	
3...MXG..CUY..JYW		54...PFR	
4...KXB..ROS..YXV		55...FSM	
5...FUB..SNV..FGL		56...DOT	
6...PES..BSP..NBA		57...XPR	
7...WUS..NFC..BAF		58...AWX	
8...OXV..GEX..SGV		59...NOR	
9...AFV..NGK..PAR		60...QSO..LPU	
10...FWP..WBS..YPB		61...DUL	
11...LUP..GMP..XOP		62...LBS	
12...GNC..YMV..SXY		63...KXS	
13...DGB..ONC..DIT		64...RUG	
14...VYP..FEV..XYM		65...WYM	
15...PBX..LAV..PFW		66...ASB	
16...WXS..YBJ..LGF		67...BKX	
17...YOB..BPG..ABV		68...SAP	
18...BUN..RPO..MPB		69...MAC	
19...CJM..GAW..SOF		70...GBM..CMG	
20...NCW..DAL..SCU		71...CSX	
21...GPO..RYB..JVB		72...NPJ	Nulls:
22...XUS..KBG..VJX		73...QEK	OLD
23...NAS..GYV..MCU		74...OPY	BGX
24...KPN..VMS..QOV		75...BLG..QYV	REK
25...PWC..KSX		76...XSY	VAG
26...FCX		77...VAK	SYL
27...VEM	Nulls:	78...FAV	
28...DYB	XPO	79...KGF	
29...SUY	LBW	80...YAX..BFS	
30...JOR..LOW	MEV	81...VNP	
31...OKB	MSU	82...FSP	
32...NYV	GMA	83...JMP	
33...GLJ		84...RFS	
34...DEL		85...FXM	0'clock:
35...PUM		86...QJW	OSY
36...QMP	0'clock:	87...PWY	BET
37...GOS	VPN	88...LOB	VPN
38...YJX	OSY	89...WJX	
39...WMP	BET	90...VXY..YSJ	
40...KMS..DPW		91...JGB	
41...OGW		92...AXF	
42...AGL		93...OBG	
43...PLO		94...QPA	
44...APJ		95...YWC	
45...QPM		96...PNA	
46...DXM		97...JYM	
47...POM		98...MEP	
48...MSP		99...RGU	
49...GMC		100...SCK..XFS..OLG..ZVA	
50...CFA..DSB			

Appendix 16K.—EXTRACTS FROM THE "OSAGE" CODE

SECRET

MUST NOT FALL
INTO HANDS OF
ENEMY

MEMORIZE THIS GROUP:
"DAM---Code Lost."

The

"OSAGE"

TRENCH CODE

Precede every message in this code by
"OSA"

NOTE: The * indicates new word or phrase.

ENCODING

*00...DAN..PNW		50...SAK..LBC	
0...FRP..SNG..YPV		51...BGW	
1...DGW..OXK..WSB		52...SYF	
2...KBM..VYP..BNF		53...OCJ	
3...LGF..MCO..YAS		54...RAV	
4...NGS..DYN..QSG		55...GMX	
5...BOL..PLY..JSK		56...WNO	
6...ZOB..LES..AFV		57...CJB	
7...SPO..FUW..VPN		58...PCB	
8...MSO..DPB..KMX		59...JPK	
9...XFC..BAR..RKO		60...VJS..ABY	
10...FUC..PSM..JVY		61...GPB	
11...ZBP..OBC..BKS		62...OKG	
12...OVK..KXW..BWC		63...LBX	Nulls:
13...VNF..GNY..KBA		64...PYN	GXJ
14...OWE..BUS..RFO		65...DWX	AGY
15...COS..LBP..NCV		66...BPF	WSO
16...DOB..OSV..WPA		67...NBP	DYW
17...CMU..YXZ..NAS		68...QMP	ZBS
18...JEV..PEV..GFX		69...ASO	
19...ANO..XOB..FAM		70...GPY..KVX	
20...PAR..WOF..BMA		71...WUO	
21...ROW..GOP..SUN		72...FPL	
22...DSB..XGW..NXA		73...JPS	
23...AWB..QYP..FOB		74...FBP	
24...XMP..FSA..DUN		75...RPJ..DXO	
25...RWY..LAN		76...YMX	
26...YUM		77...FGW	
27...KPW	Nulls:	78...XAY	
28...MAR	JBA	79...MBX	
29...QVP	XAM	80...DCP..CBP	
30...AXS..ZAB	JSM	81...JXW	
31...QJS	XBY	82...WBJ	0'clock
32...GAK	RUC	83...ORA	OKU
33...MJS		84...NEF	YWU
34...NWB		85...BFA	JEW
35...CAF		86...SKM	
36...YBX		87...JBU	
37...FED		88...NOK	
38...SBW		89...BSA	
39 ..JYS		90...RGU..XPB	
40...VCU..BEV		91...MBC	
41...RBL	0'clock:	92...NUR	
42...KVF	YWU	93...DMX	
43...MGI	OKU	94...QAM	
44...GVA	JEW	95...LOC	
45...PXK		96...BXW	
46...BLX		97...PON	
47...BXK		98...YSV	
48...YOU		99...FLP	
49...OGN		100...QEX..OPV..JOG..WJB	

Appendix 16L.—EXTRACTS FROM FIELD CODE No. 1

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

No. 271

MEMORIZE THIS GROUP:
"DAM---Code Lost."

FIELD CODE
No. 1

Precede every message in this code by "FC1"

Appendix 16M.—EXTRACTS FROM FIELD CODE No. 2

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

No. 2504

MEMORIZE THIS GROUP:
"DAM—Code Lost."

FIELD CODE
No. 2

Precede every message in this code by "FC2"

SECRET

EMERGENCY CODE LIST

To be used only with Field Code No. 2.
To be issued to companies.
To be used only for communications within divisions.
To be completely destroyed, by burning, when in danger of capture or after a new code has been issued.

Precede Every Message in This Code by "C 2"

About to advance...FX
Ammunition exhausted...CZ
Are advancing...AV
At...ZB
Attack failed...XP
Attack successful...ZX
Barrage wanted...PM
Be ready to attack...FZ
Being relieved...BJ
Captured...PX
Casualties heavy...FY
Casualties light...BD
Center...XA
Enemy...FB
Enemy barrage commenced...PF
Enemy fire has destroyed...SB
Enemy machine gun fire serious...PO
Enemy trenches...XB
Everything O. K....AZ
Everything quiet...CP
Falling back...AP
Gas is being released...SC
Have broken through...XG
How is everything...ZP
Increase range...SF
Left...PV
Look out for signal...CX
Machine gun ammunition needed...FA
Message not understood...BX
Message received...ZJ
Near...AG
Need water...BP
Not ready...PB
Objective reached...AX
Our...XF
Our artillery is shelling us...FM
Raiders have left...AW
Recall working party...SM
Reinforcements needed...XY
Relief being sent...BS
Relief completed...CA
Rifle ammunition needed...CB
Right...SP
Rush...AF
Situation improving...ZF
Situation serious...BM
Stopped...FC
Stretcher bearers needed...SZ
Strong attack...AB
Tank stuck...PG
Trenches...FS
Trenches have been occupied...CM
Troops...SX
Using gas shells...BF
Using high explosive shells...SA
Wire entanglements destroyed...BY

AB...Strong attack
AF...Rush
AG...Near
AP...Falling back
AV...Are advancing
AW...Raiders have left
AX...Objective reached
AZ...Everything O. K.
BD...Casualties light
BF...Using gas shells
BJ...Being relieved
BM...Situation serious
BP...Need water
BS...Relief being sent
BX...Message not understood
BY...Wire entanglements destroyed
CA...Relief completed
CB...Rifle ammunition needed
CM...Trenches have been occupied
CP...Everything quiet
CX...Look out for signal
CZ...Ammunition exhausted
FA...Machine gun ammunition needed
FB...Enemy
FC...Stopped
FM...Our artillery is shelling us
FS...Trenches
FX...About to advance
FY...Casualties heavy
FZ...Be ready to attack
PB...Not ready
PF...Enemy barrage commenced
PG...Tank stuck
PM...Barrage wanted
PO...Enemy machine gun fire serious
PV...Left
PX...Captured
SA...Using high explosive shells
SB...Enemy fire has destroyed
SC...Gas is being released
SF...Increase range
SM...Recall working party
SP...Right
SX...Troops
SZ...Stretcher bearers needed
XA...Center
XB...Enemy trenches
XF...Our
XG...Have broken through
XP...Attack failed
XY...Reinforcements needed
ZB...At
ZF...Situation improving
ZJ...Message received
ZP...How is everything
ZX...Attack successful

00...OWG..SMD				50...CAM..RMC			
0...VOR..WNC..XBC				51...ZAB			
1...GWU..FLY..DOK				52...SBY			
2...CUW..BKV..ASK				53...OBP			
3...JOY..PLX..ZBP		O'clock:		54...FCO			
4...WYK..PBN..KGM		CJM		55...WUX			
5...WSY..LGA..DEM		DMB		56...GAD			
6...VBO..QOF..SXB		SCB		57...OSV			
7...BFJ..WCP..JGB				58...YAB			
8...AFD..ROX..NXA				59...QXO			
9...FBL..GBM..XOG		Minutes:		60...DUC..RFG			
10...MEN..NOR..WBJ		AXF		61...MPJ			
11...GLO..RWP..BXG		BNK		62...JXW		Nulls:	
12...FOK..YJA..XWB		ONP		63...PUK		YAX	
13...WPC..QSO..OLJ				64...KSP		OMB	
14...RGN..DWS..JXA				65...JMS		REF	
15...MUG..KPN..COD				66...LOX		DYK	
16...LYP..PWY..SOX				67...BMO		JOM	
17...BNW..VJX..JAB		Nulls:		68...MGL			
18...WJO..NBL..AXG		PFY		69...QJM			
19...OPV..SBL..YWC		FMO		70...SUM..NAB			
20...FEW..GPX..YBO		ZAS		71...VEP			
21...OXS..FRM..CPS		GAV		72...DXS	first...JUM		
22...RAG..QBM..JSX		XFW		73...WBX	[..OVS		
23...BAW..KVY..PYV				74...OGF	second...KBY		
24...MJO..NEK..SNY				75...AMC..XFB	[..DOP		
25...XGO..VYB				76...RYP	third...LEG		
26...GCK				77...NSO	[..NCO		
27...ANP				78...FLJ	fourth...MEW		
28...PEW				79...BUT	[..DCV		
29...FGU				80...XOS..GSY	fifth...SWB		
30...GUV...XSC				81...FUK	[..PXK		
31...CFK				82...PCU	sixth...VNP		
32...RBP				83...JVN	[..BPJ		
33...BSO	battalion...MOB			84...CBJ	seventh...WEG		
34...YPF	[..OWE..DYL			85...KBS	[..GYL		
35...ONC	brigade...FXA			86...NGF	eighth...APN		
36...JPW	[..LOM..GNS			87...LAD	[..YOP		
37...DPX	corps...SYK..PBO			88...DGX	ninth...RMY		
38...KBA				89...MAR	[..CBP		
39...DAY	division...NOW			90...MXG..SNA	tenth...SAM		
40...LBC..BOW	[..QAX			91...CJV	[..GPJ		
41...MBU	regiment...DMO			92...VAG			
42...JEB	[..XWU..VOD			93...BGW			
43...SGM				94...WAM			
44...YMO				95...GXP			
45...VMP				96...ABO			
46...GFP				97...NYF			
47...WMJ				98...RUM			
48...POK				99...GMY			
49...AUS				100...FAK..YSX..FWY..XAB			

Appendix 16N.—EXTRACTS FROM FIELD CODE No. 3

SECRET

MUST NOT FALL INTO HANDS OF ENEMY

Nº - 2393

MEMORIZE THIS GROUP:
"DAM---Code Lost."

FIELD CODE
No. 3

Precede every message in this code by "FC3"

00...GFM..SWC				50...DYB..ASG			
0...DAB..KVF..PWB				51...CSM			
1...MGW..RAG..QMC				52...OWA			
2...NGU..JMP..FRO				53...MES			
3...BWA..REM..GAY				54...YUJ			
4...CFO..MSP..VCS		O'clock:		55...WNA			
5...WPJ..YXJ..JUD		LES		56...NOW			
6...XGW..AGE..KBO		GOP		57...JEG			
7...YAP..PNB..DOT		XYB		58...GPS			
8...FCK..ROG..OMS				59...XBC			
9...BNC..LBX..WAP				60...SOB..QOJ			
10...COS..SMA..GLJ		Minutes:		61...XUP			
11...LUN..YOC..PYW		RUW		62...RWY			Nulls:
12...NYK..NCX..QAP		BOP		63...PUB			PBA
13...BYV..YPS..FUR		ORA		64...FAM			VNP
14...XAJ..PBY..VAF				65...AUW			BOS
15...XPL..SAM..JOM				66...FSM			ZAB
16...FJO..KMU..DIS				67...BLD			KGM
17...BEP..SYG..OKY		Nulls:		68...YJO			
18...CJX..ZOB..VXF		QEF		69...VBC			
19...MBY..NAP..WJX		XWC		70...CUB..MXF			
20...NSV..QXO..GUM		LGB		71...JPO			
21...BXM..JFW..PSC		GAD		72...MJP		first..WPO..APJ	
22...WYB..GXV..QPF		FMC		73...KGA			
23...XFA..RGA..FYB				74...GWC		second..FBO	
24...YFA..RPX..GEK				75...NWU..DPX			[..WSX
25...XJW..LAP				76...OCA		third..VAG..WJC	
26...VJM				77...AMX			
27...FEW				78...OCW		fourth..QMO	
28...SPK				79...BSX			[..XYM
29...VOR				80...RKY..WBY		fifth..WCU..AMS	
30...BKC..MOP				81...WSC			
31...JXO				82...KPV		sixth..PUX..KMA	
32...DEF				83...VSM			
33...QVC		battalion..YWX		84...XOK		seventh..QYJ	
34...DSV		[..QEM..CJO		85...SGR			[..MEN
35...LOR		brigade..LEP		86...GNB		eighth..PUS	
36...JAS		[..JSV..CUS		87...FBL			[..QEV
37...OPY		corps..BXU..ABF		88...POT		ninth..YWJ..CBJ	
38...MAV		division..XWU		89...PXA			
39...RBV		[..VAK		90...FLY..OXW		tenth..BNK..ROP	
40...NUP..WOB		regiment..MGD		91...BFX			
41...AXY		[..APX..GAK		92...QJC			
42...BPW				93...ABV			
43...VYL				94...DCA			
44...CAX				95...FPK			
45...PFR				96...LYW			
46...GOD				97...MYS			
47...WUA				98...GBU			
48...SBX				99...OBA			
49...PYB				100...PEG..VMB..FON..JVC			

Appendix 17.—THE EMERGENCY CODE LISTS

SECRET

EMERGENCY CODE LIST

To be used only with Field Code No. 1.
To be issued down to companies.
To be used only for communications within divisions.
To be completely destroyed, by burning, when in danger of capture or after a new code has been issued.

Precede Every Message in This Code by "C 1"

About to advance...BY
Ammunition exhausted...FB
Are advancing...PX
At...SX
Attack failed...BM
Attack successful...PF
Barrage wanted...XF
Be ready to attack...ZF
Being relieved...XA
Captured...CB
Casualties heavy...AW
Casualties light...FZ
Center...PB
Enemy...FC
Enemy barrage commenced...PV
Enemy fire has destroyed...SP
Enemy machine gun fire serious...AF
Enemy trenches...BP
Everything O. K...CA
Everything quiet...XG
Falling back...BX
Gas is being released...AG
Have broken through...SA
How is everything...BD
Increase range...SB
Left...AB
Look out for signal...SZ
Machine gun ammunition needed...CX
Message not understood...PO
Message received...ZX
Near...SM
Need water...CP
Not ready...FA
Objective reached...CZ
Our...XP
Our artillery is shelling us...FM
Raiders have left...BS
Recall working party...AV
Reinforcements needed...CM
Relief being sent...XY
Relief completed...AZ
Rifle ammunition needed...XB
Right...BF
Rush...ZP
Situation improving...FY
Situation serious...BJ
Stopped...FX
Stretcher bearers needed...AP
Strong attack...PG
Tank stuck...SF
Trenches...PM
Trenches have been occupied...ZJ
Troops...SC
Using gas shells...AX
Using high explosive shells...FS
Wire entanglements destroyed...ZB

AB...Left
AF...Enemy machine gun fire serious
AG...Gas is being released
AP...Stretcher bearers needed
AV...Recall working party
AW...Casualties heavy
AX...Using gas shells
AZ...Relief completed
BD...How is everything
BF...Right
BJ...Situation serious
BM...Attack failed
BP...Enemy trenches
BS...Raiders have left
BX...Falling back
BY...About to advance
CA...Everything O. K.
CB...Captured
CM...Reinforcements needed
CP...Need water
CX...Machine gun ammunition needed
CZ...Objective reached
FA...Not ready
FB...Ammuntion exhausted
FC...Enemy
FM...Our artillery is shelling us
FS...Using high explosive shells
FX...Stopped
FY...Situation improving
FZ...Casualties light
PB...Center
PF...Attack successful
PG...Strong attack
PM...Trenches
PO...Message not understood
PV...Enemy barrage commenced
PX...Are advancing
SA...Have broken through
SB...Increase range
SC...Troops
SF...Tank stuck
SM...Near
SP...Enemy fire has destroyed
SX...At
SZ...Look out for signal
XA...Being relieved
XB...Rifle ammunition needed
XF...Barrage wanted
XG...Everything quiet
XP...Our
XY...Relief being sent
ZB...Wire entanglements destroyed
ZF...Be ready to attack
ZJ...Trenches have been occupied
ZP...Rush
ZX...Message received

SECRET EMERGENCY CODE LIST

To be used only with the "Huron Code."
To be issued down to companies.
To be used only for communications within divisions.
To be completely destroyed, by burning, when in danger of capture or after a new code has been issued.

Precede Every Message in This Code by "RO"

About to advance...SP
Ammunition exhausted...BX
Are advancing...XF
At...AG
Attack failed...FS
Attack successful...XA
Barrage wanted...BD
Be ready to attack...SM
Being relieved...ZB
Captured...AX
Casualties heavy...BJ
Casualties light...SF
Center...XY
Enemy...PF
Enemy barrage commenced...SB
Enemy fire has destroyed...AV
Enemy machine gun fire serious...ZF
Enemy trenches...BS
Everything O. K...CZ
Everything quiet...FC
Falling back...SX
Gas is being released...AB
Have broken through...PG
How is everything...FA
Increase range...XG
Left...BP
Look out for signal...AZ
Machine gun ammunition needed...XB
Message not understood...CM
Message received...ZP
Near...SA
Need water...CP
Not ready...FZ
Objective reached...AP
Our...CA
Our artillery is shelling us...PV
Raiders have left...CX
Recall working party...FB
Reinforcements needed...PX
Relief being sent...AW
Relief completed...XP
Rifle ammunition needed...SZ
Right...BF
Rush...PO
Situation improving...ZX
Situation serious...CB
Stopped...FM
Stretcher bearers needed...ZJ
Strong attack...PM
Tank stuck...FY
Trenches...AF
Trenches have been occupied...PB
Troops...SC
Using gas shells...BM
Using high explosive shells...FX
Wire entanglements destroyed...BY

AB...Gas is being released
AF...Trenches
AG...At
AP...Objective reached
AV...Enemy fire has destroyed
AW...Relief being sent
AX...Captured
AZ...Look out for signal
BD...Barrage wanted
BF...Right
BJ...Casualties heavy
BM...Using gas shells
BP...Left
BS...Enemy trenches
BX...Ammunition exhausted
BY...Wire entanglements destroyed
CA...Our
CB...Situation serious
CM...Message not understood
CP...Need water
CX...Raiders have left
CZ...Everything O. K.
FA...How is everything
FB...Recall working party
FC...Everything quiet
FM...Stopped
FS...Attack failed
FX...Using high explosive shells
FY...Tank stuck
FZ...Not ready
PB...Trenches have been occupied
PF...Enemy
PG...Have broken through
PM...Strong attack
PO...Rush
PV...Our artillery is shelling us
PX...Reinforcements needed
SA...Near
SB...Enemy barrage commenced
SC...Troops
SF...Casualties light
SM...Be ready to attack
SP...About to advance
SX...Falling back
SZ...Rifle ammunition needed
XA...Attack successful
XB...Machine gun ammunition needed
XF...Are advancing
XG...Increase range
XP...Relief completed
XY...Center
ZB...Being relieved
ZF...Enemy machine gun fire serious
ZJ...Stretcher bearers needed
ZP...Message received
ZX...Situation improving

SECRET

EMERGENCY CODE LIST

To be used only with the "Seneca Code."

To be issued down to companies.

To be used only for communications within divisions.

To be completely destroyed, by burning, when in danger of capture or after a new code has been issued.

Precede every message in this code by "NA."

About to advance...AV
Ammunition exhausted...XA
Are advancing...CB
At...PO
Attack failed...CZ
Attack successful...ZB
Barrage wanted...XP
Be ready to attack...BF
Being relieved...AP
Captured...ZF
Casualties heavy...XG
Casualties light...FY
Center...BX
Enemy...CA
Enemy barrage commenced...AF
Enemy fire has destroyed...BY
Enemy machine gun fire serious...FZ
Enemy trenches...ZJ
Everything O. K....SB
Everything quiet...FA
Falling back...BS
Gas is being released...PX
Have broken through...PG
How is everything...AZ
Increase range...XY
Left...SZ
Look out for signal...FS
Machine gun ammunition needed...BD
Message not understood...SF
Message received...BM
Near...SA
Need water...CX
Not ready...PF
Objective reached...AX
Our...PM
Our artillery is shelling us...CM
Raiders have left...BP
Recall working party...ZP
Reinforcements needed...ZX
Relief being sent...SX
Relief completed...AB
Rifle ammunition needed...FM
Right...FB
Rush...CP
Situation improving...FC
Situation serious...AW
Stopped...AG
Stretcher bearers needed...XB
Strong attack...SP
Tank stuck...PB
Trenches...SM
Trenches have been occupied...PV
Troops...BJ
Using gas shells...FX
Using high explosive shells...XF
Wire entanglements destroyed...SC

AB...Relief completed
AF...Enemy barrage commenced
AG...Stopped
AP...Being relieved
AV...About to advance
AW...Situation serious
AX...Objective reached
AZ...How is everything
BD...Machine gun ammunition needed
BF...Be ready to attack
BJ...Troops
BM...Message received
BP...Raiders have left
BS...Falling back
BX...Center
BY...Enemy fire has destroyed
CA...Enemy
CB...Are advancing
CM...Our artillery is shelling us
CP...Rush
CX...Need water
CZ...Attack failed
FA...Everything quiet
FB...Right
FC...Situation improving
FM...Rifle ammunition needed
FS...Look out for signal
FX...Using gas shells
FY...Casualties light
FZ...Enemy machine gun fire serious
PB...Tank stuck
PF...Not ready
PG...Have broken through
PM...Our
PO...At
PV...Trenches have been occupied
PX...Gas is being released
SA...Near
SB...Everything O. K.
SC...Wire entanglements destroyed
SF...Message not understood
SM...Trenches
SP...Strong attack
SX...Relief being sent
SZ...Left
XA...Ammunition exhausted
XB...Stretcher bearers needed
XF...Using high explosive shells
XG...Casualties heavy
XP...Barrage wanted
XY...Increase range
ZB...Attack successful
ZF...Captured
ZJ...Enemy trenches
ZP...Recall working party
ZX...Reinforcements needed

Appendix 18.—THE "STAFF CODE" AND SAMPLE OF ENCIPHERING TABLES

Secret

STAFF CODE

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY
FORCES

A. G. O. PRINTING DEPARTMENT, G. H. Q. A. E. F.
1918

INSTRUCTIONS

This code will be known as the Staff Code and will be used only at General Headquarters and such other headquarters as may hereafter be designated.

DESCRIPTION.

The book is built up in two series, known respectively as the Righthand and Lefthand Columns. Each series has its own distinctive four-letter groups, but the number groups run consecutively throughout the book. The Lefthand Column is intended primarily to provide a comprehensive alphabetical list of proper names of towns, cities, rivers, persons; a large number of spelling combinations; numerals; the less commonly used articles of equipment and supply; and a list of the army organization in France.

In the Righthand Column appear the commonly used words and phrases.

The book is made up with 100 groups on a page, 50 groups in the Righthand Column and 50 groups in the Lefthand Column.

The code is arranged alphabetically throughout, and there are no caption headings. In coding a message it is necessary simply to take the words in the order in which they appear in the written message. For example, in coding the phrase, "Field Supply and Ammunition Train," the operator will look for the word "Field," not for "Supply" or "Ammunition," as might be the case under a caption code.

Throughout the book there appear certain words known as variants, which are to be used in messages from time to time to avoid the repetition in a long message of certain words most commonly used. These variants are indicated on the margins of the pages on which they occur alphabetically. They appear after such words as "with," "to," "commanding officer," "paragraph," "period," etc. It must be borne in mind that it is the frequent repetition of groups which makes easy the breaking down of coded messages by the enemy.

A further safeguard is provided by an alphabet in the Lefthand Column which makes it possible to change from one column to the other in spelling words.

In the Righthand Column the groups are built up entirely of consonants, arranged in alphabetical sequence, the apparent breaks in this sequence being intentional omissions of bad telegraphic combinations.

In the Lefthand Column the groups invariably contain two vowels and two consonants, arranged in logical sequence.

Groups will be taken from whichever column they appear, as, for example, in the phrase, "An aeroplane brought down at Toul," the word "Toul" would be found in the Lefthand Column, while the remainder of the phrase would be in the Righthand.

For messages whose importance makes absolute clarity imperative, phrases are provided for punctuation, beginning and ending of spelling, and for quotations.

In certain places throughout the book marginal reference is made to certain parts of the Lefthand Column to facilitate coding of messages.

CODING.

The following message indicates the manner of coding by using the letter combinations:

May 21. 21:45 (JOFO DUMY)

Your division (XMNR)	will move (XDSW)	on the night of (NXPW)	May (MRFM)
30 (VPNR)	31 (VPRP)	to (VSPG)	Boston (FACO)
in the (KVRS)	rest camp (RSXM)	formerly (JFXM)	occupied by (NVRX)
the (BFSP)	101st Infantry (AKOC)	Period (BKPK)	Further orders (JRPB)
will be sent (XDFP)	you (XMCP)	there (VNRM)	(end of message) (GMFS)

Unless directed to the contrary, all messages will be sent in the four-letter combinations, figure groups being used only under certain prescribed conditions.

DISTORTION OF MESSAGES.

In connection with this code certain distortion tables will be used, and these tables will be in force from and to such time as may be designated.

The method of distortion is simple and consists in the substitution of the groups as they appear in the finished message for the combinations appearing in the distortion table. These tables are made up in groups of two letters each. It is necessary, therefore, to divide the four-letter groups into two-letter groups. and substitute for use in the completed message the equivalents taken from the distortion tables. In putting up messages in code the Enciphering Table will be used, and in taking out code messages the Deciphering Table.

For example, the following message:

"How many rounds have you on hand?"

would appear in code as follows:

"How many rounds	have you	on hand	?"
(KJGJ)	(KBXB)	(NXFJ)	(RBRM)

and would be sent in that way provided no distortion were used. After distortion it might read:

(KJGJ)	(KBXB)	(NXFJ)	(RBRM)
SABL	RLAC	DUFZ	ANLY

and would be so dispatched.

The process would be reversed on receipt, using the Deciphering Table.

DATE AND HOUR TABLE.

The following table is provided for use in designating concisely and accurately the exact date and hour of a message, and the telegram so designated may thereafter be referred to by the use of those particular groups.

January	B	0	A	0	B	0	A	0	B	0	A	0	D
February	D	1	I	1	F	1	I	1	D	1	E	1	F
March	F	2	O	2	G	2	O	2	F	2	I	2	G
April	G	3	U	3	J			3	G	3	O	3	J
May	J			4	L			4	J	4	U	4	L
June	L			5	M			5	L	5	Y	5	M
July	M			6	N			6	N			6	P
August	N			7	P			7	P			7	V
September	P			8	S			8	V			8	X
October	R			9	V			9	W			9	Z
November	S												
December	V												

..O (Before 12 noon) ..Y (After 12 noon)

For example, the date, January 29, 22:53, will appear as:

January 29, 22:53
B OV OF YJ

Add to this message the letter "Y," since the message is *after* 12 o'clock noon, and divide into two groups of four letters each. The date group then reads: BOVO FYJY.

In referring to this message it may be designated as "Your BOVO FYJY."

These groups should invariably contain four letters.

In the date group, May 1, 8:16, the groups would appear as follows:

May 1, 8:16
J AF AV EP

Add to this "O" since the message is *before* 12 o'clock noon, and the group reads: JAFA VEPO.

It will be noticed that the date is coded as though it read: "May (0)1, (0)8:16," in order to complete the four-letter combinations.

PERMUTATION.

Frequently a group will be received in a garbled condition through errors in transmission. This necessitates testing each letter of the garbled group until the correct group is found, and this is done by substituting for the tested letter all letters found in the same relative position to the three remaining letters of the garbled group.

For example, should the group PNPX come in garbled form, and be received SNPX, by substituting for the first letter S every letter found to be the first letter of a group having for the last three letters NPX, you will try BNPX, CNPX, FNPX and so on, changing the first letter each time, until by the context you find that PNPX is the correct group. Should the test on the first letter give no result, the second letter of the garbled group must be tested, and this is done by trying all groups having the first, third and fourth letters similar to the garbled group. For example, should the group PNGV be received in a garbled condition, reading PJGV, the context of the message indicating that PJGV is not the correct group, you will try PBGV, PDGV, PFGV, and so on, until you strike PNGV and find that group to be the correct one. In the Righthand Column it will be seen that the first two letters of every group are repeated one hundred times; that the third letter is repeated ten times, and that the last letter changes each time. For example, there are one hundred groups commencing with PN, ten groups having PNV for the first three letters, and so on throughout the Righthand Column. In testing the last letter of a group it will be seen that the correct group is one of the ten groups having the same first three letters as the garbled group. In testing the third letter of a group it will be seen that the correct group is one of a possible ten having the first, second and fourth letters similar to the garbled group. Permuting a garbled group simply consists in substituting for the tested letter a letter which bears the same relative position to the three remaining letters of a garbled group. If figure characters are used instead of letter characters, the process is the same. In testing the first figure of the group 43,649 you will try 23,649, 33,649, and when you reach 43,649 the context will show that the correct group has been found. In testing the second figure try 40,649, 41,649, 42,649 until by the context the correct group is found. Tests on the Lefthand Column are conducted in the same manner, substituting each letter by one having the same relative position to the three remaining letters of the garbled group. In the Lefthand Column the frequency of the first three letters is not consistent throughout as in the Righthand Column.

By reference to the Morse Telegraphic Code the correcting of garbled groups is often made simpler. An effort has been made in this book to avoid as many possibilities of confusion in transmission as possible. The letter H being four dots (....) is sometimes confused with P, being five dots (.....), and for this reason H has been omitted; T has been omitted for a similar reason, it sometimes being confused with L. For example, the group PNXC could, under some conditions, be confused with PNAYE, the similarity being in the Morse characters:

PNXC being ..... —. .—.. .. .
PNAYE being ..... —. .— .. ..
FBSR being .—. —... ... . ..
FBZI being .—. —... ... . ..
BCLS being —... .. . — ...
BCB being —... .. . —...

By thus placing the Morse equivalents of a garbled group on paper and comparing them with similar Morse characters the error may frequently be discovered.

N. B.

It will be noticed that the Lefthand Column series ends with the number group 40,149.

Beginning with the number group 40,200 the "Righthand Column" is carried in *two* columns on each page to the end of the book.

- 5-inch

20,000 ABAC....0
20,001 ABAD....1
20,002 ABAF....2
20,003 ABAG....3
20,004 ABAJ....4
20,005 ABAK....5
20,006 ABAM....6
20,007 ABAN....7
20,008 ABAP....8
20,009 ABAS....9
20,010 ABAV....1-horse
20,011 ABAW....1-inch
20,012 ABAX....1-mule
20,013 ABAZ....1-pound
20,014 ABBA....1-ton
20,015 ABBE....1½
20,016 ABBI....1½-ton
20,017 ABBO....1.5-inch trench mortar (s)
20,018 ABBU....2-inch
20,019 ABBY....2-pound
20,020 ABCA....2-ton
20,021 ABCO....2.24-inch
20,022 ABCU....2½-ton truck (s)
20,023 ABCY....2.95
20,024 ABDA....3-inch
20,025 ABDE....3-inch Field Gun (s)
20,026 ABDI....3-inch gun (s)
20,027 ABDO....3-inch Stokes
20,028 ABDU....3-pounder
20,029 ABDY....3-ton truck (s)
20,030 ABEB....3.2-inch
20,031 ABEF....3.2-inch Field Gun (s)
20,032 ABEG....3½-ton truck (s)
20,033 ABEJ....3.6-inch Field Gun (s)
20,034 ABEK....3.6-inch Field Mortar (s)
20,035 ABEP....3.7-inch
20,036 ABER....3.7-inch Trench Mortar (s)
20,037 ABES....4-cylinder
20,038 ABEV....4-inch
20,039 ABEW....4-inch Stokes (heavy)
20,040 ABEX....4-inch Stokes (light)
20,041 ABEZ....4-pounder
20,042 ABFA....4-ton truck (s)
20,043 ABFE....4.2-inch
20,044 ABFI....4.5-inch
20,045 ABFO....4.5-inch howitzer (s)
20,046 ABFU....4.7-inch
20,047 ABFY....4.75mm.
20,048 ABGA....5-inch
20,049 ABGE....5-inch siege gun (s)

- Abbreviate

20,050 BCFG....A
20,051 BCFK.... certain amount
20,052 BCFL.... day ('s)
20,053 BCFM.... delay (of)
20,054 BCFP.... direct hit
20,055 BCFR.... dispatch (from)
20,056 BCFS.... distance of A
20,057 BCFV.... few 34,982 JRWG
20,058 BCFW.... ... hours 45,079 RNVX
20,059 BCFX.... ... miles
20,060 BCJB.... front of
20,061 BCJF.... height of
20,062 BCJK.... large amount
20,063 BCJL.... ..... force
20,064 BCJM.... ..... number (of)
20,065 BCJP.... length of
20,066 BCJS.... little
20,067 BCJV.... mile
20,068 BCJW.... minute
20,069 BCJX.... mistake
20,070 BCKC.... misunderstanding
20,071 BCKD.... month
20,072 BCKJ.... movement
20,073 BCKL.... number (of)
20,074 BCKN.... part (of)
20,075 BCKP.... possibility (of)
20,076 BCKS.... reliable source
20,077 BCKV.... series of
20,078 BCKW.... shell
20,079 BCKX.... short distance
20,080 BCLB.... .... time
20,081 BCLC.... shortage (of)
20,082 BCLJ.... slope of
20,083 BCLK.... source (of)
20,084 BCLM.... strength of
20,085 BCLP.... surplus
20,086 BCLS.... thorough investigation
20,087 BCLV.... total (of)
20,088 BCLW.... week
20,089 BCLX.... .... ago
20,090 BCMC.... year
20,091 BCMD....Abandon (s)
20,092 BCMG..... first line
20,093 BCMJ..... the attempt
20,094 BCMK....Abandoned
20,095 BCML....Abandoning
20,096 BCMP....Abandonment
20,097 BCMS....Abate (s)
20,098 BCMV....Abated
20,099 BCMX....Abbreviate (s)

- Your base

50,300 XMBC Yard (s) short
50,301 XMBD ..... wide
50,302 XMBG (An)
50,303 XMBJ Year (s)
50,304 XMBM Yellow
50,305 XMBP ..... rocket (s)
50,306 XMBR Yes
50,307 XMBS Yesterday
50,308 XMBW ..... afternoon
50,309 XMBX ..... evening
50,310 XMCB ..... morning
50,311 XMCF Yet
50,312 XMCG Yield (s) — You
50,313 XMCJ Yielded — 25,562 DFRG
50,314 XMCM Yielding — 45,357 RVPS
50,315 XMCP You — 48,056 VSMS
50,316 XMCR ... are
50,317 XMCS ... ... assigned to
50,318 XMCW ... ... authorized
50,319 XMCX ... ... directed
50,320 XMDC ... ... informed
50,321 XMDG ... ... not
50,322 XMDJ ... ... ordered to proceed (to)
50,323 XMDM ... had
50,324 XMDP ... have
50,325 XMDR ... may
50,326 XMDS ... propose
50,327 XMDV ... should
50,328 XMDW ... . not
50,329 XMDX ... will
50,330 XMGB ... . advance
50,331 XMGF ... . arrange
50,332 XMGJ ... . be
50,333 XMGM ... . advised
50,334 XMGP ... . governed by
50,335 XMGR ... . notified
50,336 XMGS ... . relieved
50,337 XMGV ... . join
50,338 XMGW ... . report
50,339 XMGX ... . retire
50,340 XMJB ... . therefor
50,341 XMJC ... wish
50,342 XMJG Young
50,343 XMJM Y. M. C. A.
50,344 XMJP (Of the)
50,345 XMJR Younger — Your
50,346 XMJS Your — 36,081 KBJC
50,347 XMJV ..... action — 47,942 VRMF
50,348 XMJW ..... attention is invited
50,349 XMJX ..... base

50,350 XMNB Your battalion
50,351 XMNC ..... battery
50,352 XMNF ..... brigade
50,353 XMNG ..... command
50,354 XMNP ..... discretion
50,355 XMNR ..... division
50,356 XMNS ..... flank
50,357 XMNV ..... headquarters — Your
50,358 XMNW ..... infantry — 36,081 KBJC
50,359 XMNX ..... instructions — 47,942 VRMF
50,360 XMPB ..... judgment — 50,346 XMJS
50,361 XMPF ..... left
50,362 XMPG ..... letter
50,363 XMPJ ..... message
50,364 XMPM ..... number
50,365 XMPR ..... orders
50.366 XMPS ..... organization
50,367 XMPV ..... patrol (s)
50,368 XMPW ..... position
50,369 XMPX ..... recommendations desired
50,370 XMSB ..... request approved
50,371 XMSC ..... right
50,372 XMSD ..... sector
50,373 XMSG ..... telegram
50,374 XMSJ Yours
50,375 XMSM Yourself (ves)
50,376 XMSP Youth
50,377 XMSV Z.
50,378 XMSW Zeal
50,379 XMSX Zealous (ly)
50,380 XMVB Zenith
50,381 XMVC Zero
50,382 XMVG ..... hour
50,383 XMVJ Zig-zag
50,384 XMVM Zone (s)
50,385 XMVP ..... of
50,386 XMVR .... action
50,387 XMVS .... advance
50,388 XMVW .... fire
50,389 XMVX .... operations
50,390 XMXB ..... . the army (ies)
50,391 XMXC .... S. O. S.
50,392 XMXF .....
50,393 XMXG .....
50,394 XMXJ .....
50,395 XMXL .....
50,396 XMXP .....
50,397 XMXS .....
50,398 XMXV .....
50,399 XMXW .....

ENCIPHERING TABLE

AB mp	BA gw	CA pv	DA za	EB mk	FA wm	GA oj	IB yv	JA sk	KA bg	LA gv	MA xs	NA bw	OB za	PA ov	RA fk	SA zj	UB fs	VA gi	WA ju	XA wp	YB pu	ZA sj
AC on	BC as	CB ma	DB wn	ED xl	FB mc	GB dg	ID gu	JB gz	KB de	LB ij	MB ws	NB xv	OC gx	PB fd	RB gj	SB cx	UC gk	VB od	WB ve	XB nk	YC sd	ZB vf
AD lb	BD yx	CD vj	DC be	EF ny	FC gp	GC vb	IF og	JC zg	KC gf	LC dy	MC gb	NC ji	OD nv	PC wg	RC nw	SC vd	UD nj	VC px	WC or	XC gm	YD wv	ZC xm
AF ro	BE gy	CE sn	DE ag	EG je	FD wl	GD on	IG xp	JD df	KD as	LD ok	MD ap	ND wx	OF bi	PD jc	RD cm	SD rs	UF cv	VD kl	WD in	XD jb	YF jm	ZD yj
AG vl	BF ou	CF yg	DF op	EJ dx	FE ps	GE fg	IJ aj	JE rf	KG jl	LE zv	MF li	NE er	OG ev	PE nb	RE sv	SF ml	UG by	VE us	WE mu	XE wr	YG xd	ZE mo
AJ nd	BG di	CG gs	DG pa	EK pf	FG gd	GF po	IK ps	JF op	KI cb	LG wp	MG bd	NF gl	OJ xk	PF sn	RF bv	SG np	UJ pr	VF cm	WF kd	XF fn	YJ zw	ZF yk
AK gn	BI vs	CJ ed	DI kx	EP vb	FI xl	GI kr	IL ud	JG pc	KJ jw	LI jy	MI vx	NG my	OK cl	PG bp	RG sy	SI zm	UK rw	VG yw	WG fj	XG ab	YK vi	ZG ur
AM sp	BJ of	CK lr	DJ si	ER fu	FJ iv	GJ am	IM dk	JI lu	KL lw	LJ bn	MJ wu	NI ar	OL up	PI cy	RJ kc	SJ fe	UL mj	VI is	WI es	XI pm	YL fw	ZI lg
AN ex	BK pd	CL kv	DK ix	ES kg	FK so	GK ly	IN ki	JK cw	KM fy	LK fi	MK uj	NJ la	OM so	PJ xa	RK pj	SK dc	UM ac	VJ su	WJ ac	XJ lc	YM os	ZJ kj
AP un	BL nf	CM bs	DL ga	EV bm	FL sw	GL jg	IP ym	JL zk	KN gr	LM sx	ML ef	NK ol	ON kn	PK ku	RL db	SL pe	UN xo	VK jr	WK py	XK wk	YN lw	ZK pi
AR xw	BM jp	CN ul	DM le	EW ld	FM da	GM yn	IS ms	JM mx	KO fv	LO wj	MN ja	NM vy	OP ls	PL mg	RM jo	SM xg	UP dw	VL sf	WL md	XL rl	YP ms	ZL wd
AS fx	BN ka	CO fl	DN ew	EX im	FN ax	GN xe	IV bo	JO fp	KP bj	LP pl	MO ng	NO ep	OR fm	PM zx	RN fb	SN gc	UR es	VM ws	WM kb	XM yc	YR bk	ZM er
AV dr	BO lx	CP xb	DO rx	EZ ge	FO ek	GO ub	IW nx	JP vg	KR no	LR vo	MP fo	NP ij	OS jz	PN vr	RO vz	SO di	US fa	VN eb	WN ee	XN mf	YS sy	ZN xf
AW is	BP od	CR ak	DP so		FP nm	GP rk	IX fs	JR aw	KS uv	LS oo	MR zd	NR ko	OV wc	PO ds	RP os	SP rd	UV jx	VO an	WO xc	XO rs	YV vc	ZO jf
AX yp	BR vu	CS mn	DR ob		FR js	GR ik	IZ jd	JS yb	KU dv	LU ks	MS ux	NS um	OW zb	PR ig	RS uw	SH kp	UW wi	VP mb	WP lo	XP us	YW af	ZP va
AZ re	BS id	CU rj	DS br		FS vk	GS mv		JU sa	KV ox	LV av	MU bf	NU vw	OX ej	PS fr	RU ba	SU lk	UX rp	VR we	WR dj	XR wa	YX ry	ZR ys
	BU xy	CV nr	DU ro		FU dn	GU sp		JV bl	KW cs	LW ug	MV ru	NV zf	OZ rs	PU rv	RV cf	SV og	UZ oa	VS co	WS if	XS bx	YZ go	ZS du
	BV rm	CW do	DV jv		FV km	GV se		JW kw	KX pb	LX xu	MW sg	NW rn		PV xn	RW xj	SW ad		VU pn	WU rg	XU sr		ZU ns
	BW yd	CX ib	DW na		FW uc	GW eg		JX wf	KY mu	LY ce	MX ky	NX pk		PW lp	RX yl	SX ip		VW el	WV ow	XV nc		ZV yf
	BX ew	CY pg	DX zs		FX ok	GX dp		JY dz	KZ xr		MY xi	NY be		PX jk	HY il	SY wo		VX uk	WX fc	XW su		ZW or
	BY wb		DY ks		FY wy	GY ni		JZ pw			MZ lv			PY oj		SZ mw		VY iw	WY bu	XY mi		ZX sb
			DZ vm		FZ ys	GZ vn								PZ uf				VZ mr	WZ ne	XZ dm		ZY si

DECIPHERING TABLE

ab XG	ba RU	ca UZ	da FM	eb VN	fa US	ga DL	ib CX	ja MN	ka BN	la NJ	ma GB	na DW	ob DR	pa DG	ra OZ	sa JU	ub GO	va ZP	wa XR	xa PJ	yb JS	za OB
ac WJ	bc DC	cb KI	db RL	ed CJ	fb RN	gb MC	id BS	jb XD	kb WM	lb AD	mb VP	nb PE	oc LS	pb KX	rb EP	sb ZX	uc FW	vb GC	wb BY	xb CP	yc XM	zb OW
ad SW	bd MO	cd VB	dc SK	ef ML	fc WX	gc SN	if WS	jc PD	kc RJ	lc XJ	mc FB	nc XV	od BP	pc JG	rc AF	sc UM	ud IL	vc YV	wc OV	xc WO	yd BW	zc FK
af YW	be NY	ce LY	de KB	eg GW	fd PB	gd FG	ig PR	jd IZ	kd WF	ld MW	md WL	nd AJ	of BJ	pd BK	rd SP	sd YC	uf PZ	vd SC	wd ZL	xd YG	yf ZV	zd MR
ag DE	bf MU	cf RV	df JD	ej OX	fe SJ	ge EZ	ij LB	je EG	kg ES	le DM	mf XN	ne WZ	og SV	pe SL	re AZ	sf VL	ug LW	ve WB	we VR	xe GN	yg CF	ze GV
aj IJ	bg KA	cg IF	dg GB	ek FO	fg GE	gf KC	ik GR	jf ZO	ki IN	lg ZI	mg PL	nf BL	oj PY	pf EK	rf JE	sg MW	uj MK	vf ZB	wf JX	xf ZN	yj ZD	zf NV
ak OR	bi OF	cj GA	di BG	ep NO	fi LK	gi VA	il RY	jg OL	kj ZJ	li MF	mi XY	ng MO	ok FX	pg CY	rg WU	si ZY	uk VX	vg JP	wg PC	xg SM	yk ZF	zg JC
am GJ	bj XP	ck LD	dj WR	er NE	fj WG	gj RB	im EX	ji NC	kl VD	lj NP	mj UL	ni GY	ol NK	pi ZK	rj CU	sj ZA	ul GN	vi YK	wi UW	xi MY	yl RX	zi DJ
an VO	bk YR	cl OK	dk IM	es WN	fk RA	gk UC	in WD	jk PX	km FV	lk SU	mk EB	nj UD	om VF	pj RK	rk GP	sk JA	um NS	vj CD	wj LO	xj RW	ym IP	zj SA
ap MD	bl JV	cm RD	dl SO	ev OG	fl CO	gl NF	ip SX	jl KG	kn ON	lm KL	ml SF	nk XB	on GD	pk NX	rl XL	sl VW	un AP	vk FS	wk XX	xk OJ	yn GM	zk JL
ar NI	bm EV	cn AC	dm XZ	ew DN	fm OR	gm XC	is AW	jm YF	ko NR	lo WP	mn CS	nm FP	op JP	pl LP	rm BV	sm FL	up OL	vl AG	wl FD	xl FI	yp AX	zl ED
as BC	bn LJ	co VS	dn FU	ex AN	fn XF	gn AK	iv FJ	jo RM	kp SR	lp PW	mo ZE	no KR	or ZW	pm XI	rn NW	sn PF	ur ZG	vm DZ	wm FA	xm ZC	ys ZR	zm SI
av LV	bo IV	cp DP	do CW	ez UR	fo MP	go YZ	iw VY	jp BM	kr GI	lr CK	mp AB	np SG	os YM	pn VU	ro DU	so OM	us XP	vn GZ	wn DB	xn PV	yv IB	zn CE
aw JR	bp PG	cr WC	dp GX		fp JO	gp FC	ix DK	jr VK	ks LU	ls OP	mr VZ	nr CV	ov PA	po GF	rp UX	sp GU	uv KS	vo LR	wo SY	xo UN	yw VG	zo DP
ax FN	br DS	cs KW	dr AV		fr PS	gr KN	iz VI	js FR	ku PK	lu JI	ms YP	ns ZU	ow WV	pr UJ	rs SD	sr ZM	uw RS	vp LG	wp XA	xp IG	yx BD	zp AM
az KD	bs CM	cu BF	ds PO		fs IX	gs CG		ju WA	kv CL	lv MZ	mu KY	nu WE	ox KV	ps FE	ru MV	su XW	ux MS	vr PN	wr XE	xr KZ	yz FZ	zr XU
	bu WY	cv UF	du ZS		fu ER	gu ID		jv DV	kw JW	lw YN	mv GS	nv OD	oz RP	pu YB	rv PU	sv RE	uz VE	vs BI	ws MB	xs DX		zs DA
	bv RF	cw JK	dv KU		fv KO	gv LA		jw KJ	kx DI	lx BO	mw SZ	nw RC		pv CA	rw UK	sw BX		vu BR	wu MJ	xu LX		zu VJ
	bw NA	cx SB	dw UP		fw YL	gw BA		jx UV	ky MX	ly GK	mx JW	nx IW		pw JZ	rx DO	sx LM		vw MU	wv YD	xv NB		zv LE
	bx XS	cy PI	dx EJ		fx AS	gx OC		jy LI	kz DY		my NG	ny EF		px VC	ry YX	sy YS		vx MI	wx ND	xw AR		zw YJ
	by UG		dy LC		fy KM	gy BE		jz OS			mz IS			py WK	rz XO	sz WI		vy NM	wy FY	xy BU		zx PM
			dz JY		fz UB	gz JB								pz IK				vz RO	wz VM	xz MA		zy RG

Appendix 19.—MISCELLANEOUS AEF CODES

460519 O—42——15

CONTENTS OF APPENDIX 19

Appendix 19A (1).—EXTRACTS FROM FRONT LINE CODE

G. H. Q.
AMERICAN EXPEDITIONARY FORCES

Secret

FRONT LINE CODE

No. 11900

This Code Book has been issued to

for official use under his direction only

By command of General Pershing:

JAMES G. HARBORD,
Brigadier General,
Chief of Staff.

Official:
BENJ. ALVORD,
Adjutant General.

A. G. PRINTING OFFICE
1918

INSTRUCTIONS
FOR THE USE OF THE CODE.

This book is to be used, in connection with secret instructions, in sending messages to and from the front line trenches.

A code group is provided for each word or phrase.

A number of commonly used prefixes and suffixes will be found arranged in alphabetical order.

To code a message substitute for the word or phrase to be sent the group corresponding to it. *Under no circumstances* should a word be sent "in plain" in a code message. Time should be taken to spell the word in code. Never repeat any code message in clear or in any other code or cipher.

The loss of a code book should be reported at once by number through military channels to G. H. Q. A. E. F.

Destroy by burning at once all scraps of paper on which coding or decoding memoranda have been made.

You will inform the appropriate subordinate where you carry this code, and instruct him as to his conduct in the event that you become a casualty.

THIS CODE MUST NOT FALL INTO THE HANDS OF THE ENEMY.

AB..... 0
AC..... 1
AD..... 2
AF..... 3
AG..... 4
AH..... 5
AI..... 6
AK..... 7
AL..... 8
AM..... 9
AN..... A (an)
AO..... Abandon (ed)
AP..... Able
AR..... About
AS..... Action (s)
AT..... Activity (ies)
AU..... Advance (d)
AV..... Aeroplane (s)
AW..... After
AY..... All
AZ..... (This group means nothing)
BA..... All right
BC..... Am (A. M.)
BD..... Ammunition
BE..... Ammunition automatic rifle
BF..... Ammunition caliber .30
BG..... Ammunition M. G. in strips
BH..... And
BI..... Answer
BK..... Any
BL..... Are
BM..... Arrive (d)
BN..... Artillery
BO..... Assist (ed)
BP..... Assistance
BR..... At
BS..... At once
BT..... Attack (s)
BU..... Automatic (s)
BV..... Automatic rifle ammunition
BW..... B
BY..... Back
BZ..... Bad
CA..... Balloon (s)
CB..... Barbed wire
CD..... Barrage
CE..... Battalion (s)
CF..... Battery
CG..... Be
CH..... Been

WT.....Wind favorable for cloud gas attack
WU.... Wire (s)
WV.... Wire entanglements
WY.....With
WZ.....Withdraw (ing)
YA..... Withdrawn
YB..... Work (ing)
YC..... Working party (ies)
YD..... Wounded
YE..... X
YF.....Y
YG..... Yard (s)
YH..... Yes
YI..... Yesterday
YK..... Yet
YL.....You
YM..... You will be relieved (at)
YN..... Your
YO..... Your men
YP.....Your position
YR..... Your sector
YS.....Z
YT.....Zero
YU..... Zero hour
YV..... Zero hour has been postponed
YW.....
YZ.....
ZA.....
ZB.....
ZC.....
ZD.....
ZE.....
ZF.....
ZG.....
ZH.....
ZI.....
ZK.....
ZL.....
ZM.....
ZN.....
ZO.....
ZP.....
ZR.....
ZS.....
ZT.....
ZU.....
ZV.....
ZW.....
ZY.....
ZZ.....

Appendix 19A (2).—SAMPLE OF ENCIPHERING CARD FOR FRONT LINE CODE

SECRET

31-a

THIS TABLE MUST NOT FALL INTO THE HANDS OF THE ENEMY.

1. If destroyed to prevent capture, report will be made to the office to which its return is ordered.

2. This table will be used from 3 a. m..... until further notice.

ENCIPHER

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	U	V	W	Y	Z
o	i	z	n	t	p	w	s	h	g	u	l	f	m	d	c	a	y	b	e	v	r	k

DECIPHER

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	r	s	t	u	v	w	y	z
S	U	R	P	V	N	K	I	B	Z	M	O	D	A	F	Y	H	E	L	W	G	T	C

Appendix 19B.—GHQ, AEF, BULLETIN No. 46

G. H. Q.
AMERICAN EXPEDITIONARY FORCES,

BULLETIN No. 46. FRANCE, *July 12, 1918.*

In order to shorten telegraphic reports of casualties as required by G. O. No. 40, c. s., these headquarters, as amended by G. O. No. 77, c. s., these headquarters, the following three letter words are prescribed for use as code equivalents for the phrases shown. These code equivalents will be used in the preparation of all casualty reports throughout the A. E. F.

Report following accidentally killed	AWL
Report following killed in action	BOX
Report following died of wounds	COW
Report following died of disease	DAY
Report following missing in action	END
Report following severely wounded	FEW
Report following slightly wounded	GAS
Drowned, body recovered	INK
Drowned, body not recovered	JAR
Death in line of duty	KIT
Death not in line of duty	LEG
Result of own misconduct	MOP
Not result of own misconduct	NAG
All in line of duty, not result of own misconduct	OAK
All entitled to wound chevron	PUN
Not entitled to wound chevron	RAM

BY COMMAND OF GENERAL PERSHING:

JAMES W. McANDREW,
Chief of Staff.

OFFICIAL:
ROBERT C. DAVIS,
Adjutant General.

A. G. PRINTING DEPT., G. H. Q. A. E. F., 1918.

Appendix 19C.—G. S., 82ND DIVISION, AEF, MEMORANDUM NO. 66

SECRET

COPY NO. 22

DLM

Hq. 82nd Division, American E. F., G-3

France, 24, June 1918.

SECRET.

G. S. MEMORANDUM NO. 66.

1. This list of code names becomes effective at 9:00 o'clock 28, June 1918. All previous code lists that conflict with this one are hereby rescinded. Until that time lists found in the Sector will be used.

2. This code alone will be used in calling up parties on the telephone. Names of towns or individuals will not be given under any circumstances.

3.

TOWNS	CODE NAMES
Andilly	Chattanooga
Ansauville	Bull Run
Beaumont	New Orleans
Bernecourt	Poirel
Bouconville	Gettysburg
Boucq	San Francisco
Bouvron	Boulogne (Bu-lone)
Cornieville	Manila
Domevre	Dunkerque (Dun-kirk)
Flirey	Vicksburg
Grosrouvres	Great Heck
Hamonville	Appomattox
Jouy	Cold Harbor
Lagney	Wilderness
Lironville	Loudeac (Lu-di-ack)
Limey	Jean d'Arc
Lucey	Santiago
Mandres	Little Horn
Menil-la-Tour	Quebec
Minorville	Marceau
Manoncourt	Meaux (Mo)
Manonville	Mortier
Noviant	Ney
Rambucourt	Tippecanoe
Remenauville	Reims (Rans)
Raulecourt	Ramel
Regnieville	Rouen (Ru-ong)
Royaumeix	Rostock
St. Jacques	Saumur (So-mur)
Sansey	Illinois
Seicheprey	Colorado
Xivray	Texas
Gerard	Utah

SECTOR TELEPHONE CENTRALS

360.6-225.2	Waterloo
358.5 -223.9	Antietam
359.95 -232.15	Horner

ARTILLERY CENTRALS

TOWNS	CODE NAMES
Ansauville	Give Oaks
Ancilly	Anthill
Rambucourt	Delaware
Sanzey	Illinois
Mandres	Lundy's Lane
Maudres	Agua Prieta
Hannonville	Monterey
Bruey	O. P. 23
Bernecourt	Poirel
Berrecourt	Rain-in-the-Face

CO-ORDINATES

355.5 -225.5 ..... Spotsylvania

NAME	CODE	TOWN	PHONE
General Burnham	Eagle	Santiago ..	38
Chief of Staff	Oriole	Santiago ..	39
General Cronin	Sea Gull	Waterloo ..	
163 Inf.Brig.Hq. ...	Albatross ...	Waterloo ..	
General Lindsey ...	King Fisher .	Cold Harbor	
164 Inf.Brig. Hq. ..	Jay Bird	Cold Harbor	
General Rhodes	Hornet	Santiago ...	5 A
157 F.A.Brig.Hq. ...	Bumble Bee ..	Santiago ...	7 A
Colonel Whitman	Mocking Bird		
Colonel McArthur ...	Stormy Petrel		
Colonel Ely	Jack Snipe		
Colonel Nelson	Whip-poor-Will		
Colonel Williams ...	Rattle-snake		
Colonel Deems	Copper Head		
Colonel Pearce	Bull Snake		

NAME	TOWN	PHONE
ADMINISTRATION G-1) Major Maddox)	..... Santiago	37
INTELLIGENCE G-2) Lt. Col. Lee)	..... Santiago	35
OPERATIONS G-3) Major Wainwright)	..... Santiago	36
ADJUTANT'S OFFICE) Major Boyd) Capt. Kaefring)	..... Santiago	33
DIVISION SURGEON) Lt. Col. Koerper)	..... Santiago	32
DIV'N SIGNAL OFFICE) Lt. Col. Hemphill)	..... Santiago	28

ORGANIZATION	CODE NAME	TOWN
Hdqrs. 325th Infantry ...	Blackbird	
1st Battalion ...	Pigeon	
2nd Battalion ...	Kito	
3rd Battalion ...	Bulfinch	
Hdqrs. 326th Infantry ...	Red Bird	
1st Battalion ...	Buzzard	
2nd Battalion ...	Rail	
3rd Battalion ...	Sparrow	
Hdqrs. 327th Infantry ...	Humming Bird	
1st Battalion ...	Wood Pecker	
2nd Battalion ...	Meadow Lark	
3rd Battalion ...	Swallow	
Hdqrs. 328th Infantry ...	Blue Bird	
1st Battalion ...	Pheasant	
2nd Battalion ...	Grouse	
3rd Battalion ...	Partridge	
319th Machine Gun Bn. ...	Roanoke	
320th Machine Gun Bn. ...	Tecumseh	
321st Machine Gun Bn. ...	Oceola	
307th Trench Mortar Btry.	Rain-in-the-Face	
307th Field Signal Bn. ..	Wild Bear	Santiago 2
157th F.A.Brigade Hq. ...	Bumble Bee	
319th F.A. Hq.	Red Snapper	Poirel
1st Battalion	Salmon	
2nd Battalion	Bass	
320th F.A. Hq.	Cherry Blossom-.....	Bull Run
1st Battalion	Lily	
2nd Battalion	Pansy	
321st F.A. Hq.	Sullivan	Santiago
1st Battalion	Kilrain	
2nd Battalion	Corbett	
3rd Battalion	Ketchell	
307th Engineers	Alligator	Santiago
1st Battalion	Crocodile	
2nd Battalion	Turtle	
325th Field Hospital	Polecat	Podunk
326th Field Hospital	Mole	Quebec
327th Field Hospital	Weasel	Podunk
328th Field Hospital	Chipmunk	Podunk
325th Ambulance Co.	Caterpillar	Podunk
326th Ambulance Co.	Scorpion	Quebec
327th Ambulance Co.....	Tarantula	Arizona
328th Ambulance Co.	Centipede	Quebec

4. The listening in sets have disclosed the fact that indiscreet and damaging conversations have been carried on over the telephone. The enemy is able to pick up these conversations by means of the "listening in" sets. The possible results are obvious.

5. This order is SECRET. Each copy will be signed for and will be required to be turned in upon the issue of a new one. No other copies of this Code must be made.

6. This sector is infested with enemy spies and sympathizers. They tap telephone lines, signal to the enemy, and are responsible for many losses.

7. The Signal Officers of Infantry and Artillery Organizations will listen in on their switchboards with a view to checking indiscreet and improper conversations. They are authorized to terminate any conversation that might give information to the enemy, and in such cases immediate report of the circumstances will be made to the Division Signal Officer.

BY COMMAND OF MAJOR GENERAL BURNHAM:

R. E. Beebe,

Lieut. Col., General Staff,
Chief of Staff.

G-3
6/29/18

Appendix 19D.—EXTRACTS FROM AMERICAN RADIO SERVICE CODE No. 1

SECRET

MUST NOT FALL INTO ENEMY'S HANDS

American Radio Service Code No. 1

(For the exclusive use of the Radio personnel.)

This book has been issued to

for official use of Radio Station located at

Precede every message in this code by "RAD"

NOT TO BE TAKEN IN FRONT OF BRIGADE HEADQUARTERS

AMERICAN RADIO SERVICE CODE NO. 1

(IT IS POSITIVELY FORBIDDEN TO MAKE COPIES OF THIS CODE.)

1. This code book, to be known as "The American Radio Service Code No. 1," is issued to all continuous wave radio stations down to and including brigades, and to all artillery units equipped with continuous wave radio. It is to be used for all radio service messages for which no special abbreviations are provided.

2. Absolutely nothing will be transmitted "in clear."

3. Avoid the use of words not in code book when other words of the same significance are provided in the code. Words spelled out, letter by letter, not only take time to code, transmit and decode, but they are one of the favorite points of attack by enemy code men.

4. Coded and decoded copies of messages must never be filed together. All notes and memoranda used in coding or decoding messages must always be destroyed by burning, if practicable.

5. Messages must be short. Several short messages will be less likely to be read by the enemy than one long one.

Except in emergency a long message, if it must be sent, will be divided into two or more parts and each sent as a complete message.

Very often the best way to handle a long message is to leave out unnecessary words.

6. Addresses will not be used when context of message indicates for whom intended When used, they must be in code.

7. Signature should be sent only when absolutely required. When sent, they must be encoded, letter by letter, if necessary.

8. Blank spaces are for the designation of organizations and local geographical points, or for such other use as may be desired, and these designations will be furnished by higher authority.

9. Suggestions for the improvement of this code book are desired.
These should include such points as:

(1) Unnecessary words.
(2) Necessary words which have been omitted. (It is not considered practicable to enlarge this book. Therefore, for each word or phrase to be added a word or phrase to be taken out should be indicated.)
(3) Relative merits of letters and figures in code groups.
(4) Form of books.
(5) Arrangement of contents.
(6) Size and style of type used.
(7) Any other suggestions having for its object the making of future editions more convenient for use at the front.

Suggestions should be addressed:

"Radio Officer of the Army."

10. The first group in every message will be "RAD," which group will be counted as one word in the check.

11. For convenience a list of "Conventional Abbreviations" has been printed in the back of the book.

12. IN CASE THIS CODE BOOK IS LOST OR OPEN TO SUSPICION THE FACTS WILL BE REPORTED IMMEDIATELY TO THE RADIO OFFICER OF THE ARMY DIRECT.

BY COMMAND OF GENERAL PERSHING:

JAMES W. McANDREW,
Chief of Staff.

OFFICIAL:
ROBERT C. DAVIS,
Adjutant General.

TABLE OF ENCODING

PHRASES USED IN TRANSMISSION:

304...Antenna was damaged
450...I am obliged to stop sending until ..... o'clock
367...I have been calling you since ..... o'clock
513...I have increased my radiation
584...It is forbidden to transmit until .....
024...Send faster
169...Send slower
242...Stop sending. You are interfering
312...Transmitting set was damaged
669...Wait few minutes; am changing batteries
739...Was obliged to stop sending until ..... o'clock
814...Will call you at ..... o'clock
745...Your sending is bad
957.....
461.....
182.....
109.....
036.....
086.....

ADJUSTMENTS:

292...Are you sure your accumulators are well charged?
219...Are you sure your accumulators are well insulated?
436...Decrease your wave length ..... meters
524...Examine your radiated wave length
674...Examine your transmitting set
590...I am working on following wave length
946...Increase your wave length ..... meters
754...My radiation is good
822...Send V for two minutes
442...Take wave length of ..... meters
301...What wave length are you working on?
018...When will you require additional accumulators?
319...Your wave length is correct
468...Your wave length is not correct
542.....
536.....
679.....
690.....
328.....
255.....

RULES FOR USING RADIO SERVICE CODE

This service code is intended to be used for communication between radio operators, chiefs of posts and officers of the radio service of the Army and subordinate units. It may also be used for practice telegrams.

It is divided into two principal parts.

The first part, called the "Table of Encoding", is divided into:

(1) Usual phrases relative to incidents of transmission.

(2) Usual phrases relative to adjustments of the station.

(3) Usual phrases relative to working in the net.

(4) Miscellaneous phrases.

(5) Phrases descriptive of radio apparatus.

(6) A list of technical terms, words, and syllables used for composing words not listed in their entirety.

Before each word or phrase is a group of three figures which is the code combination representing the words or phrase after it.

The second part, called "Table of Decoding," contains the three-figure groups arranged in numerical order and after each is the word or phrase which they represent.

Simple Coding:

Each phrase or word is coded by using the three-figure group corresponding to it. Example:

"Your wave length is correct,"
(319)

To encode a word not found in this code the syllables shown in the code will be used as in the following example:

"Bad-ly damage-d"
(642) (742) (860) (724)

Simple Decoding:

The three-figure code groups are arranged in the Decoding Section in regular sequence, beginning with 001 and ending with 999.

In decoding a message, the operator looks for each group and writes down the words or phrase appearing thereafter. For example:

(319) equals: "Your wave length is correct."
(642) (742) (860) (724) equals: "Badly damaged."

—A—

948...A
216...able
430...about
506...above
299...ac
321...accident
459...acid
102...accord
010...account
151...accumulator
727...accur
972...acknowledge
684...act
463...action
334...ad
269...add
094...address
992...Adjutant
780...adjust
563...advis
489...aerial
337...aerienne
549...aero
613...aeronautic
677...again
043...age
178...agree
247...aid
033...air
457...al
528...alert
665...all
001...alone
762...along
486...already
276...also
208...alter
067...alternator
493...altogether
638...always
773...am
475...ambulance
987...American
837...ammeter
571...ampere
852...amplifier
835...an
394...and
040...angle
160...answer
244...antenna
922...antenna inductance
710...anti
845...any
280...apparatus
062...approv
266...approximate
422...April
123...ar
399...arc
259...are
478...armature
622...army
904...Army Corps
829...arrival
595...artillery
453...ary
375...as
185...at
332...ate
699...ation
910...ator
843...attack
420...au
056...Audion bulb
205...August
470...automobile
129...average
210...aviation

—B—

426...B
642...bad
704...bag
908...balloon
994...bandages
545...base
325...battalion
180...battery
467...Baume
607...be
962...bearings
824...been
052...before
636...Belgian
387...better
237...between
887...bi
602...bicycle
958...big
738...binding
412...bis
355...blanket
137...blank
069...blouse
714...bo
916...bombard
768...bomb-carrier
812...bond
575...book
532...boots
392...box
252...breeches
113...bridge
406...bridage
378...British
735...broken
878...bu
610...but
777...buzzer
920...by

—C—

345...C
203...cable
465...call
687...call letter
906...can
706...cancel
060...cannot
625...capacity
786...captain
498...car
999...carbur
792...case
572...cavalry
646...ce
439...cell
967...cent
795...central
444...ch
363...charge
136...charging plant
433...chart
153...chief
088...Chief Signal Officer
229...choice
027...ci
382...cigarette
448...cipher
587...circuit

TABLE OF DECODING

001...alone
002...oil
003...ies
004...infantry
005...officer
006...except
007...code
008...fault
009...ing
010...account
011...grouping
012...cr
013...kilo
014...fly
015...ground
016...receiving station
017...those [cumulators?
018...When will you require additional ac-
019...fuse
020...Thursday
021...cylinder
022...dispatch book
023...heliograph
024...Send faster
025...line
026...messenger
027...ci
028...T.P.S.
029.....
030...demand
031...eighty (80)
032...enough
033...air
034...how
035...net
036.....
037...miss
038...compensator
039...note
040...angle
041...J
042...third
043...age
044...panel
045...enemy
046...park
047...today [station and personnel
048...You will report with your complete
049...gener
050...safe
051...up
052...before
053...map
054...sergeant
055...good
056...Audion bulb
057...Can you relay a telegram to...
058...weather
059...understood
060...cannot
061...major
062...approv
063...service regulations
064...accumulators, 4-volt
065...must
066...system
067...alternator
068...twenty (20)
069...blouse
070...plan
071...You are being called by
072...I am re-entering net
073...yes
074...German
075...X
076...Your
077...during
078...receiver
079...slow
080...will
081...accumulators, 6-volt
082...radio-gonio
083...drawers
084...wavelength
085...director
086.....
087...wrong
088...Chief Signal Officer
089...Master Signal Electrician
090...fourth
091...indispensable
092...list
093...station
094...address
095...undamped
096...decimal
097...radiat
098...continu
099...pursuit
100...meteorological bulletin

Appendix 19E.—CODE FOR DESIGNATION ORGANIZATIONS, COMMANDERS AND STAFF OFFICERS

SECRET

No 93

For Official Use of Officers to Whom Entrusted

CODE FOR DESIGNATION ORGANIZATIONS, COMMANDERS AND STAFF OFFICERS.

1. This code will be used when it is necessary to conceal the true designation of organizations, commanders and staff officers in letters, telegrams or telephone conversation.
2. An organization is designated by a single christian name. Example: 33rd Division—"MARIAN."
3. A commander is designated by two names. Example: C. G., 33rd Division—"MARIAN SNOW."
4. A staff officer is designated in the same way by two names.
5. THIS CODE MUST NOT BE USED FOR TELEGRAPHIC ADDRESSES OR TELEPHONE CALLS. (The operators are not furnished with the code.)

ORGANIZATIONS.

G. H. Q.	Ida
1st Army	Bertha
2nd Army	Dolly
3rd Army	Kate
4th Army	Vera
5th Army	Maude
6th Army	Alma
7th Army	Kitty
8th Army	Florence
1st Corps	Agnes
2nd Corps	Grace
3rd Corps	Winifred
4th Corps	Ruth
5th Corps	Daisy
6th Corps	Carrie
7th Corps	Violet
8th Corps	Gabriella
9th Corps	Alice
10th Corps	Helen
11th Corps	Wilhelmina
12th Corps	Peggy
13th Corps	Ursula
14th Corps	Clara
15th Corps	Gladys
16th Corps	Anna
1st Division	Della
2nd Division	Joan
3rd Division	Frances
4th Division	Olive
5th Division	Sadie
6th Division	Maggie
7th Division	Tilly
8th Division	Irene
9th Division	Blanche
10th Division	Julia
11th Division	Laura
12th Division	Effie
13th Division	Claire
14th Division	Lois
15th Division	Irma
16th Division	Victoria
17th Division	Tina
18th Division	Agatha
19th Division	Hazel
20th Division	Jane
21st Division	Dot
22nd Division	Lydia
23rd Division	Sarah
24th Division	Molly
25th Division	Pearl
26th Division	Theresa
27th Division	Rachel
28th Division	Jennie
29th Division	Elsie
30th Division	Eva
31st Division	Kathryn
32nd Division	Nell
33rd Division	Marian
34th Division	Sylvia
35th Division	Rose
36th Division	Georgia
37th Division	Letty
38th Division	Jessie
39th Division	Mary
40th Division	Ellen
41st Division	Stella
42nd Division	Mabel
43rd Division	Virginia
44th Division	Mildred
45th Division	Belle
46th Division	Gwendolyn
47th Division	Leona
48th Division	Enid
49th Division	Martha
50th Division	Prudence
76th Division	Beatrice
77th Division	Imogen
78th Division	Margaret
79th Division	Priscilla
80th Division	Nora
81st Division	Alexandra
82nd Division	Caroline
83rd Division	Genevieve
84th Division	Iris
85th Division	Lucille
86th Division	Naomi
87th Division	Rebecca
88th Division	Betty
89th Division	Rhoda
90th Division	Hortense
91st Division	Cornelia
92nd Division	Fanny
93rd Division	Bessie
94th Division	Edith
95th Division	Rosalind
96th Division	Theodora
97th Division	Christine
98th Division	Eloise
99th Division	Ernestine
100th Division	Constance
101st Division	Dorothy
102nd Division	Jocelyn
103rd Division	Drusilla
104th Division	Evangeline
105th Division	Lucy
106th Division	Zora
107th Division	Clemantine
108th Division	Yetta
109th Division	Yvonne
110th Division	Emelia
111th Division	Ray
112th Division	Susan
113th Division	Ethel
114th Division	Edna
115th Division	Marcia
116th Division	Sybil
117th Division	Beulah
118th Division	Eliza
119th Division	Harriet
120th Division	Louise
121st Division	Jerusha
122nd Division	Miranda
123rd Division	Pauline
124th Division	Emma
125th Division	Audrey
H. Q. S. O. S.	Zenobia
A. S. S. O. S.	Tilda
I. S. S. O. S.	Carmen
Base Sec. No. 1	Barbara
Base Sec. No. 2	Josephine
Base Sec. No. 3	Elizabeth
Base Sec. No. 4	Charlotte
Base Sec. No. 5	Henrietta
Base Sec. No. 6	Annabelle
Base Sec. No. 7	Mattie

TITLES OF OFFICERS.

C.-in-C. or C. G	Snow
C. of S	Dow
Deputy C. of S	Jones
A. C. of S. G-1	Fuller
A. C. of S. G-2	King
A. C. of S. G-3	Burns
A. C. of S. G-4	Wells
A. C. of S. G-5	Kelly
Chief of Cavalry	Wise
Chief of Infantry	Rush
Chief of Artillery	White
Chief of T. C	Dick
A. G	Long
I. G	Smith
J. A	Black
C. Q. M	Adams
C. S	Greene
C. E. O	Brown
C. O. O	Pratt
C. S. O	Hart
C. A. S	Fry
C. C. W. S	Brady
P. M. G. or P. M	Page
Chief of M. T. C	Hand
D. G. T	Silver

SECRET

ORGANIZATIONS.

Agatha.....18th Division
Agnes.....1st Corps
Alexandra.....81st Division
Alice.....9th Corps
Alma.....6th Army
Anna.....16th Corps
Annabelle.....Base Section No. 6.
Audrey.....125th Division
Barbara.....Base Section No. 1.
Beatrice.....76th Division
Belle.....45th Division
Bertha.....1st Army
Bessie.....93rd Division
Betty.....88th Division
Beulah.....117th Division
Blanche.....9th Division
Carmen.....Int. Sec. S. O. S.
Caroline.....82nd Division
Carrie.....6th Corps
Charlotte.....Base Section No. 4.
Christine.....97th Division
Claire.....13th Division
Clara.....14th Corps
Clemantine.....107th Division
Constance.....100th Division
Cornelia.....91st Division
Daisy.....5th Corps
Della.....1st Division
Dolly.....2nd Army
Dorothy.....101st Division
Dot.....21st Division
Drusilla.....103rd Division
Edith.....94th Division
Edna.....114th Division
Effie.....12th Division
Eliza.....118th Division
Elizabeth.....Base Section No. 3.
Ellen.....40th Division
Eloise.....98th Division
Elsie.....29th Division
Emelia.....110th Division
Emma.....124th Division
Enid.....48th Division
Ernestine.....99th Division
Ethel.....113th Division
Eva.....30th Division
Evangeline.....104th Division
Fanny.....92nd Division
Florence.....8th Army
Frances.....3rd Division
Gabriella.....8th Corps
Genevieve.....83rd Division
Georgia.....36th Division
Gladys.....15th Corps
Grace.....2nd Corps
Gwendolyn.....46th Division
Harriet.....119th Division
Hazel.....19th Division
Helen.....10th Corps
Henrietta.....Base Section No. 5.
Hortense.....90th Division
Ida.....G. H. Q.
Imogen.....77th Division
Irene.....8th Division
Iris.....84th Division
Irma.....15th Division
Jane.....20th Division
Jennie.....28th Division
Jerusha.....121st Division
Jessie.....38th Division
Joan.....2nd Division
Jocelyn.....102nd Division
Josephine.....Base Section No. 2.
Julia.....10th Division
Kate.....3rd Army
Kathryn.....31st Division
Kitty.....7th Army
Laura.....11th Division
Leona.....47th Division
Letty.....37th Division
Lois.....14th Division
Louise.....120th Division
Lucille.....85th Division
Lucy.....105th Division
Lydia.....22nd Division
Mabel.....42nd Division
Maggie.....6th Division
Marcia.....115th Division
Margaret.....78th Division
Marian.....33rd Division
Martha.....49th Division
Mary.....39th Division
Mattie.....Base Section No. 7.
Maude.....5th Army
Miranda.....122nd Division
Mildred.....44th Division
Molly.....24th Division
Naomi.....86th Division
Nell.....32nd Division
Nora.....80th Division
Olive.....4th Division
Pauline.....123rd Division
Pearl.....25th Division
Peggy.....12th Corps
Priscilla.....79th Division
Prudence.....50th Division
Rachel.....27th Division
Ray.....111th Division
Rebecca.....87th Division
Rhoda.....89th Division
Rosalind.....95th Division
Rose.....35th Division
Ruth.....4th Corps
Sadie.....5th Division
Sarah.....23rd Division
Stella.....41st Division
Susan.....112th Division
Sybil.....116th Division
Sylvia.....34th Division
Theodora.....96th Division
Theresa.....26th Division
Tilda.....Adv. Sec. S. O. S.
Tilly.....7th Division
Tina.....17th Division
Ursula.....13th Corps
Vera.....4th Army
Victoria.....16th Division
Violet.....7th Corps
Virginia.....43rd Division
Wilhelmina.....11th Corps
Winifred.....3rd Corps
Yetta.....108th Division
Yvonne.....109th Division
Zenobia.....Headquarters S. O. S.
Zora.....106th Division

TITLES OF OFFICERS.

Adams.....Chief Quartermaster
Black.....Judge Advocate
Brady.....Chief Chemical Warfare Service
Brown.....Chief Engineer Officer
Burns.....Assistant Chief of Staff G-3
Dick.....Chief of Tank Corps
Dow.....Chief of Staff
Fry.....Chief of Air Service
Fuller.....Assistant Chief of Staff G-1
Greene.....Chief Surgeon
Hand.....Chief of Motor Transport Corps
Hart.....Chief Signal Officer
Jones.....Deputy Chief of Staff
Kelly.....Assistant Chief of Staff G-5
King.....Assistant Chief of Staff G-2
Long.....Adjutant General
Page.....Provost Marshal General or Provost Marshal
Pratt.....Chief Ordnance Officer
Rush.....Chief of Infantry
Silver.....Director General of Transportation
Smith.....Inspector General
Snow.....Commander-in-Chief or Commanding General
Wells.....Assistant Chief of Staff G-4
White.....Chief of Artillery
Wise.....Chief of Cavalry

Appendix 19F.—PAMPHLET "TELEPHONE—T. P. S.—T. S. F.—VISUAL"

PAMPHLET

SECRET

TELEPHONE -T. P. S. - T. S. F. -VISUAL

No. 578

Name of Pamphlet: OLIVE
Code Name: Q Q Q

It is forbidden to send any message in the clear by T.S.F. or T.P.S.

BURN THIS PAMPHLET IF IT IS IN DANGER OF BEING CAPTURED

AIC	A	CMT	my	EQA	to bombard	NBT	meter
AKE	A	CMV	our	EQR	to cease	NCI	minute
AKI	B	CMX	our	EQS	to begin	NCK	little, weak
ALB	B	CMZ	we	ERC	to complete		
ALD	C	CNK	by	EST	to lead		ORIENTATION
ALG	C	CNN	for	ESL	to keep		
ANO	D	DAR	your	[illegible]	to keep on	NCV	to the right
AUP	D	DBD	you	ESS	to outflank	NDE	to the left
ANS	E			ETE	to emerge	NDK	at end, rear
APG	E		Numbers	ETG	to decide	NDO	at the head
ARS	E			ETK	to defend	NDR	going to
BIC	F	DCD	0 or nul	EUI	to demand	NEG	in centre
BKT	F	DCG	1 or first	EUV	to destroy	NEK	back
BLN	G	DCK	2	FAR	to direct	NES	before, in front of
BLR	H	DCO	3	FAT	to fail	NFT	direction of
BNO	I	DCS	4	FAZ	to hear	NGA	east
BNS	I	DCV	5	FCZ	to send	NGK	north
BOA	J	DDE	6	FDV	to be	NGN	west
BOG	K	DDK	8	FEI	to evacuate	NKV	south
BOI	L	EAR	9	FET	to do	NKX	coming from
BOS	M	EAZ	10	[illegible]	to advise		
BPC	M	EBI	11	FIN	guide		
BPD	N	EBR	12	FKA	leave		LOCATION
BPG	N	EDZ	13	FKR	miss or lack		
BPQ	O	ECA	14	FKT	put	NKZ	felling, abatis
BPR	P	ECF	15	GAI	occupy	NLH	shelter
BPS	Q	ECK	16	GAS	oppose	NLR	wood
BQA	R	ECR	17	GAT	command	NLT	communication trenches
BSC	R	ECT	18	GDA	organize	NOB	drain
BSQ	S	EDR	19	GBO	appear	NOK	cross road
BSS	S	EDZ	20	GBV	place	NOV	quarry
CAR	T	EEI	30	GCI	prepare	NRF	strong point
CAZ	T	EEM	40	GCR	receive	NRR	grave yard
CBI	U	EET	50	GCT	reduce	NSC	hill
CBL	V	EFG	60			NSE	crest
CBN	W	EFI	70	GCV	come in	OAR	church
CCY	X	EFT	80	[illegible]	answer		
CDB	Y	EGL	90	GEA	repulse		

PDL	trench mortar	QEV	field cable	SGK	visual station
PDO	tanks	QFI	light cable	SGS	prisoner
PDP	allied artillery will open fire on	QFS	captain	SHO	regiment
		QFV	cartridge 86	SHP	relief
PEI	allied artillery is shelling	QFY	cartridge D A M	SHQ	answer
		QGE	head receiver	SHS	not
PEK	allied artillery has ceased firing on	QGH	cavalry	SII	reserve
		QHC	certainly	SID	14 c/m searchlight
PET	enemy artillery will open fire on	QHI	tanks	SIP	24 c/m searchlight
		QKE	colonel	SKO	situation
PFI	enemy artillery is shelling	QKG	battle	SKV	evening
		QKP	Major	SLY	non-comm.officer
PFK	enemy artillery has ceased firing on	QLE	counter attack	SLZ	4 line switchbrd
		QLO	army corps	SMI	12 line swthbrd
PFT	battery	QLY	raid	SND	torpedo
PFZ	bombardment	QNI	critic	SMT	troop
PGA	bombardment by gas shell	QNK	defense	SMY	vacuum bulbs
		QMN	material damages	SNF	killed
PGE	Casemate	QMT	demain, tomorrow	SNG	urgent
PGK	cease fire	QMZ	request	SNL	supplies
PHI	anti-air craft	QOB	missing		
PHT	anti tank	QOH	available		
PHZ	time fuse	QOK	distance		
PKD	percussion fuse	QOR	division		
PKT	instantaneous	QOV	doubtful		
PLE	observe fire on	QPE	water		
PLG	gas shell	QPK	enemy		
PLL	lacrymatory shell	QPN	squadron		
PME	shrapnel shell	QPP	execution		
PNF	melinite shell	QQA	general		
PNA	piece	QQF	engineers		
PND	range too short	QRB	non-commissioned officer		
PNK	range too long				
PNL	range too far to the right	QRD	wire mesh strips		
		QRE	group		
PNT	range too far to the left	QRH	guide		
		QRT	yesterday		
POO	barrage on	QSA	man		
POS	counter preparation range	QSS	at once		
		QST	impossible		

PHRASES

SNV	everybody under shelter except the guard	VBB	the patrol is back
		VBD	the patrol is out
SOP	alarm	VKK	the patrol will go out at once
SOV	gas alarm	VKS	do complete the chain of the runners
TAR	attack under previous condition	VSE	first line pass by
TAT	enemy attack seems to have failed	V3K	the artillery preparation seems to be sufficient
TAV	attack is started		

Appendix 19G.—TEMPORARY CODE FOR TRANSMISSION OF CASUALTY DATA BY TELEPHONE AND TELEGRAPH

COPY.inp PH G-3

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY FORCES

SECRET: THIRD SECTION G.S.

16 September, 1918

MEMORANDUM

1. The accompanying Temporary Code for Reporting Casualties (Copy No. 35) is furnished to your for use in rendering telephonic or telographic reports involving the mention of casualties.

2. Its use is necessary because of the strong objections made by the French to reporting casualties in plain text.

3. This code will be used until further orders by all concerned in reporting casualties by telephone or telegraph to Corps Headquarters or to G-2 or G-3 G.H.Q.

4. Please acknowledge receipt of attached code by number.

By direction:

W. B. HOWE
Captain, Infantry
Secretary G-3.

1 encl.
jem

SECRET COPY No. 35.

TEMPORARY CODE FOR TRANSMISSION OF CASUALTY DATA BY TELEPHONE & TELEGRAPH.

Plain Text:	Code:
Casualty report, officers	Following required
Casualty report, soldiers	Following estimated
No casualties, officers	Nothing required
No casualties, soldiers	Nothing estimated

Character of casualty (report in order given)

Plain text:	Code:	Plain text:	Code:
Killed	January	Slightly gassed	July
Wounded	February	Taken prisoner	August
Seriously wounded	March	Wounded and prisoner	September
Slightly wounded	April	Wounded by shell fire	October
Gassed	May	Wounded by accident	November
Seriously gassed	June	Missing	December

Table for numbers (1 to 999):

HUNDREDS:	TENS:	UNITS:
0	Caps	Bacon 0
1 Oil	Shoes	Rice 1
2 Ink	Belts	Beef 2
3 Paper	Gloves	Flour 3
4 Chairs	Socks	Pork 4
5 Tables	Coats	Salt 5
6 Candles	Shirts	Ham 6
7 Lanterns	Leggins	Bread 7
8 Pencils	Drawers	Mutton 8
9 Blanks	Breeches	Corn 9

EXAMPLE

Casualty report: officers - 1 killed, 5 gassed, 2 wounded and prisoners; soldiers - 26 wounded, 15 prisoners, 18 missing.

CODE AS FOLLOWS:

Following required: January rice, May salt, September beef; following estimated: February belts ham, August shoes salt, December shoes mutton.

(G-3)
jem

Copy if.

Appendix 20.—THE "BASEBALL CODE"

Headquarters
52nd Infantry Brigade
26th Division
A.E.F.

S-E-C-R-E-T

France, 17 April 1918.

BULLETIN
No. 1

The following code for communications between Companies, Battalions, Regiments and Headquarters 52nd Infantry Brigade will be effective 18 April 1918, 12 o'clock.

CASUALTIES

KILLED.....Strike out
SERIOUSLY WOUNDED.....Base on balls
SLIGHTLY WOUNDED.....Hit by pitched ball
ACCIDENTALLY WOUNDED.....Balk
MISSING.....Put outs
COMMISSIONED OFFICER.....Major
ENLISTED MAN.....Minors

CAPTURES

HAVE TAKEN (No)_____PRISONERS.....Stolen Bases_____(NO)
Have Lost (NO)_____PRISONERS.....Left on Bases_____(NO)
HAVE LOST MACHINE GUNS.....Errors
HAVE TAKEN MACHINE GUNS.....Assists

ARTILLERY, TRENCH WEAPONS

WE WERE BOMBARDED BY MINNENWERFERS.....Johnson using spit ball
WE BOMBARDED WITH TRENCH MORTARS.....Leonard using slow ball
WE BOMBARDED WITH STOKES MORTARS.....Leonard using spit ball
WE BOMBARDED WITH 37 M.M. CANON.....Leonard using a curve
FIRED ON BY MACHINE GUNS.....Johnson using fast ball
FIRED WITH MACHINE GUNS.....Leonard using fast ball
WE WERE UNDER BOMBARDMENT.....Wagner at bat
WE WERE UNDER HEAVY BOMBARDMENT.....Wagner knocked a home run
WE WERE UNDER MODERATE BOMBARDMENT.....Wagner tripled
WE WERE UNDER LIGHT BOMBARDMENT.....Wagner doubled
WE WERE BOMBARDED WITH GAS.....Wagner singled
ENEMY REGISTRATION FIRE.....Wagner bunted
WE BOMBARDED.....Cobb at bat
WE BOMBARDED HEAVILY.....Cobb knocked a home run
WE BOMBARDED MODERATELY.....Cobb tripled
WE BOMBARDED LIGHTLY.....Cobb doubled
WE BOMBARDED WITH GAS.....Cobb singled
REGISTRATION FIRE (OURS).....Cobb bunted
BARRAGE REQUESTED FROM_____.....fanned
OUR ARTILLERY LAID DOWN A BARRAGE.....Sent in a pinch hitter

MISCELLANEOUS

NO UNUSUAL TRENCH EVENTS.....Game called, rain
QUIET DAY.....Game called darkness
ACTIVE DAY.....Extra inning game
THE ENEMY IS DOING TRENCH WORK at_____.....He is warming up
WE ARE DOING TRENCH WORK at_____.....We are warming up

LIAISON

WE ARE WORKING IN CONJUNCTION WITH
REGIMENT ON RIGHT OR LEFT.....We are playing doubleheader with Braves or Giants

INFANTRY

RAIDS, ENEMY.....They tried hit and run game
RAIDS, ours.....We tried hit and run game.

ATTACKS-ENEMY

STRONG ATTACK.....Kauff drives to the outfield
SMALL ATTACK.....Kauff drives to the infield.

ATTACKS-OURS

STRONG ATTACK.....Baker drives to the outfield
SMALL ATTACK.....Baker drives to the infield

SUCCESSIVE ATTACKS

SLIGHT.....1 on base
MODERATE.....2 on base
AT ALL POINTS.....Bases full

ATTACK FAILED PARTIALLY.....We made double play
ATTACK FAILED COMPLETELY.....Bases clear

RELIEF

RELIEF BEGAN_____.....Went to bat_____inning
RELIEF COMPLETED.....Scored

ENEMY PATROLS OUT.....They worked squeeze play
OUR PATROLS OUT.....We worked squeeze play

OCCUPATION OF TRENCHES

ENEMY IN OUR TRENCHES.....They put a coach at_____
WE OCCUPIED ENEMY TRENCHES.....We put a coach at_____

LOCATIONS WILL BE INDICATED AS FAR AS POSSIBLE BY CODE NUMERALS

1.....BOSTON
2.....NEW YORK
3.....PHILADELPHIA
4.....ST. LOUIS
5.....CHICAGO
6.....CLEVELAND
7.....WASHINGTON
8.....DETROIT
9.....BROOKLYN
0.....BUFFALO

For purposes of encoding, the sous sector of GIRONVILLE may be described as a base ball field, and the various elements are represented by the positions on the diamond. Field is divided into 2 parts, an imaginary line separating the right from the left battalion, on the 1 to 20,000 map by straight line drawn from GIRONVILLE to the tip of the "goose neck" at 5804 just west of APREMONT. It will be necessary to have two center fields to be designated RIGHT CENTER and LEFT CENTER respectively. The locations of units are encoded as follows:

REGIMENTAL HEADQUARTERS AT GIRONVILLE.....Home plate

RIGHT BATTALION
THE RIGHT COMPANY IN THE FIRST LINE.....Right field
LEFT COMPANY IN THE FIRST LINE.....Right center field
RIGHT COMPANY IN SUPPORT.....1st Base
LEFT COMPANY IN SUPPORT.....2nd Base

LEFT BATTALION
RIGHT COMPANY IN FIRST LINE.....Left center field
LEFT COMPANY IN FIRST LINE.....Left field
RIGHT COMPANY IN SUPPORT.....Short stop
LEFT COMPANY IN SUPPORT.....3rd Base

COMMUNICATING TRENCHES ON RIGHT.....1st to 2nd Base line
COMMUNICATING TRENCHES ON LEFT.....2nd to 3rd Base line

To designate the P.C. of individual units, the names of players are used as follows:

REGIMENTAL P.C.....~~Carrigan~~ Grandville

RIGHT BATTALION
RIGHT BATTALION P.C.....Janvrin
RIGHT SUPPORT COMPANY P.C.....Gainor
LEFT SUPPORT COMPANY P.C.....Barry
RIGHT COMPANY FIRST LINE P.C.....Hooper
LEFT COMPANY FIRST LINE P.C.....Speaker

LEFT BATTALION
LEFT BATTALION P.C.....~~Ruth~~ Appert
RIGHT COMPANY FIRST LINE P.C.....Walker
RIGHT SUPPORT COMPANY P.C.....Scott
LEFT SUPPORT COMPANY P.C.....Gardner
LEFT COMPANY FIRST LINE P.C.....Lewis
THE SUB-SECTOR ON THE RIGHT (51st Brigade).....Braves
SUB-SECTOR ON THE LEFT (10th Col.I.D.).....Giants

The place where activity occurs may be indicated by the use of the code names of the positions, for example

WE WERE BOMBARDED WITH GAS ON THE FRONT OF
FIRST LINE COMPANU OF THE LEFT BATTALION
at 11 o'clock.....Wagner singled to left field in 11 inning.

THEY ARE BOMBARDING THE RIGHT SUPPORT COMPANY
OF THE RIGHT BATTALION WITH MINNENWERFERS.....They are using spit ball at 1st base

BARRAGE FROM P.C. RABIER(RIGHT BATTALION).....~~Ruth fanned~~ Appert
OUR ARTILLERY LAID DOWN A BARRAGE IN
FRONT OF THE RIGHT CO. OF THE LEFT BATTALION.....We sent in a pinch hitter for Walker

10 killed.....10 strike outs
5 seriously wounded..... 5 bases on balls
1 Commissioned Officer..... 1 Major
3 Missing..... 3 put outs

BY COMMAND OF BRIGADIER GENERAL COLE:

FRANCIS V. LOGAN
1st Lt. Inf. N.G. A.D.C.
ACTING ADJUTANT

Appendix 21.—"SECRET INSTRUCTIONS FOR THE USE OF ARMY CODES"

Secret

NOTES ON USE OF CODE

TO BE ISSUED DOWN TO COMPANIES.
TO BE COMPLETELY DESTROYED AFTER BEING READ.

In order that information and reports, when they must be transmitted by radio-telegraphy or other means subject to interception, may not furnish valuable information to the enemy, some form of code or cipher is necessary.

No cipher sufficiently simple to be used in the field will long resist solution. For this reason, their use should be limited to absolute necessity, and messages made as short as possible. The "Playfair" cipher has been in use for many years, and is regarded as the best means for temporarily concealing the meaning of a message when a code book is not available. It can, however, be solved in a few hours, and should never be used except in emergency.

The safest means of preparing messages for transmission is by use of a code book. The code book now issued to divisions will, if properly used, be entirely safe for a period of from two to four weeks. If instructions are disregarded, and groups unnecessarily repeated, or "nulls" omitted, or if the code book is used for routine "form" report, the enemy will probably be reading your messages within a week. The surest ways of helping the enemy in the solution of your code are to send a large number of spelled-out words (one group for each letter), or to send part of the message in clear and part in code. A very few messages of this kind will give enough solutions to enable most other messages to be read.

The instructions printed in the code book are based on actual solution of enemy codes, and their importance cannot be overestimated.

To show the serious consequences of disregarding instructions contained in the code book and in General Orders No. 103, G. H. Q., 1918, the following instances of carelessness, or worse, are quoted:

(1) A division engaged in maneuvers in the rear area sent messages reporting progress of various units during the maneuver. These messages gave organizations and names of commanders in clear. This division might as well have notified the Germans definitely of its location, of the organizations forming part of the division, and of its future intentions.

(2) In one organization six code books were lost in action and that fact reported only after the return of the code books had been demanded. Whether these books reached the hands of the enemy or not is not known. No harm was done, for the reason that officers, with a greater sense of responsibility, lost books at the same time and made immediate telegraphic report of that fact, thus insuring the issue of a new edition of the code.

(3) Code messages with address in clear have been intercepted by our control station, and if intercepted by the German stations, gave the exact location of various units.

(4) A number of messages in straight code contain no "nulls." Such messages are always desired by enemy code men.

(5) Many messages contain unnecessary repetition of code groups. In one instance, a message of less than 30 code groups contained the letter "E" repeated three times. The first code group appearing after "E" was used each time. From that one message, the Germans were able to make a good guess at to which one of our code groups stood for "E."

(6) One officer reports the destruction of all the code books in his organization because the division was moving forward and he had no safe in which to store his books. While the destruction of code books to prevent capture is entirely proper, this officer destroyed his books at the very time they might be of the greatest use to him.

(7) Orders now permit the destruction of code books when a new issue is made. The greatest care, however, must be taken that the books are actually destroyed. There are now on file in this office certificates to the effect that certain code books have been destroyed in the presence of the officer signing the certificates. The code books themselves are also on file here. If this can occur with respect to code books returned, it would seem that it could also occur with respect to code books captured by the enemy. The greatest care in verifying the destruction of code books is essential.

To meet the demand of companies and other organizations for a very short code which will permit the sending of important messages without the delay now required to search through a rather large book, there is being published an emergency code list. This will contain about 50 of the phrases most used at the front. It will be republished and issued with each edition of the code book. Its return after use will not be required. It will be printed on a single sheet, which can be readily destroyed, and no effort should be spared to keep it out of the hands of the enemy.

It should be clearly understood that any carelessness in the use of our code endangers not only the officer or organization concerned, but every Allied organization on the Western front.

Before the March offensive the Germans published a complete new code for use by all troops on the Western front. This code was entirely different from anything that had yet been used, and its appearance was regarded as an indication of a coming offensive. Its solution was considered one of the most important duties

of cipher men in French, British or American service. Through the carelessness of a single German officer this code became known, and was being read by all the Allies before March 21st. The carelessness of this one officer undoubtedly cost the lives of thousands of German soldiers, and it is not impossible to believe that it changed the result of the war.

Similar carelessness on the part of American officers may in the same way cost the lives of American soldiers. The careful study of General Orders No. 103, G. H.Q., 1918, and the instructions contained in the code book issued to divisions cannot be too strongly urged.

One of the difficulties in the use of our code is the lack of experience on the part of officers in coding and decoding messages. If the instructions are followed, the work will at first be discouragingly slow, but decoding and encoding a few messages for practice will increase the speed to a surprising degree.

The code should be used freely, but according to instructions. It is the safest means of concealing the meaning of a message from the enemy, and its use for that purpose is urgently recommended.

Not all American organizations use the same code. In particular, each Army has its own code book. Divisions transferred from one Army or independent Corps to another, should leave their code books with the organization from which transferred and procure new ones on new assignment. Independent divisions when assigned to Corps or Army should immediately ascertain whether or not they have the proper code book and, if not, should make application to Corps for necessary issue.

The transmission of messages encoded in the regular way and then having the groups transposed so as to appear out of normal order, is one of the best ways in which to confuse enemy code men. Messages of this character are much feared by all code men. The preparation of this type of message is valuable experience for all officers, and helps to give enemy code men problems which they can never solve.

Appendix 22.—EXAMPLES OF LETTERS, TELEGRAMS, AND NOTES CONCERNING VIOLATIONS OF RULES FOR CRYPTOGRAPHIC SECURITY

GENERAL HEADQUARTERS,
AMERICAN EXPEDITIONARY FORCES,
France, September 20, 1918.

From: Adjutant General.
To: Commanding General, 1st Army.
Subject: Intercepted Radio Message.

The following radio message intercepted by one of our control stations is brought to your attention for suitable action:

Rec'd at U W Control Station. Time Rec'd 04.50 Date 9–18–19

M97 de K69 PO NR 1 W 120 12.15 Sept 17

BWD	CSA	QOV	FWP	BWU	NUW	DOW	JAC	BKJ	WCO	BSU	QVA	QEX	GAN	BMD	TRP	CPB	
PBY	BKJ	PCS	GKC	AJP	GAN	BMD	WOL	MPO	BGY	FGC	FRX	SXM	LGB	FPL	FGC	FSM	WSM
LGB	GES	.....	NBP	BMD	JPW	BSU	VNO	JGS	FRX	FPL	MON	JVB	OWU	DAV	DMY	ASX	
VXF	AMV	ABE	.....	J–B	.....	NBV	WNC	WUC	WBV	CAT	DPB	MON	JFC	GOS	MMP	BWY	
NAG	NET	WNC	BKC	SYK	OCA	JSA	FES	REK	QVA	LAN	DXB	.....	BKJ	BWU	MPO	GWO	
OPX	LGA	BAT	GBI	PYF	MSG	DMG	OMS	SUK	OSX	JUF	VEB	MUP	LAW	OSX	GMU	XUJ	
WOL	NBV	FRX	BMD	REK	BUW	WNC	SCP	APO	FYS	ROG	LGO	MBA	VEB	WUX	PJM	BGR	

(Sig) O E BENELL

The following violations of instructions found in the code book are noted:

Eighteen code groups representing letters of the alphabet and figures are repeated from one to three times. Without changing the text 14 of these could have been avoided by using alternate groups that were available.

A message of this length should have been sent in at least three parts as separate messages.

Words were spelled out which could have been omitted or replaced by words appearing in the code book. The message reads as follows:

"356 Infantry suggests (that) Boche observation aeroplane over Bois de Charey almost before the crack of dawn and (3 groups missed)—at to it and also a pursuit patrol might do good business at that time (1 gr. garbled) field located 60.5–41.5 Thiacourt group over by 1 Battalion 340th Field Artillery."

The word "Boche" spelled out, could have been replaced by either "German" or "enemy," words which are in the code book. By dividing "Bois de Charey" as follows: "B-o-is-d-e-Ch-are-y" it could have been encoded by 8 groups instead of the 12 groups used. "Day light" would have conveyed the same meaning as "almost before the crack of dawn" and 2 groups would have replaced the 18 groups used in encoding the latter phrase. "Work" should have been used instead of "business" and 1 code group would have done the work of the 8 used in spelling out the latter word. If it is necessary to use "business" in a message it should be divided in this manner, "b-us-i-ness" and encoded with 4 groups instead of using a group for each letter.

By using the code group for "60" instead of the 2 groups for "6" and "0" another code group could have been saved. The same is true of "41." "Thiacourt" should have been encoded by the groups representing "the" "i'," "ac," "our," "t," instead of using a group for each letter. This would have saved 4 groups. By sending "356" and "340th" as "3–56" and "3–40," the "th" after the latter number being unnecessary, 3 more groups would have been eliminated.

The above suggestions would eliminate 40 unnecessary groups and make any repetitions unnecessary, without materially changing the phrasing of the message. By rephrasing it the length could have been reduced to one-half. For example, 55 groups would have encoded the message, allowing for a sufficient number of nulls, if it had been phrased somewhat as follows:

"Enemy observation aeroplane over Bois de Charey daylight 356 Infantry believes it advisable station pursuit patrol field 60.5-41.5 Thiacourt group near First Battalion 340 Field Artillery."

The message was signed "O. E. Benell." Signatures should be sent only when absolutely required. When sent, they must be encoded, letter by letter, if necessary, and sent as a part of the code message.

Only 4 nulls were used. At least 1 null should be used for each 10 code groups. A null should always be used between double letters, which was not done in the case of the two letters at the end of "business."

Action taken will be reported to these headquarters.

By Command of General Pershing.

J. S. JONES,
Adjutant General.

GENERAL HEADQUARTERS,
AMERICAN EXPEDITIONARY FORCES,
France, September 17, 1918.

From: Adjutant General.
To: Commanding General, 1st Army.
Subject: Intercepted Radio Messages.

The following messages are brought to your attention:

(*A*) Time Rec'd 15:25. Date 9–10–18.

K95 de S95 PO NO 5 PC W18 HO 1500
ILLUSTRIOUS K95
BYM JWU GXA FEW ROS QYB MJO QEX JWU AUB CFK ONS RFG
LONDON IMMORTAL 1

(*B*) Time Rec'd 12:50. Date 9–10–18.

S95 de K95 PO NO 2 W45 ZP
TO S95 IMMORTAL
SAR QEM RPX JWU PNW JGL WXP XFV AHV BAP NBJ AGY WCK VCP DUG SAR KBX ABG
YJX UBV GWX BPL DPB DAY DPO JVC AGF VSF SBX MOS JSX XUB VJP QSC DAB PEM
XGW KBX
ILLUSTRIOUS NO 1

(*C*) Time Rec'd 11:35. Date 9–9–18.

U34 de U07 PO NO 4 HO 1110 CK 24 FM U07 TO U34 RELAY TO H33
COX WAJ KMC XOP COX JWW PNW GMJ AUB CUB RFG XYP WAV OCU BNY OLP OKP
GEORGETOWN IMMORTAL 1

Message *A* has one word in clear, the rest in code. It reads as follows: "Messages by phone and telegraph should be sent as usual to London."

The word "sent," not occurring in our code book, is spelled out letter by letter. If this message in clear had been made to read "Send telephone and telegraph messages to London," it would have been considerably shorter, would have answered the same purpose as that of the message actually transmitted, and would have given less assistance to enemy code men.

Message *B* reads: "Please furnish at least 3 copies of annex (?) V (?) to field order 12. We have no means of making copies."

The words "please furnish" are spelled out letter by letter, when the word "request" would have answered the same purpose, and could have been represented by one code group. No reason for including the words "at least" is known. If it were assumed that the officer sending this message would not ask for copies unless they were necessary, the last clause could have been eliminated.

It cannot be too strongly insisted that the sending of these long messages gives the most valuable assistance to the enemy, and will enable him to read our code within a very few days.

Message *C* reads: "Submit all subsequent reports to First Brigade Headquarters of the First Division."

The words "submit" and "subsequent" are spelled out letter by letter. If this message had read "Send reports to First Brigade, First Division," its length would have been decreased by one-half, there would have been no spelled out words, time in coding and decoding would have been saved, and the recipient would have gotten the same information that was included in the message as transmitted.

Action taken will be reported to these headquarters.

By Command of General Pershing:

J. S. JONES,
Adjutant General.

[Copy]

Signal Corps, United States Army
[Telegram]

Sept. 1, 1918.

Commanding General, 2d Div., A. E. F.:

No. 36, G–2 period Messages sent by units of your command have been intercepted by one of our control stations. These messages were undoubtedly intercepted by German stations likewise. They positively identify your division as being in reserve.

Howell

General Headquarters, A. E. F.,
General Staff, Second Section (G. 2 A. 6),

France, September 18, 1918.

Memorandum for Deputy Chief of Staff:

Subject: Indiscreet telephone conversation

In accordance with attached memorandum from Deputy Chief of Staff, I have consulted with Colonel Richardson, representing G–3, and Colonel Gibbs, the Deputy Chief Signal Officer.

I recommend that the service of checking telephone conversation from these headquarters be combined with that of supervising our own radio activity and our own use of code. I now have an officer in my office whose duty is to check all radio messages copied by our own control stations, and prepare letters for the Adjutant General's signature, reporting improper use of code or the transmission of dangerous messages. Copies of these letters are filed in my office and will be checked from time to time to see what action has been taken in each case. If it appears that proper action has not been taken or no answer is received within a reasonable time, the matter will be brought to your attention.

It would seem that letters in reference to indiscreet telephone conversation might well follow the same system. These will be addressed to the commander or individual concerned, direct that suitable action be taken and report made to these headquarters. They will then be submitted through G–2–A to your office for approval and transmission to the Adjutant General for signature.

Authority has already been given for the establishment at Army and Army Corps headquarters of an officer for duty of checking our radio-telegraphic service, and I see no reason why this same officer should not at the same time supervise the telephone conversation at such headquarters. This has the approval of the Deputy Chief Signal Officer and, with your approval, as soon as officers are available they will be sent to the various headquarters as already planned, but will, in addition, have the duty of checking indiscreet telephone conversation.

The Deputy Chief Signal Officer states that necessary listening-in equipment can be furnished at each Army and each Corps Headquarters. I will detail a stenographer for duty with the officer at these headquarters immediately, and as soon as available will also furnish stenographers for duty at Army and Corps headquarters.

Approved 9/19/18.
By direction.

Ettinger.

Appendix 23.—LECTURE DELIVERED BY LT. COL. MOORMAN BEFORE OFFICERS OF M. I. D., FEBRUARY 13, 1920

LECTURE DELIVERED TO THE OFFICERS OF THE MILITARY INTELLIGENCE DIVISION, GENERAL STAFF, FEBRUARY 13, 1920

By Lt. Col. Frank Moorman, A. E. F., G. H. Q.

WIRELESS INTELLIGENCE

General Churchill. Gentlemen, we have heard about our own M. I. 10, and this morning Colonel Moorman, of G. H. Q., A. E. F., is going to tell us about a similar service in the A. E. F.—Radio interception. From General Nolan's remarks, you know in general, the vital importance of this kind of work, and now we are going to hear from a man who really handled the thing as an expert.

Colonel Moorman. I understand that you are not particularly interested in the troubles we had in getting organized and started. What you want to know is how we worked after getting organized. There are two troubles which we had that I think you should more generally understand. One is the difficulty in getting men who are trained in the work. General Nolan expressed the situation very well toward the latter part of the war when he said that he started in with a misconception of what was required. He said that the next time he would put into this work the best brains of the country. He also admitted that he had not appreciated the importance of the code and cipher work.

Next we lacked liaison with Washington. I do not think that Washington understood our problems in the beginning. We did not understand Washington, and did not make any particular effort to appeal to them for help. Later we discovered that there was such an organization in Washington, and at the same time they found out that we were in existence in France, and then a real effort was made to work together. This would have made more efficient work had not the signing of the armistice made further efforts in this line unnecessary.

Major Yardley was sent over but got lost somewhere between London and Paris, and so never got to us until after the armistice was signed. On that account we never got the advantage of what he was going to tell us, nor to tell him what we needed.

After we got our organization started, we divided the work into five heads, namely:

(1) The intercepting and decoding of enemy messages.
(2) Locating and grouping enemy radio stations.
(3) Following their aeroplanes when they were registering for artillery.
(4) Getting what information we could from enemy telephone conversations. We had listening sets provided for that purpose.
(5) The fifth, which we did not take up until towards the last with any particular interest, was the control of our own communication, a very important phase of radio intelligence, to keep our own people from telling the enemy about what we were going to do.

Taking these up in order we find the copying and decoding of enemy messages required a line of stations along the front with a 24-hour service in most cases. Incidentally we discovered that the French with whom we worked had, on the quiet front, lost interest to a large extent on account of their having rested in one place so long. They felt that they knew the enemy's habits and what he was going to do, and that it was not worth while to keep too close a watch on him. Our men being new and keen on the job maintained a 24-hour service, with the result that we picked up several messages of extreme importance, especially at night. I understand that in one case we notified the French of an attack that was to take place on their front, and they ordered a court of inquiry to find out why they got that information from the Americans instead of from their own station.

Our system was to have the message copied at the radio station and sent to the nearest telegraph office, which we tried to make close by. The message was then telegraphed to Army headquarters and there decoded from keys furnished from our headquarters. The Army radio men will not agree with that because they did considerable work solving new codes. When the men at the Army headquarters found out that they could not handle any message, it was telegraphed to General Headquarters, where we had men far enough from the front

so that the enemy activity did not worry them, and where they had a comfortable place in which to work. They worked out the more difficult messages and telegraphed the solutions to the Army headquarters. We had six men at each Army headquarters to handle the work there, and what they could not handle they turned over to us. We tried to turn over to them as much of the work as we could.

We found in the work that the hardest job was that of the Signal Corps man. He sat in a cold station and received groups of letters quite meaningless to him, put them on the wire, and got back a code message which he could not understand and did not know anything about, so that his work was more or less mechanical. By lectures to the men who handled this we tried to impress on them the importance of the work, even though they could not see it themselves. In one case a message copied about 9 o'clock at night was telegraphed in to our headquarters, decoded and then gotten back to the front. It was about a fairly important raid which was planned to take place at 1 o'clock that night. The news had been received by us and gotten back to the front in less than 4 hours. The division at the front which was most concerned had 30 minutes' notice. The Signal Corps man handling it did not know the importance of the message, he was simply obeying orders. The Signal Corps men certainly deserve credit for staying with the work and seeing it through. It took a kind of skill that is hard to develop and hard to find. That is one important item when looking for operators for radio intelligence work, to get operators to do the mechanical work of copying and sending messages. At the Army headquarters they maintained a 24-hour service in three reliefs, two men on each relief. The result was that those men were always busy and had to be familiar with all the different phases of the work. At our headquarters we had more men. We went up to about 60 men so that we had enough to let them specialize. We had certain men to do the decoding, others to handle the goniometric work. Each man had his own specialty. We divided codes and ciphers at our headquarters, that is we had one group of men on ciphers, and another on codes. Now some of you here are perhaps particularly interested in the kinds of codes that we used, but I believe that has already been pretty thoroughly taken up, and do not think it is necessary to go into that too deeply. When we went over there in the first place, we had studied Colonel Hitt's book on ciphers, and thought we were prepared to handle the whole thing from the beginning. We got there and found that the British code on which we had put a great deal of stress and considerable work had been discarded. A British officer told me that they had discovered that it took about 30 minutes to break the Playfair cipher and for that reason they had quit using it. Before very long we discovered that we did not know anything at all about the work. Our line of instruction had been all out of date. We also found out that ciphers were scarcely ever used. Codes were the big thing on the front, something that we had never taken up. The code the Germans used was a three-letter code. They had about 2,000 code groups, and assigned to them letters, words and certain phrases. They changed this code about once a month. We found an order at one time directing that the code be changed every 4 weeks unless there was reason to believe that the enemy had the key. If a code book were lost, they immediately changed the code.

We found that at the end of the first week we were reading some of the routine messages. We found there were a number of stations that were sending regular reports at regular hours. When we got those reports, we could make a good guess as to what was in them. At the end of the second week we were reading many of the messages, and at the end of the third week we practically controlled the code. This really meant that we had for 1 week a real control of each code. The Germans had 14 different codes along the front so that there were always several in good working order. They changed their system just before the March offensive in 1918 by using a number code. You may be interested to know that that was our first real victory at American headquarters. We had close liaison with the British and French headquarters, and there was considerable competition to see who would do the work. The British and French, I must say, until the spring of 1918 were actually doing the work and we were taking advantage of it. In the latter part of February 1918 we got word from the British and French to put our best men on the new code because they thought that the change indicated something serious and that we must get busy. We happened to pick up a code message that called for a repeat of the last message in the old code. It did not take us long to hunt up the message sent from the receiving station about 20 minutes earlier, and we found another from the same station about 20 minutes later. We put the two together and read the message right off. We could read the old code, and it happened that there were two words each of which appeared twice in the message, and they fitted exactly, so we were sure we were right. That gave us an excellent start on the new code. We sent this to French headquarters by wire, but we did not have a special code for use with the British, so sent an aeroplane to take it to British headquarters. This was so no one could by any chance find out we were getting into the new code. At French headquarters a Captain Painvin who was a wizard on that kind of thing worked out in 2 days the system on which the code was built, and the result was that by the time the March offensive started we knew almost as much about the code as the Germans did themselves. They, however, did not use it as much as we hoped, and at that particular time they had adopted a new scheme for deceiving us. On the whole front where the first attack was launched they apparently moved out all the stations. There was absolute stillness so far as radio work was concerned. There was great activity, however, on their other fronts. Large numbers of messages were sent, which we afterwards learned were only fake messages. It was all

false activity, and the Germans were rather successful in their first effort to fool somebody. They fooled the British without any doubt, and we were looking in the St. Mihiel salient for a big attack that didn't come. They had taken a good many troops away. They only left enough men to keep the radio stations working. In spite of that, however, we got valuable information, and after the fighting started, they used the same code, and we still got valuable information.

Shortly afterward the Germans adopted a system of using a different key on the number code for each division. In that way we could follow the divisions.

We picked up a message one night giving orders for a raid, but as the sending station was missed, we could not locate it, and therefore did not know where it came from. One of our men figured out that a certain division, which our battle order map showed was located in a certain place, had sent the message. We took a chance and advised the troops that the raid would take place. Fortunately for us, we guessed correctly and the raid did not take place. We had hit it right.

The Germans did use ciphers at bigger headquarters. They used a combination substitution and transposition cipher. This made a lot of trouble for a long time. Lieutenant Childs, who was on duty in my office and was the best cipher man, did work up a solution for a number of special cases. The different cases he worked out soon developed so that there was little doubt, but of our finding one or two messages to fulfill the special requirements to make the solution possible. Captain Painvin, at French headquarters developed new ideas in that cipher, but I can tell you now that if you ever wish to make trouble for the other fellow use a combination of transposition and substitution or double transposition. That was another cipher they used in the east, between Berlin and the commanders in the east, and we pretty nearly gave up on that. However, some fellow got in a hurry one day and sent a long message with a single transposition. Lieutenant Childs was on the job and got the single transposition, solved it, and decided just exactly what had happened. The fellow had gotten in a hurry and failed to make the second transposition. Childs tried it out on some old messages and by making the first transposition he solved practically every one of them. He solved others as they came in.

Another cipher that was used with considerable good to us was a substitution with a long key word. They had 30 key words used one after the other. For instance message number 1 used the first key word, and so on. Between Childs and the British they got all the key words so that the reading of these messages was a matter of just the length of time it took to rearrange the letters. We did not get anything of particular military value from those messages. They were from Berlin to agents in Northern Africa and Turkey, but they did keep us informed of the troubles they were having. We got some vary interesting sidelights on the difficulties the German headquarters were having to keep their forces in line.

I think here I should bring up another point as to the necessity of keeping secret what you are doing. It works to a disadvantage for the men who are doing the job, because no one appreciates it. They must do their work and keep still. The first real message we got in our office was reported to General Nolan, who attached so much importance to it both on account of the message itself and the fact that we had really done something, that he took it to General Pershing, who must have told one of his friends. The next morning when I was going down the street, I was continually being stopped and asked all about it. A peremptory order was issued to all that code and cipher work must not be discussed. The Germans changed their code right afterwards. The work appeals to the popular imagination, and once getting started it wouldn't be downed. Everybody wants to hear about it. We tried several ways to make ourselves known so that people would appreciate us without making too much talk, but it didn't work. We finally decided that the only thing to do was to do our work and say nothing about it.

One thing we had to overcome in our own headquarters was the idea which those over us had that we were doing a lot of unnecessary work. What they wanted us to do was to pick out the important messages, decode them, and let the rest go. They understood that the greater part of these messages were valueless and so thought what was the use of bothering with them. It was a matter of considerable difficulty to make them see that we had to work them out and that the Germans did not tag their important messages before sending them. I think they got it, but you can look for that in the future; that is what they will expect of you; pick out the ones of value, work them out and let the rest go.

Taking up the question of what we got out of the enemy radio station location and grouping. We did not attach so much importance to this at first. Later we found it very important in handling the decoding work. Also in following divisions. For a time the Germans kept certain radio outfits with the divisions. They followed the divisions. Our men got familiar with them. They carried their call letters with them for a while, and we could follow the division by the call letters of the station. We would plot stations on large scale maps, and find out which ones were communicating with others, and before the Germans made an effort to try to fool us on that, we could show you which stations were at corps headquarters, division headquarters, regiments, and could divide the whole line into division, corps, and army areas. Divisions rarely communicated with anyone but division stations and corps headquarters. Regiments would only communicate with division headquarters. This divided the German front into divisions, corps, and regiments just as clearly as if the Germans had sent us a map. Later they got to changing the call letters frequently, and finally changed them every day. They

got to sending messages across army, corps, and division lines. They would send fake messages designed to confuse us as to army and division boundaries, and give us code words to work on which did not mean anything It served the purpose for a time, but later we found out the way they were sending the messages across division and army lines, and we used the fake messages to check up on one another. When we found the messages which crossed the division boundaries were fake messages, they were discarded. When we found messages went within the division limits we assumed that they were real messages. They put out too many schemes and one checked against the other. They got to sending a great many meaningless groups to break the continuity of special groups. But our men got to working that out fairly well.

We had one thing to do in locating stations, however, after they got to changing the call letters every day, and that was to work out a scheme for locating the army boundaries. The battle order attached a great deal of importance to army boundaries, and messages got to going so thick across army boundaries that we could not break them up for a while, until we discovered that in each alternate army they duplicated the call letters. That is in the First Army they had a certain set of call letter, in the Second Army another set, in the Third Army they duplicated the set in the First Army. It did not take long to compare with the map and check up. In this way we discovered the formation of two new armies, when the Germans were planning a new drive. We discovered this by the fact that the call letters had been changed. We found duplicates where we didn't expect them. We decided that they had put in a new army. We took a chance on that and we were right. The French did most of the work along that line and helped us out.

We found that the Germans had adopted a scheme in assigning call letters, in assigning them for 10-day periods. They were given a list of call letters for 10 days, one to be used for each day. To save making the list too long they were gotten out in such a way that a number of stations used the call letter from right to left, others from left to right. It was not long until we so observed. We then began keeping a list of the call letters of a given station for the first 5 days of a 10-day period. If on the sixth day some other station used the call letter that had appeared on the fifth day, we knew the next four calls and could follow the station for 4 days. This was important to us as call letters would often mean much to us. They would show us where the stations were when the goniometric service failed to get a reading.

We worked on our goniometric service very closely with our code and cipher service, because they connected up so closely. The British were unfortunate in their original organization and they were quite separated. The cipher men would learn 2 days later about movements of enemy stations. We had the advantage of coming in late and could profit by the mistakes of the British. Reorganization in the British service was very difficult to make. We were put there and charged with building up an organization. We did not have anything to break down.

The next duty we had was the following of enemy aeroplanes in registering for artillery. The British had the best success with this and we copied after them. But owing to our troops being first on a quiet front where there was not much firing, and later on a very active front where the line was moving all the time, we didn't have as good success. The British had all the advantage for that kind of work in that heavy fighting was going on on their front and the line moved very little. They had enemy batteries well located by sound and flash ranging, and by photographs and other means.

When an aeroplane went up to observe fire, there was a regular line of procedure. The first thing they would do would be to signal to the station they were to communicate with and see if the radio worked well and this would give us two bits of information—the plane that was going up and the battery that was going to fire. They had a system for following these planes on a chart. When a plane went up, the fact that this was the case was marked down in one of the little square services provided, one for each day of the month for each plane. If the fellow who flew up saw an antiaircraft gun and went back, they filled in the square with yellow. If one went up and got results, they filled in the square with red. By this system of colors it was possible to identify the kind of plane. So that if it was the yellow fellow going up, we didn't bother, but if it was the red fellow we would go after him and get all we could.

The next thing, after the plane circled up there for a few minutes, would be to signal a target. Sometimes if we knew where the targets were, we could notify the troops that they were about to be shelled. If we didn't know the target, we made a record and found out later who was shelled with the idea that we would know the next time the same target was signaled. This worked all right so long as the same call letters were kept by the same stations, but when they were changed it was more difficult. We still got excellent results, however.

Another duty: When it was found out that the German battery was going to open fire, we notified our own heavy artillery, and it has happened we brought fire to bear on the battery that was going to fire on us and did it first. The British were very well organized and got quick action. Another thing they did was to put their ground observers on the job to see where enemy planes were and report the location, getting quicker action than they could from their own radio stations. Radio stations for locating aeroplanes were connected by wire but had difficulty in getting readings from each other where necessary.

The service of charting of aeroplanes, to my mind, is entirely for trench warfare. When we got into a situation where the troops are moving back and forth or in one direction as the Germans got to doing after July 1918, the batteries move too fast and targets are moving so that the service has very little value for mobile warfare.

This same service was used for following the zeppelins. For a time this was done with considerable profit. We could notify London or Paris that zeppelins would arrive at a certain time. After a time the Germans installed a system, as did the Allies, by which the zeppelin could locate itself from stations on the ground. Previous to that the zeppelin in flight would have to keep sending out the question, Where am I?—and the goniometric station on the ground would tell them. During this operation the Allies were always on the job and finding out where they were also. I saw some very interesting maps of the course of different planes across France and over England. They followed them and took regular readings. The Allies followed those planes in October 1917 when the L–45 came down in France. The zeppelins got lost and went wandering all over Europe looking for home, because the radio broke down. Only a couple of them got back. Their course, however, was being carefully plotted by the French, who had full information as to where they were going. As far as our own service was concerned, zeppelins had gone out of fashion, and we never made any effort to handle the zeppelin situation.

Our next activity was intercepting the telephone conversations of the enemy with listening sets. We had an amplifier on our telephone sets. We got much valuable information in that way. The Germans, however, I believe, put in generators at some places along the front to make a roaring in the ground and drown out the telephone calls. We made use of the German generators and put men on the job all the time to listen for the sound and when it stopped notify our telephone operators to stop talking.

The service was not particularly popular with the troops for quite a while. In particular, one division commander objected on the ground that he thought it was all foolishness. It happened that just a few days after registering his objections he called up a regimental commander giving the location of the regimental commander, the designation of the regiment, the location of the division headquarters, and what division it was. One of our men with the listening sets 8 miles away picked up the conversation. When this was shown to the commander in question, he decided that it was an instrument worth having.

Last is our control over our own radio communications and that was an important point that we overlooked at first. It was difficult to get those in authority to see the importance of it for a time. We installed several stations to copy the American messages and send them in to our headquarters to be turned over to a man who knew nothing about the battle order or plans. He solved our code, located the divisions, prepared the American battle order and notified the Assistant Chief of Staff that an attack was to take place. He missed the hour of attack by 24 hours. It was the mistake of the Signal Corps man who sent a message, he stating that the attack was to take place the next morning, when it wasn't to take place until the morning after. When we realized what our men had worked out from these messages, every one of which could be copied by the Germans, it gave an impetus to plans for the control of our own service.

The important thing is to educate troops of the line to use codes and ciphers, and codes in particular. We had the greatest difficulty with our troops in the front lines. They did not see the need of all the "foolish" instructions. One message I recall had been written out in full and then divided into groups of five letters. The man who sent it didn't have time to use the code and so devised this scheme as "just as good." The troops could not see the necessity for changing the code, for putting in the nulls that were prescribed, and for keeping words in clear out of code messages. We tried to tell them that we would rather they sent the whole message in clear than in a mixture of code and clear, because sending them in this way gave the Germans every possible assistance in the solution of our code.

Just about the time the necessity for controlling our own radio communication came up we got a report from the German radio people. They gave every division, French and American, over a wide front, and apologized for missing one or two divisions for a few days. That also had some effect on our plans for controlling our own service. We never got a real control because the armistice came along just about that time, just when we were getting to work.

That will be the real problem for the future, to make the men at the front realize the importance of handling codes carefully and observing "foolish" little details that the code man insists on. They cannot see the need of it and they do not want to do it. They will do anything they can to get out of it. My idea would be to hang a few of the offenders. This would not only get rid of some but would discourage the development of others. It would be a saving of lives to do it. It is a sacrifice of American lives to unnecessarily assist the enemy in the solution of our code.

General Churchill's closing remarks

We are very much indebted to Colonel Moorman for stimulating our instructive training, which, without boasting, I think we can call our Intelligence University course.

In addition to that particular phase of the work that his section handled, he has given us important things to think about which concerns not only intelligence as a whole but the General Staff work, and the Army as a

460519 O - 42 - 18

whole. As far as intelligence work in concerned, he has told us why he had to generally preach the intelligence gospel, one chapter at least a day, and how he had to work against ignorance and to a certain extent preach and train. We know, all of us, that anyone who has ever had anything to do with intelligence has had to preach that same gospel, and I want to impress this strongly, that simply because the war is over, we cannot stop preaching that gospel. Everyone that knows anything about intelligence has to keep preaching that national doctrine, so that when we begin the next war, we won't begin it like the last.

The remarks made by Colonel Moorman referring to each one not understanding what the other was doing are well deserved criticisms. We often held that the Atlantic Ocean was the greatest obstacle to military progress, but when we thought that we simply thought of the ships and submarines. But it was a greater mental and physical obstacle. I am perhaps particularly well qualified to criticize people who had a lack of understanding because I was in France nearly 3 years, and when I came home, I knew very little of what was going on in America. We all thought of America sentimentally, but our minds were all turned the other way.

In M. I. D. there was gotten out a weekly report of the activities of M. I. D. This was a confidential document and was sent to G–2 of the A. E. F. In it was given the particular work that Major Yardley was doing, which linked itself with the work that Colonel Moorman was doing in France, and all phases of the work of M. I. D. were touched on this report. Now I believe that if that weekly summary of the work and activities of M. I. D. had been read by everybody in G–2, the Atlantic Ocean would have been partially bridged, but they were too busy to read it.

There is a tendency in the American Army not to read official documents, which is a very serious tendency. I think there are documents from the War Department and the General Staff that pass over many desks and are never read. I know, too, there are officers in the General Staff today who have never read G. O. 80 and yet that is the order on which the General Staff was organized. I think that everybody should try to turn over a new leaf and read the official documents that are sent to them. I know there is a perfect barrage of printed and mimeographed material and it seems almost impossible to read it all, but in a small division like M. I. D., it seems that it could be made possible, by a division of labor, to read and digest the printed and written material that comes in, so that every branch knows the information that is passed about in writing. But no matter how carefully you may read what is sent you, the full story cannot be told without personal contact. That is something that we did not get started in time between G–2 and M. I. D. I think, however, we can be very proud of our contribution both in numbers and quality. We sent Colonel Van Deman, Colonel Mason, Colonel Miles, Colonel Coxe, and Major Smiley from the Negative Branch, and toward the end we had a system whereby in each section and branch they knew that periodically certain men would be sent over to carry the gospel from M. I. D. It gave the incentive to the men in M. I. D. that they might go to France. General Nolan regretted the fact that he could not send the men back this way as quickly. Everyone knows how important it was when Colonel Dengler came back, and started to put the instruction in personnel on its feet. I regret extremely that circumstances prevented General Nolan sending more men back who could bring the A. E. F. gospel this way.

There was one reason why we were late in getting our system across the ocean. Up until August we were a branch of a division. At first thought, you would not realize that that was an obstacle, as there was only one superior between us and the Chief of Staff. If we only had one superior interested in what we were doing, it would have been different, but he was running a division made up of unrelated branches, which was unfortunate. The Chief of the Division could not know and would not know anything about what we were doing. His desk was simply swamped with an amount of detail, so that when M. I. D. papers came up to him, they were like Greek to him, and he was so busy, that it was hard to get to him to explain things, and the idea of sending someone to G–2, looked to him as though somebody wanted to go to France when he was needed here.

Now just as soon as General March reorganized the General Staff and put M. I. D. where it belonged, at the same place where General Pershing put his Intelligence at the beginning, we could then direct the Adjutant General to send our men to France and we didn't have to consult anybody. In matters of approved policy we had the right then to carry out the details. The only policy laid down to me was to develop the Intelligence Service and help out General Nolan. If I thought it was a good thing to send Major Yardley to France to get hooked up with the Intelligence people there, I could send him.

If you ever have a staff to establish, you will have to get people to carry out policies they are supposed to execute.

Appendix 24.—EXTRACT FROM THE ANNUAL REPORT OF THE CHIEF SIGNAL OFFICER (1919)

CHAPTER XXXIII

CODE COMPILATION SERVICE

The Code Compilation Section was organized in January 1918, and consisted of a captain, three lieutenants, and one enlisted man.

The first work entrusted to it was the compilation of a code book for use in the front-line trenches and the zone of the advance. A book called the Trench Code was compiled and printed. One thousand copies, with distortion tables, were issued and turned over to the General Staff for distribution.

See p. 132

The danger of capture was at once realized, and these books were not issued beyond battalions.

To meet the needs of the front line, a much smaller book was prepared and printed, known as the Front Line Code. Three thousand copies of this book were issued, with 30 different tables of distortion, so that the key might frequently be changed.

The need for a large code to meet the requirements of an expeditionary force was soon felt, and the section was put to work upon the preparation of a code for the transmission of messages between the various staff organizations in the field and at the various headquarters. This was a task of considerable magnitude and required several months' study of telegrams, confidential papers of organization, replacement, operations, and of military documents generally.

In May 1918, the Staff Code was sent to press and was completed 1 month later. This code book contained approximately 30,000 words and phrases and was primarily intended for field work.

It contained, among other things, the names of several thousand French towns and villages, and a complete list of the Army organization up to May 1918.

It is believed that this is the largest and most comprehensive code book ever printed by an army in the field. It contained both number and letter group equivalents. More than 50,000 telegraphic combinations were sent over the instrument in order by selection to reduce to a minimum the chances of error in transmission over the telegraph lines. One thousand copies of this code were printed and bound.

With this Staff Code five different tables of distortion were provided for the five divisions of the General Staff as a further protection to the secrecy of the code. These code books remained in the possession of the section and were issued from time to time upon the direction of the adjutant general.

A short three-letter group code was prepared in June for use in certain telegraph offices in order to conceal troop movements.

A more complete code of some 1,300 words and phrases was issued in July to replace the former edition.

The first trench codes in service were found to be too limited in scope and too easily decoded by the enemy to be satisfactory and a revised edition was put out in June. This book, known as the Potomac Code, the first of the so-called River Series, appeared on June 24, and 2,000 copies were issued. It contained approximately 1,700 words and phrases and was made up with a coding and decoding section in order to reduce the work of the code operators at the front.

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 enciphering, and put the burden of work upon general headquarters, where it properly belonged. Under this system one issue of codes would 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 1 month after issuance, but within 2 days it had been replaced throughout the entire Army in the field.

After this followed the Suwanee, Wabash, Allegheny, and Hudson Codes, all for the First Army and isolated units. In October 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 between 5,000 and 6,000 copies of any one issue.

Thus the Champlain, the first of what was known as the Lake Series, was issued with the Colorado of the River Series, followed by the Huron and the Osage and the Seneca and the Niagara, in editions of 2,500 each.

A short code of two-letter combinations was prepared in September to meet a measure of the needs of the front line. Six thousand copies of this emergency code list were printed and distributed down to companies. It contained some 50 commonly used emergency phrases, principally for communication from front to rear by officers who had no other code. These lists were also printed in the front of each Trench Code. Six different editions of this code were printed and distributed.

In March an addenda sheet for the War Department Code was compiled, embracing a list of transports, French cities and towns, and a number of words which had been omitted from the old code. One thousand copies of this supplement were issued.

A short code list for reporting casualties was prepared in May and printed. This list was printed in a general order.

A Telephone Code was compiled in March disguising the names of organizations and commanding officers, to be used primarily for communication by telephone. This code was reprinted with a decoding section in October. Five hundred copies were issued.

A series of distortion tables for the Staff Code were prepared and printed in July. This work was done at the Engineer Press in Langres.

A code was prepared in October, to be used as a service code by radio stations to replace the French code used up to that time by the American armies. Two thousand copies of this code were printed. The entire work of compilation and printing of this code was completed in 6 days.

In addition to the regular routine work of the office, the section at different times superintended the printing of certain confidential documents for other organizations.

During all the work of printing, which was done at The Adjutant General's office printing plant, the officers of this section were on constant duty night and day. So close was the surveillance that at all times the officers were prepared to certify that no copy had been lost or stolen during the process of composition or printing.

In the 10 months of active operation, the Code Compilation Section completed and printed more than 80,000 code books and pamphlets, all numbered, recorded, issued, and receipted for when issued. The record is complete and not a single copy is missing from the records.

Two lieutenants were transferred from this Section to take charge of the message centers of the First and Second Armies. The personnel at the close of work consisted of a captain, one first lieutenant, two second lieutenants, two noncommissioned officers, and one enlisted man.

The Special Service Division was the last division of the office of the chief signal officer, American Expeditionary Forces, to be formed. It was established on November 11, 1918, to handle all matters concerning the meteorological, pigeon, code and cipher, and visual signaling services except insofar as any of these matters had been definitely assigned to other divisions of the office of the chief signal officer.

The first officer in charge of the new division was Maj. (now Lt. Col.) Henry G. Gale, previously officer in charge of the Meteorological Section, which was at that time the principal unit absorbed in the Special Service Division. From November 27 this Division also represented the Photographic Division at headquarters, Services of Supply.

Owing to the fact that this Division operated only after the armistice, its activities were not of a constructive nature, but consisted rather in cutting down the personnel and equipment of the various sections as required by their gradually decreasing volume of business.

On February 1, 1919, the Research Division (formerly Research and Inspection Division) was disbanded and its remaining activities turned over to the Special Service Division. On February 12 the Radio Division was turned over, and its former officer in charge, Lt. Col. L. R. Krumm, became officer in charge, relieving Major Gale. On February 23, the Photographic Service was absorbed by the Special Services Division and Lt. Col. Karl Truesdell became officer in charge.

During the period between the signing of the armistice and the preliminaries of peace, the Special Service Division continued to administer these various branches of Signal Corps technical work.

Appendix 25.—Notes by J. Rives Childs after reading draft of this paper

The following notes were made by J. Rives Childs, formerly First Lieutenant, United States Army Reserve, after reading a draft of this paper:

Page 5, line 3.—A message in the Playfair Cipher exchanged between units of the American Army in France came over my desk at GHQ AEF in 1917. I took it in to Colonel Moorman and requested his permission to decipher it in order to illustrate its ineffectuality. Colonel Moorman demurred; I concluded he feared to disturb the brass hats. I agree that it was probably little used.

Page 11, line 26.—One day in May, 1918, Colonel Moorman called for me and introduced me to Col. Parker Hitt in his office. I was told they wanted me to test the system of encipherment used in connection with the Army Field Code. I was given a copy of the code and a set of messages set up expressly for the test. I was given a clerk and told to go to work and devote myself exclusively to the test. I did so and the report Colonel Friedman has correctly identified was the result. I was never informed of the use to which my report was put.

Page 11, line 40.—See above.

Page 12, line 14.—See above.

Page 12, line 21.—This is correct. See above.

Page 12, line 25.—This time I was in possession of the code book, but, as far as I can now recall, I did not have any prior knowledge of the American method of encipherment. That was my job: To learn how quickly that could be discovered.

Page 12, line 46.—See above.

Page 14, line 24.—I do not believe these relations were as close as they might or should have been. After making the report I did, I never had any further contact with Major Barnes' work. In view of the work we were doing in Major Moorman's section, the breaking down of enemy codes and ciphers, I consider it would have been highly helpful to the work of Major Barnes' section if he had been in constant touch with all the personnel of G–2 A6.

Page 17, line 22.—Upon a review of my correspondence with W. F. F., I consider the point made by him well taken, i. e., that the fact that I knew nothing of the cooperation between Moorman and Barnes does not prove there was no such cooperation. The evidence he offers establishes that there was greater cooperation than I even suspected. I still hold to the opinion, however, that this cooperation, to have been most effective, should have extended down to the personnel of the two sections.

Page 26, line 14.—This is correct.

Page 28, line 12.—It is clear to me from Colonel Friedman's study that my sweeping conclusion * * * of the lack of liaison between Major Barnes and Colonel Moorman and with others was unwarranted.