ACKNOWLEDGEMENTS.

This brochure on the methods of solving the codes and ciphers used by the Germans would have been almost impossible were it not for the assistance rendered us by the code and cipher officers of our allies. In the exchange of results attained, we were by far the gainers. They have never hesitated to place at our disposal all the methods and the results of their labors, without which, our efforts would have been very much less productive. It is a great pleasure to acknowledge our indebtedness to them.

Some of the material forming the basis of this survey is taken from reports by various officers who were members of this section, and due acknowledgements have been made to their work at the proper points. Special mention is due to Captain H. A. Berthold, C. A. C., for his invaluable assistance in instructing the officers who came after him in most of the details of the methods as regards codes described herein. In this work he may well be said to have been a picneer.

To Captain P. B. Whitehead, F. A., are due my sincere thanks for his many suggestions offered during the course of my labors and for his kindness and invaluable assistance in proof-reading the final copy.

W. F. FRIEDMAN,
1st Lt. M.I.D.

General Headquarters,
American Expeditionary Forces,
February 5, 1919.

REPORT ON ENEMY CODES AND THE METHODS USED IN THEIR SOLUTION.

	Page
Introduction	1
Types of code and cipher used	3
General remarks on code	6
Preparing the messages for study	9
RECORDING AND INDEXING THE THREE LETTER CODE TEXT	15
I. Necessity for and purpose of recording	15
II. Methods of recording	15
1. Charts	15
2. Record books	17
III. Advantages and disadvantages of each system	19
1. Charts	19
2. Record books	20
IV. The "BIBLE"	20
V. Triptics	21
VI. Extracts	22
METHODS OF SOLVING THE THREE LETTER CODE	23
THE "K R U" CODES	28
Solution by Classification and Identification	28
The uses and characteristics of the main classes of code groups	30
I. Numbers	
A. Uses	30
B. Characteristics	30
C. Classification and identification	31
II. Spelling groups	
A. Uses	33
B. Characteristics	36
C. Classification and identification	37
III. Words and phrases	
1. Military Units	38
2. Interrogatives	39
3. Prepositions	40
4. Other frequent words	42
IV. Punctuation	44
V. Auxiliary signs	47
VI. Blind groups	49
Solution by Analogy	50
THE "K R U S A" CODES	59
1. Increasing complexity	59
2. System of enciphered spelling	65
3. Decknamen	68
4. Distortion	70
Length of time codes were in use	72
"Preliminary remarks to KRUSA code # 152	74
Method of breaking into KRUSA codes	77

	Page
CAMOUFLAGE OF LIAISON	80bis
1. Changes in procedure as regards call signs	81
2. Regulations regarding the number, direction, and contents of messages	83
Practice messages	85
(1) Practice tactical and operation. messages	87
(2) Proverbs, etc.	87
(3) Fictitious messages	88
(4) Artificial messages	89
(5) Distorted messages	89
(6) Blind group chains	90
Conclusion	93
THE THREE NUMBER CODE	95
Directions for use and discription	95
Methods of solution	106
Numbers	107
Spelling groups	107
Words	111
Special methods of solution	111
Secret keys and supplements	113
General remarks and estimate of the code	114
EXTRACT FROM THE THREE NUMBER CODE	130
Local SYSTEMS	131
EMERGENCY SIGNAL SYSTEM	132
AVIATION CODES	133
METEOROLOGICAL CODES	134

INTRODUCTION

This report is intended to give a detailed account of the technical work of the Radio Intelligence Section insofar as it was concerned with the main function of the section, viz., furnishing to the proper authorities such information regarding the enemy and his intentions as could be secured from (1) the solution of his code and cipher messages, and (2) a detailed study of his wireless traffic.

It is but natural that the progress made in all phases of military activity during the European War should have included marked advances in methods of secret communication. The development and improvement in German military cryptography began not long after the outbreak of the war and continued steadily until the end, attaining by the fall of 1918, a remarkably high state of efficiency.

In what follows it will be presumed that the reader already has a fair knowledge of the fundamental principles of ciphers and cryptography in general, and that he understands the nature of the mental requirements necssary for all cryptographic work.

First, it is necessary that the reader understand the organization of the German Signal Service, especially the so-called DIFUA or DIVFUNKA, (Divisions-Funker-Abteilung) or Divisional Wireless Detachment, so that he has a proper understanding of the relative positions of the various stations in the DIFUA, and their relations.

Exhibit 1, which is a copy and translation of a German chart, will repay close scrutiny. It shows the arrangement of the stations in a typical DIFUA within a divisional area, and the various means of liaison which existed between them. For a detailed exposition of the German Signal Service, the reader is referred to the report of Capt. P. B. Whitehead, F.A., of this Section.

2 To facilitate reference, the entire length of the Western Front was divided up arbitrarily according to the number of German Armies occupying it, and to the "sectors" thus determined the consecutive letters of the alphabet were applied, commencing on the coast and proceeding in the general direction south. Since on the

whole, the number and relative positions of the German Armies on this front underwent no marked change throughout the war, the letters applied to the sectors could be applied also to designate the Armies. Each of these sectors in turn was divided up according to the number of divisions holding it; to the sub-sectors thus formed beginning on the left, consecutive numbers were applied in multiples of 5 (to allow for the appearance of new divisions). A DIFUA could then be referred to by us according to the sector and sub-sector occupied by it, or by the division to which the DIFUA was attached. Thus the DIFUA serving the German 29th Division when that organization was located in January 1918, on the right bank of the Meuse was referred to as G-30, "G" indicating the sector, or the German Fifth Army, and"30" the sub-division of the sector (see Table I, below). Sectors were also referred to by a general name derived from the geographical location, and it may be useful to give them here.

The following names and limits of sectors and "group sectors" i.e., the sub-divisions of sectors closely allied by reason of the topography in the vicinity of the American troops were designated as official in May, 1918:

TABLE I.

SECTOR:	LIMITS:
ARGONNE or F-Sector	The AISNE River to the eastern limit of ARGONNE FOREST
VERDUN or G-Sector	Eastern Limit of ARGONNE FOREST to MOULAINVILLE
WOEVRE or H-Sector	MOULAINVILLE to the MOSELLE River
LORRAINE or I-Sector	The MOSELLE river to the PLAINE River

GROUP SECTOR:

ARGONNE or F-SECTOR, GERMAN III ARMY

PY-Group Sector	F-10, F-15, F-20
DORMOISE-Group Sector	F-25, F-35
ARGONNE-Group Sector	F-40, F-45, F-50

VERDUN or G-SECTOR.	GERMAN V ARMY
W.MEUSE-Group Sector	G-10, G-30, G-25
E. MEUSE-Group Sector	G-30, G-40
ORNE-Group Sector	G-50, G-55
VAUX-Group Sector*	H-5, H-7
WOEVRE or H-SECTOR.	GERMAN DETACHMENT "C".
EPARGES-Group Sector	H-10, H-20
ST. MIHIEL-Group Sector	H-25, H-30, H-35
THIACOURT-Group Sector	H-40, H-45
LORRAINE or I-SECTOR.	GERMAN XIX. ARMY.
BERSDORF-Group Sector	I-5, I-10
BLAMONT-Group Sector	I-20, I-25, I-30, I-35

*(NOTE: In the spring of 1918 the left boundary of the German Fifth Army was extended and made to include the region formerly occupied by the right wing of Detachment "C", but the sub-sector designations were unchanged.)

TYPES OF CODE AND CIPHER USED

A brochure on the methods of secret communication used by the Germans may well begin with a description of the accompanying chart which was issued by the Germans themselves in April 1918 to illustrate the regulations for the use of code and clear text. This chart ~~which forms Exhibit 2,~~ is almost self-explanatory. Within the three-kilometer danger-zone no clear text whatsoever was permitted. The only authorized method of communication within the danger zone, whether it was by means of dogs, pigeons, ground-telegraph, lamps, radio, telephone, or even in the case of couriers, had to be in a code called the THREE-NUMBER CODE. No other code or cipher was permitted. Artillery observers, and forward intelligence officers also had to use this means. The only exception to this regulation was in the case of communication between aeroplanes and ground stations, in which case a specially prepared set of phrases and signals known as the EXTRACT FROM THE THREE-NUMBER CODE was permitted. There was a code, the AVIATION CODE, specially prepared for the use of giant bombing aeroplanes, and for balloons, which code is not shown in this chart, inasmuch as the latter is intended solely for illustration to troops. There was also a

special METEOROLOGICAL CODE.

For communication between regiments, divisions, and artillery sub-groups ~~and division,~~ another code, called the THREE-LETTER CODE, as well as the Three-Number Code was provided. For communication to the right and left within the danger-zone only the Three-Number Code was used; behind this zone the Three-Letter Code could be used.

Communication between division, and corps, and army headquarters was by means of the ADFGVX CIPHER, also called the Geheimschrift der Funker.

Beyond that, the WAR DEPARTMENT CODE, in addition to the aforementioned cipher was used. Since messages in this code were never sent by wireless we know nothing about it.

The Germans were consistent throughout in applying some external differentiating marks to their various codes and ciphers. For example, their various ciphers bore in their preambles the word "RICHI", "ALACHI", or "ITOCHI", etc., designations made up of the abbreviation CHI (CHIFFER=cipher) and letters indicating the system. The four different codes which were in effect simultaneously were distinguishable from their external appearance. For example, the code-groups in both the Three-Letter Trench Code and the Aviation Code, consisted regularly of combinations of three letters, but in the former the initial letters in each group were different from those in the latter, and in both cases the number of initial letters was very limited, at first only three, finally, five. The exact reasons for limiting the number of initial letters are not known, but there are two which seem probable:

5

1) These distinguishing features not only as regards the initial letters in these two codes, but also as regards all the external designations which went with their various codes and ciphers such as RICHI, ALACHI, etc., would tend to prevent confusion, and expedite delivery and decoding or deciphering of messages within their own lines of communication.

2) Limiting the number of letters to a given few would tend to reduce to a minimum the errors of transmission, to which all messages transmitted by telegraph are subject, and

enable such errors as do creep in to be rectified more speedily. It is obvious that if the receiving operator is listening for a few of a limited number of letters he is apt to get them nearly correct. Also, in endeavoring to trace the incorrect letter in a code-group, the decoder will have to deal with only a very limited number of possibilities as regards the initial letter in these codes or in other words, the number of possibilities are extremely limited as regards one-third of each group. In the case of the ADFGVX Cipher, the fact that only six different letters were used enabled errors to be corrected very readily. In this cipher each plain text letter ~~is~~ was represented by a combination of two of the letters A, D, F, G, V or X, and it was rare that two letters in succession would be mutilated. Given one-half of each combination as correct, the number of possibilities was very much reduced as regards the letter for which it stood.

As regards these codes, however, there was one disadvantage to the limitation of the initial letters; it enabled us to devise a compact, simple system of recording or indexing the groups as will be explained further. Had each group of three letters begun with the various letters of the alphabet, recording and tabulation would have been a much more serious problem to us than it actually was.

6

GENERAL REMARKS ON CODE.

A CODE may be defined as a list in which letters, words, phrases and sentences are designated by arbitrary symbols, or groups of symbols, by the combinations of which it is possible to convey a message. The code-designations usually take the form of combinations of letters or figures, termed code-groups. When such a list is extensive and is arranged in some systematic form it is called a CODE-BOOK. In order to meet the requirements of special

usage, code-books vary greatly in their contents. It is obvious that a code for a specialized branch of commerce, as for example, the rubber industry, would be very different from one adapted to warfare. The German Three-Letter Code is a good example of a highly specialized code adapted to trench warfare.

The process of transforming the clear text of a message into the corresponding code equivalents is called ENCODING. The process of converting the code equivalents of such a message into the corresponding clear text is called DECODING. It is obvious that this cannot be accomplished without possession of the code-book.

In a broad sense the distinguishing feature between cipher and code is that in the former, one deals with the individual letters of the message, whereas in the latter one deals with letters, words, phrases and even entire sentences.

The advantages of code, and of code over cipher as a system of secret communication are as follows:

(1) It permits of rapid encoding and decoding. In this respect code is much to be preferred over cipher.

(2) The encoded message is usually much shorter than the original clear text and thus represents a great economy. Cipher messages are usually just as long, sometimes longer, than the corresponding clear text.

(3) It permits of a high degree of secrecy. As distinguished from cipher in regard to the degree of secrecy, it may be pointed out that whereas the solution of a single message in a cipher discloses the whole system and enables one to decipher every ~~subsequent~~ message in the same key, the solution of a single message in code or the comparison of a code message with the corresponding clear text affords only the solutions for the particular code groups of which the message is composed, though it should be added that these may furnish valuable clues to others. Therefore, the degree of security is much higher in the case of a good code than in that of cipher.

7

The degree of security is indeed very high, unless a copy

of the code-book falls into the hands of the enemy or so many messages have been sent that the enemy is able to RECONSTRUCT the code-book by a detailed analysis of a sufficiently voluminous text; in such a case it becomes tantamount to the actual possession of the code-book. What is meant therefore by the process of "solving a code" is the reconstruction of the code-book.

There are, in general, two types of code-books. In the first type, the clear-text contents are arranged alphabetically and are accompanied by their corresponding code-designations arranged in systematic form (either numerically or alphabetically, whichever form the code-groups take). In such a code only one arrangement is necessary, the same book serving both for encoding and decoding. In the second type, the clear-text contents are arranged alphabetically, accompanied by their corresponding code-designations which have been chosen at random, and therefore follow no system whatever. Hence, in such a type, in addition to an encoding book, a decoding book is necessary, in which the code designations are arranged systematically, accompanied by their corresponding clear-text equivalents, which are then at random.

It is easy to see that in the former type the solution of a code-group will offer clues to the solution of code-groups "alphabetically or numerically related" to the solved group; for instance, if code-group 123 has been found to be the word DER, 122 may be DEN and 124 may be DES. In the latter type of code-book no such clues can be derived. The group 123 may mean DER, and 124 may mean WANN.

Now when a message has been encoded, and the code-groups are then enciphered, the result is spoken of as ENCIPHERED CODE. For example, if the code-groups for the phrase "ACCORDING TO REPORTS RECEIVED" are 472 807 and some system of encipherment is applied to them so that they appear finally as 609 851 or as RAN KVS, they would be spoken of as being "enciphered code".

If great secrecy is desired, some form of encipherment is therefore applied to code. Should the enemy possess a copy of the code-book, he would still be confronted with the necessity of

solving a cipher.

In codes of the first type defined above, it is usual to apply some form of encipherment which can be changed at will, and often, without necessitating a complete change in the form, contents, or the code-designations of the code-book. For this purpose, ENCIPHERING TABLES are used, and changed as often as necessary. But in the case of the second type, secrecy may be attained by a frequent change in the code-designations in the encoding part, necessitating, each time, of course, a complete revision or rearrangement of the decoding part. In short, in dealing with the latter type, when we will speak subsequently of a "change in code", it will be meant to indicate merely, that a new edition of the code-book went into effect; the code contents remained fixed, but the code-designations changed.

Now the Three-Number Code was an example of the first type. The form and contents of the code-book were standard throughout the German Armies on the Western Front. Each division issued its own Enciphering Table and secrecy was maintained by frequently changing it.

The Three-Letter Code was an example of the second type. The form and contents were also standard throughout the German Armies, but each Army issued and changed its editions independently of the others. Therefore, there were about ten different editions in effect simultaneously on the Western Front, and it was obviously necessary, therefore, to restrict one's study to the particular edition with which one was concerned.

9 The process, therefore, of solving the Three-Number Code, after a copy of the code-book had been captured, involved in reality only the analysis which was necessary for the reconstruction of the enciphering table, whereas the process of solving the Three-Letter Code involved the analysis necessary for the reconstruction of the code-book. The two processes were very dissimilar.

PREPARING THE MESSAGES FOR STUDY.

It will be essential first to describe the manner in which the material was prepared for study.

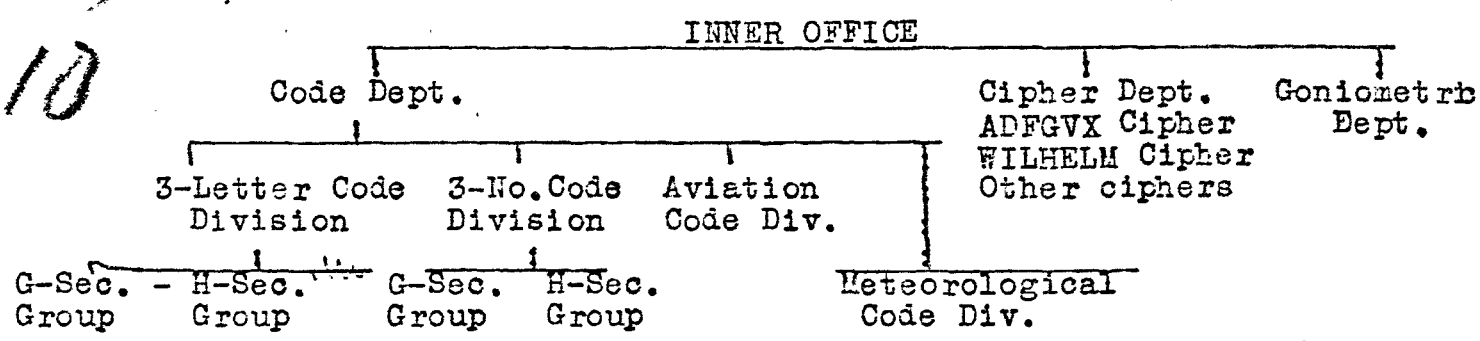
All messages as they arrived from the intercept stations first went throughthe office of the Adjutant of the code office, or the "Outer Office" as it was called. Here a clerk separted the code messages from the cipher, a process which was usually very easy and which was learned after a little experience, because the messages bore on their face the distinguishing characteristics applied by the Germans themselves, as mentioned before. On account of the impossibility of preventing the occasional filtering through of messages not in enemy code or cipher, but in our own or in that of our Allies, the clerk had to be familiar with the external appearance of the latter messages, which was also very easily learned.

First of all, the German Naval, Diplomatic, and Colonial Code text which was intercepted by the station at G.H.Q. was sent directly to the office of the Chief Clerk, who supervised the stencilling of this material, which was then sent to the proper authorities at Washington. No work on these messages was attempted in this office.

Next the cipher text and text of the codes used on the Western Front were sent directly to the respective departments concerned.

The "Inner Office" of the section was subdivided into a number of departments, each concerned with a particular enemy code or cipher. Graphically, the distribution was as follows:

10



The code department had a clerk whose duty it was to receive from the "outer office", and to arrange the code messages for stenciling. It was first necessary to separate out the various codes, and then, in the case of the Three-Letter and the Three-Number

Codes, to separate the messages into the G-Sector and H-Sector piles. The clerk did this sorting ~~This sorting was done~~ by means of the "Daily Field Station List" furnished by the Goniometric Department (see Part VII, Section 1) and the sector concerned was indicated by colored pencil on each telegram. He then arranged the messages in each pile according to the following:

(1) All messages from the same sub-sector were first brought together and the separate piles were arranged numerically. Thus there might be five messages from H-10; eight from H-15; seven from H-20, etc.

(2) All messages within the same sub-sector were then arranged as regards time of transmission from 0001 to 2359. (The 24-hour system was standard).

(3) All messages of approximately the same hour were then arranged with reference to keeping together, or as close together as possible, the messages between the same sending and receiving stations.

It is in this process of final sorting that the best judgment and experience of the clerk were brought into play, not only as regarded the ultimate sequence of the telegrams, but, what was of greater importance, the bringing together of duplicates (the same message might have been intercepted by three of four different stations) and by means of a careful comparison and a judicious discrimination, correcting one copy which was taken to represent the original telegram with a minimum number of errors of transmission.

11 In doing this the clerk was guided by the number of intercepts which agreed and by the reliability of the stations concerned; one station may have been known to be very reliable, either being closer to the transmitting station, having better apparatus, or better operators; the other station may have been known to be usually unreliable, on the same basis. All of these factors counted. Many times, however, it was impossible to decide which of two or three different readings was the correct one. In this case the clerk inserted at the proper places on one copy, the other intercepted readings in parenthesis, ~~and the final copy, the other~~

~~intercepted readings in parenthesis~~, and the final copy, when it was put into the hands of the code-solvers, showed these alternate readings.

The assorted messages were then turned over to the typists for stenciling. Each message was accompanied by all indications in clear at the beginning or at the end of messages, and the latter were carefully typed out, leaving a fair amount of space between lines to admit of the insertion of values later.

The stenciled text was then distributed to the respective sub-divisions concerned.

Let us examine in detail the attached sample sheet of text of the Three-Letter Code.

The heading on the page is as follows:

"H" SECTOR-ALBERT CODE NO.17 (Started August 22, 1918)

It was stated above that there were about ten different editions of the Three-Letter Code in operation simultaneously on the Western Front all the time, since each Army issued its own edition independently of the others. When this office was opened, study of the Three-Letter Code was restricted to the material coming from that portion of the front occupied by the Fifth German Army, i.e., The Verdun or G-Sector; later the material coming from that portion of the front occupied by the German unit called DETACHMENT "C", i.e., the Woevre or H-Sector, was added. The material from all other sectors was studied by the British and the French offices, in accordance with the portion of the front held by each.

12

For convenience in reference, the code applying to each of these sectors was given a name, chosen purely arbitrarily by the office studying the code concerned; and since these codes "changed" (i.e., a new edition went into effect) at more or less regular intervals, each particular code had in addition a serial number. As to how it was determined when the code changed, that will be taken up later (See Page--). When the type of a code changed in some very noticeable manner, a new name was applied and this formed the starting point of a new series of codes. Thus, for example, "The Fritz Code", which was in operation in the G-Sector, was replaced by "Andre Code", which in turn was succeeded by "Marcel Code". The name "Albert" was applied to the codes used by

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES
GENERAL STAFF, SECOND SECTION (G.2 A.6, (AJU)

"H" SECTOR-ALBERT CODE #17 (Started Aug. 22, 1918)

(DISTRIBUTION "A")

Aug. 29, 1918.

A) --- v LDT (--vH10-8R) S.-- CHI-6

AUW UGR KFI ULO KED SIJ NF LDT UM

B) DIM v GMI (H7-5RvH25-7D) T-4.0.48 1.25 CHI-10

ALY SXB ACW KFI UTP ROE RJW KOW SGO REI - ZWEI 2 WP GMI UM

C) GSO v GMI (H25-13BvH25-7D) T-4.1.14, T-3.1.10 2.04 CHI-10

UTE ATW RJV (or ROU) UGR RFF RLW KXJ (or KXO) KXE (or KUT) SYE SRV (or SAS) - EINS 2 WP NF GMI UM

D) GNE v GMI (H25-9RvH25-7D) T-3.8.39, T-4.8.42 9.30 CHI-9

AAX KED SER UAW KNV (or KNU (??) SVF RKA KMF APS - NF GMI

E) GMI v GNE (H25-7DvH25-9R) T-4.9.18, T03.9.15 10.07 CHI-9

SAH KUD SWA RKA STM KED KRD (or KRN) AJU (or AJO) AAX - GNE UM

F) GSO v GNE (H25-13BvH25-9R) T-3.9.24, T-4.9.25 NU ZI-3

APW KSX UXF - GNE UM

G) GMI v DRW (H25-7DvH25-4R) T-3.11.07 11.15 CHI-16

APS UGJ AQW AEL RJV SWF KME UEJ KDB RKZ RKA RGV AAW RVE STQ UPR - NF DRW UM

H) DRW v GMI (H25-4RvH25-7D) T-3.11.10, T-4.11.13 12.00 CHI-12

UPS KFI RQL SAV ADC KPS UPX RJV UWV RRK KCX SAH - GMI UM

I) DDT v GSO (--vH25-13B) S.-- CHI-10

RII AQV AIF RJV ADS ANL UNS RKA KAY AVG - NF GSO U

J) --- v GSO (--vH25-13B) S.-- 15.12 CHI-11

KKT AQI AKH RPU RLW SJW KLD RRK KED KYE AVE - GSO U

Aug. 29, 1918.

QB v GMI (H7-2vH25-7D) T-3.14.26 15.20 CHI-7
RWI KFI SZB ANY UAI RLV RKO (BRIGADE) - NF GMI UM

--- v GSO (--vH25-13B) S.-- 17.25 CHI-10
RJD UEX ULE SKH (NACH) RLW ADG ABT RXR KED KVK - NF GSO UM

RW v LKT (H25-4RvH30-7) T-3.10.50, T-4.10.49, S.5.40 5.40
(1145) CHI-12 SFN KCM (VON) AST SHN (CH) AAB (AU) UNZ SRT UOF SGF
RGP SSG RNV - NF LKT UM

K v (LKP) (H30-4Bv--) S.-- 6.05 CHI-12
VE UHT RNT UMJ SIH ABC AEP KST (IE) SXH UWX (REGT) RST KXJ
KP

H v GOK (H30-3RvH30-4B) T-3.6.29 7.10 CHI-11
J RNP RHQ KUK ANL UKL AST KGG RXM KZH SSG - NF
K UM

H v GZW (H30-3RvH30-5R) T-3.7.10 7.50 CHI-9
M ANL (HOPKEN) UVE KRN (III R) RAF KNH ADG KDM AQV - GZW UM

H v DIP (H30-3RvH30-12D) T-3.8.51 T-4.8.55 9.05 CHI-8
(or UNL) RRK KSP AST SNT UUV SWW SUR (or SNT) -
DIP UM (SIA)

v GOK (H30-5RvH30-4B) T-3.10.12, S.-- 11.05 CHI-15
UEV RRG KNB (or KHB) USQ RNP (or RRP) ADX AOB KST
KXD RIF KQX SEH KUV - GOK

v PPH (H30-12DvH30-3R) T-3.10.54 11,40 CHI-12
KNB AMM (RE) UAW (T) KCD RXU UGR (ES) ADC SEI (GIVE) SER SVJ KXJ -
PPH UM

v LKT (H21-1vH30-7) T-3.12.15, T-4.14.29 13.05 CHI-7
(or DRW) UPA (45) SM- (or SZE) KQX KED AVD RKA SAJ -
LKT UM

v LKT (--vH30-7) T-3.13.18 14.10 CHI-15
SWZ SKM KAY USQ SEI KTQ RCC AVI UKL RPP KZH SSG
RXU - NF LKT UM

SECRET

pbg

GENERAL HEADQUARTERS AMERICAN EXPEDITIONARY FORCES

General Staff Second Section G-2 A-6

(DISTRIBUTION "H") 31st August, 1918.

Daily report of grouping of German Radio Stations.

Grouping of 29th August, 1918.

Group	Div.	Brigades	Regiments	Calls
G-10	231	231 Inf.	442, 443, 444, 100 FA.	DEO'(Rear), LVW(3), PEU, PFB(8).
G-25	22R	43R.Inf,	71R., 82R., 94R., 22R.FA.	DKS(Rear), DPB, DFB, LNC, PNK, PEN.
G-30	123	245 Inf.	178, 351, 106, 245 FA.	GQR(1), GZR.
G-40	232	232 Inf.	445, 446, 447, 37 FA.	LXM.
G-50	33	66 Inf.	98, 130, 136, 33 FA.	DOX(8B), GMX, GXM(4R), LOI(3), PGX.
G-55	32	- - - - - - - - - - - - - - -		No activity.
		Detachment "C"		
H-7	8LW	56 Inf.	109 LW., 110 LW., 111 LW., 8 LW.FA.	DIM(5R), DO'L(6), GQB(2), LDG(4R) LDZ, GBA'.
H-10	13LW	60 Inf.	15 LW., 60 LW., 82 LW., 13 LW.FA.	LDT(8R).
H-25	35th Austrian Division.			DRW(4R), DFU(1), GMI(7D), GNE(9R). GSO(13B), LTN, GLU.
H-30	31	32 Inf.	70, 166, 174, 31 FA.	DIP(12D), DLO(11), GOK(4B), GZW(5F LKT(7), LVF(2B), PPH(3R), DCN, DLD, LJN.
H-35	5LW	- - - - - - - - - - - - - - -		No activity.
H-40	227	49LW.Inf.	417, 441R., 447, 92 F.A.	DZD(6), DAM(2R), DAV(7D), DDM, DAY, DGC(5R), GIH(1B), LQB.
H-45	77R	77R.Inf.	332, 255, 257, 59R.FA.	DIJ(1R), DPU, DAS, DGZ(10D), GWA, GWP(2R), DA'K, DWP, DVC.

NOTE: Numerals in parenthesis indicate location of station, See Map.

(o v e r)

pbg

alphabetical list of field radio station call signs in the German 5th Army and Detachment "C", on the 29th August, 1918.

DAH F ?
DAK H 45
DAM H 40 (2R)
DAS H 45
DAV H 40 (7D)
DAY H 40

DBE F ?
DBI I 15

DCN H 30

DDI F ?
DDM H 40

DEO' G 10 (Rear)

DFB G 25
DFU H 21 (1)

DGC H 40 (5R)
DGZ H 45 (10D)

DIA F ?
DIJ H 45 (1R)
DIM H 7 (5R)
DIO F ?
DIP H 30 (12D)
DIT F ?

DJD F ?

DKS G 25 (Rear)

DLA' F ?
DLD H 30
DLO H 30 (1)

DME I 15

DOD F ?
DO'L H 7 (8)
DOX G 50 (8B)

DPB G 25
DPU H 45

DRW H 25 (4R)

DUZ F ?

DVC H 45

DWP H 45

DZD H 40 (6)

- - - - -

GAH F ?

GBA' H 7

GDR F 50

GIH H 40 (1B)

GKV I 15

GLU H 25

GMI H 25 (7D)
DMX G 50

GNE H 25 (9R)
GNL F 50 (4)

GOK H 30 (4B)

GQB H 7 (2)
GQR G 30 (1R)

GRU' F 50 (3)

GSO H 25 (13B)

GUV F ?

GWA H 45
GWP H 45 (2R)

GXM G 50 (4R)

GZR G 30
GZW H 30 (5R)

- - - - -

LDG H 7 (4R)
LDT H 10 (8R)
LDZ H 7

LHD F ?

LIA F ?

LJN H 30

LKG I 15
LKT H 30 (7)

LNC G 25
LNK G 25

LOI G 50 (3R)

LQB H 40

LTN H 25

LVF H 30 (2B)
LVW G 10 (3)

LXM G 40
LXQ F ?

- - - - -

PEN G 25
PEU G 10

PFB G 10 (8)

PGX G 50

PHM F ?

PNH F ?

PPH H 30 (3R)

- - - - -

B - Station used by Battalion Headquarters
C - " " " Corps "
D - " " " Division "
R - " " " Regimental "

(o v e r)

the enemy, in the H-Sector, and there were in all about a dozen changes from the beginning of the study of this code until the signing of the armistice.

The heading on this sheet, therefore, shows that the text applies to Albert Code No. 17, which commenced on August 23.

Below this heading is indicated, for the attention of the mailing clerk, to what distribution this material belongs. The proper distribution of all material to other offices is a function of the Outer Office.

The date on which the messages were sent is given on the same line.

Then follow the telegrams, each numbered alphabetically beginning with A at the top of each page, ~~and~~ the ~~latter~~ pages are numbered consecutively in each code. This provides a convenient, standard way of referring to every telegram; for example, 47A. The most important use of this will be discussed later.

A standard form was adopted for setting forth each telegram, a few words on the various parts, together with a general discussion of the use of abbreviations may be necessary.

Let us take telegram 47B. First come the call-signs of the stations concerned. These are naturally given in the telegram itself. The abbreviation "v" stands for the word VON (from). This message was sent from station GMI to station DIM. Then in parenthesis is given the location of each station as determined by the Goniometric Department and given in their Daily Field Station List, a copy of which, applying to the day's traffic under consideration, is attached. It shows that GMI, the sending station, is located in H25, and is indicated as station 7 in the group, a divisional station; DIM, the receiving station, is located in H7, and is indicated as station 5 in that group, a regimental station. By referring to the GROUPING of the German Radio Stations as given on the Station List, it will be seen that DIM may be the call of the station attached to the 109th, 110th or 111th Landwehr Regiment, or to the 8th Landwehr Field Artillery Regiment. As regards station GMI, no regimental numbers have been identified as yet. We will see later how all this information may be used.

13

After this comes the name and number of the intercept stations, and the time at which they picked the message up. (the letter "T") stands for Toul, "S" for Souilly. Then follows the German time and all other indications contained in the preamble of the message. Inasmuch as the German time on the Western Front was made to correspond with the time at Berlin, there was usually a difference of about one hour between the German time and the time given by the intercept station. Also, the German time applied to the time when the message was prepared, and since messages could not always be transmitted immediately after their preparation, the discrepancy between the German time and our own varied.

The abbreviation CHI stands for CHIFFER (cipher) and ZI, for ZIFFER (cipher). As a rule, a CHI despatch was a tactical message; a ZI telegram dealt with station operation. However, these distinctions were not always used consistently and invariably by the German operators.

Then followed the number of groups in the message. Where our intercept stations failed to get this number it had to be omitted rather than indicate a number found by counting the groups received.

14

Often certain abbreviations would be given by the German operator in the preamble, and these were always included in the stencilled copy because they sometimes furnished clues of the utmost importance. A complete list of the abbreviations used in German wireless traffic is attached to this report forming a part of Section -- Part VI.

As a good example of an important clue furnished by such abbreviations and indications in clear, a case will be given.

The following message was found in the text of one day's traffic:

DZE v DGS (H-35 v H-40) T-3.17.03 (no time or CHI given)

UNM DEX HAT - MR DGS BP

When the abbreviation MR (MOTOR TROUBLE) was recognized as being part of the message, instead of regarding the two groups DEX and HAT as containing errors in their initial letters it was

seen that if UNM was the code group for STATION, the message would make complete sense as it stood. It was also noted that there was a station DEX which took part in the day's traffic some hours after this message was sent. The carelessness of this operator gave us the solution for the group UNM, evidently STATION.

Often a relayed message will contain in its preamble just before the German time-group the phrase (AN GUS) or (VON DPN) meaning that the message which follows is to be relayed to GSU, or came from DPN.

As soon as the messages of each day's traffic had been stencilled, copies were furnished to the officers assigned to each code, who kept them in loose-leaf binders. The text was recorded as it came in, by a group of clerks, and inasmuch as the method of indexing and recording was an important preliminary to the study of a code it may be useful to explain it in detail. The writer is pleased to acknowledge his indebtedness to Second Lieutenant D. D. Milliken, Infantry, for a preliminary report on this phase of the work.

RECORDING AND INDEXING THE THREE-LETTER CODE TEXT.

15

I. NECESSITY FOR, AND PURPOSES OF, RECORDING.

In working with the Three-Letter Trench Codes, two requirements in the way of recording the individual groups were immediately apparent.

1. A method by which the following features of each code-group could be referred to readily and made use of:
   a. Frequency of occurrence.
   b. In what messages the group appeared
   c. Its relative position in each message
   d. Whether or not a solution for the group had been found, and if so, what the corresponding clear text was.
2. A means of easy reference, by which any letter, word, phrase, number ~~of~~ or character, could be looked up, and if solutions had been found, the code-group or groups which represented it could be determined.

II. METHODS OF RECORDING.

In meeting the first requirement, a system of charts was used at first, and though it was soon discarded, it will be of interest to describe it.

1. CHARTS. This method, was in use for several months while the codes consisted of groups beginning with the initial letters K, R, or U, and there was a separate chart for each initial letter. The following diagram of the "K Chart" is an example:

16

"K"

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

The chart, being ruled off on a sheet of cross-section, or quadrille-ruled, paper gave 676 small rectangles, one for each of the possible combinations of two letters of the alphabet. It was 26 x 13 inches square, giving a rectangle 1 x ½ inch square for each bigramme.

In recording the group KFA, for example, the initial letter K indicated the "K-Chart"; the second letter, F was taken in the vertical column at the left side of the sheet, and third letter of the group, A, taken in the horizonatl row at the top of the chart. In the diagram ~~on the preceding page~~, the position of the rectangle for recording the KFA groups is shown by the X in the rectangle.

The system of labelling messages in the text made use of a series of alphabets to indicate the consecutive messages, because at this time the pages of text were not numbered. Thus: the first message on the first page of text was indicated AA, the second message AB, the third AC, etc. These letter indications were continued from page

to page until ZZ was reached, when a new combination began using letters A'A, A'B, including Z'Z, after which A''A, A''B, etc., and if necessary A'''A, A'''B, etc., were employed, until the code changed.

For example, the rectangle recording KFA would look somewhat like this:

17

"STATION" (45-14d-8f-95)
AC, DE, FKd, FLd, HJf, KH, LNd, MDf,
PS, RTf, RVd, SA, TK, VB, WCf, WGd,
WH, WJ, WL, WM, WP, A'B, B'Df, C'Kd,
C'L, C'N, D'K, D'Vf, - - - - - - -
- - - - - -A''B, C''Kd.

In the record above, the messages in which KFA have occurred are shown in consecutive order. The lower case letter "d", (the abbreviation of the French word "debut",), after the designation of the message, shows that in the messages FK, FL, etc., KFA is the initial group. Similarly with "f", (abbreviation for "fin"), in the messages HJ, MD, etc., KFA was the final group. The underlining of the message, e.g., RTf, TK, and WH, indicated a recurrence, or the fact that the group occurred twice.

It was customary to send all solutions, as they were discovered, to the French and British. If confirmed, the solution was entered in the rectangle, e.g. "STATION" as shown above. If not confirmed, it was entered nevertheless, but a question mark, indicating that it was doubtful, was placed after it.

The following is the explanation of the figures shown in parenthesis. After a code had run its course the more frequent groups were examined and the total number of occurrences, number of times as initial and as final groups, and number of recurrences, were noted. "(45-14i-8f-9r)" indicates that KFA appeared 45 times, 14 times as the initial group and 8 as the final, and that it recurred in ~~nine~~ 9 messages. A sample of such a chart is attached as Exhibit 2.

2. RECORD BOOKS. Shortly after the appearance of the initial letter S, in addition to K, R, and U, it was decided to use a system of record books, one for each initial letter. Each book contained 13 sheets or 26 pages, one page for each letter of the alphabet, each page being divided into 26 parts, with a line for each letter from A to Z inclusive.

At the same time, the manner of indicating the messages was changed. Each page of stencilled text was numbered, the succesive messages on each page being lettered, beginning at the top of each page with the letter A. Thus: the first message of the text would be indexed in the record books as 1-A, the third would be 1-C, the second message on page two would be 2-B, the third on page 11 would be 11-C, etc.

The method of showing the relative position of the group in the message was radically changed. A circle was drawn with a colored pencil around the number of the message as indexed in the book, the following scheme being employed:

First	----	group	in	the	message	----	Green circle
Second	---	"	"	"	"	----	Blue "
Next to last	"	"	"	"	"	----	Yellow "
Last	----	"	"	"	"	----	Red "

If the group appeared in the interior of the message there would be no circle around the index number. Where a message consisted of only one group, two circles, green and red, one within the other, were used, as the group was both the first and last. In a message of two groups, the first would have two circles, green and yellow, the second having two also, but red and blue. Similarly, in a three group telegram, the first group would be within a green circle, the third, or last, encircled in red, while the second, or middle group had two circles, blue and yellow. Recurrences were indicated by underlining, as in the case of the charts. (Exhibit 3).

In what follows, when the "color of a group" as shown by the indexes is referred to, it is this coloring scheme that is meant. After the occurrences of a frequent group had been recorded, certain inferences could be made from the colors alone.

In fact, the importance of the positional features of code-groups and their frequencies, led to the adoption of what was called the "formula of a group". This was simply a condensed statement of the frequency of each group and the positions it occupied in the text. The significance of each number in the formula was as follows:

19

1st	No.	----	Total frequency					
2nd	"	----	No. of times appearing as initial group					
3rd	"	----	"	"	"	"	"	2nd "
4th	"	----	"	"	"	"	"	next " to last "
5th	"	----	"	"	"	"	"	last "
6th	"	----	"	"	"	"	"	an interior "
7th	"	----	"	"	"	"		It is repeated in messages.

After a short acquaintance with such formulae the code solver could tell at a glance the general characteristics of a group from the formula alone. This was found to be very useful.

When the umlauted letters Ä, Ö and Ü were added, another index book was added to the system, and this was reserved for the groups containing an umlauted letter. In recording such a group, only the second and the third letter were considered in regard to the page, and the line on that page. A certain portion of each line was reserved for similar groups. Thus KFÄ would go on line A, page F, in the portion reserved to K. RFÄ would go on the same line but in a portion reserved to R, etc.

In the actual recording of the telegrams, they were taken in the order in which they were stencilled for text and each group entered from day to day as it occurred. To maintain a check on the entry of the groups and to be sure that none were missed or left out, as each group was entered

or indexed in the books, from the set of text used for recording, a dot was marked in pencil above it.

Where the number of officers and clerks working with a code was large enough to make it necessary, extra sets of books were made up, so that no time be lost. As soon as one day 's text was recorded in one set of books, the clerks were set to work ~~X~~ transferring the records in the other sets.

III. ADVANTAGES AND DISADVANTAGES OF EACH SYSTEM.

1. CHARTS. The advantage of the chart method lay in the fact that all of the groups ~~beginning with the same initial letter~~ were before one at the same time and it was easy to see which was the most frequent. This advantage was more than offset by the numerous disadvantages which this system had.

17

20

a. There was not sufficient space in each of the rectangles, especially if the code happened to run for a longer period than usual; the result was that the indexing overlapped into other rectangles, causing confusion. Furthermore, it was necessary to use very small letters and figures in recording, and this feature was not only hard on the men who did the recording, but made the index very difficult to read, and caused loss of speed both in recording and in the use of the chart.

b. There was no means of showing when the groups appeared as either second or next to last in the messages. This feature was especially desirable in certain codes where the groups in either of these positions had clearly marked characteristics or represented, for example, military units or numbers, or certain frequent words which had characteristic positions.

c. The charts required rather large sheets of paper, about $2\frac{1}{2}$ x ~~40~~ 13 inches in size, and were inconvenient to handle, liable to be torn, and the pencil records blurred after the sheets had been used for a few days.

2. BOOKS. All of the disadvantages of the chart method were eliminated in this system. The books were much more readily handled; also, they lent themselves readily to being used as "decoding parts", after solutions had been found. The only disadvantage of the book system was that the decodor did not have all groups before him at one time, enabling the eye to compare groups at a glance.

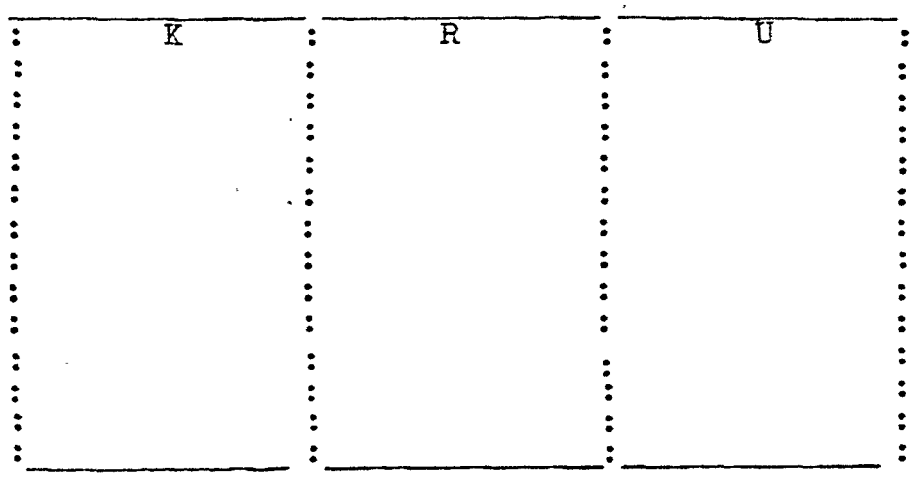
IV. "THE BIBLE".

To meet the second requirement in the way of recording, a book which was termed "The Bible" was used. This was nothing more or less than a stencilled copy of the latest ~~a~~ code-book which had been captured. However, the groups representing the various letters, words, phrases, numbers and characters, were left out, and in their stead dots were placed opposite each of them, corresponding in number to the number of groups used to represent that particular letter, word, phrase, number or character. Then, as solutions were found, they were entered, opposite the clear text which they stood for. If doubtful, or not confirmed, a question mark was placed after the solutions just as in the case of the charts and record books. (Sample, Exhibit 5).

V. "TRIPTICS".

To take the place of a "decoding part", for the purpose of decoding messages after a break had been made in a code, a system of charts called "Triptics" was employed.

Triptics consisted at first of three sheets of cardboard, (one for each of the three letters, K, R, and U), fastened together side by side, so that they could be folded up, somewhat along the following design:



Again, in solving spelling groups the presumption was that a word ~~in the~~ found in the code book would not be spelled out. ~~This however did not always hold.~~

~~The latest code book captured was always used for the "Bible", and since~~ Since one or more code books were usually ~~nearly always~~ captured in major operations, it was nearly ~~nearly~~ always possible to have a "Bible" representing ~~the code closely~~ corresponding closely if not exactly to the code in actual use.

The "Bible" was also an important use as an index of words likely to be found in the code. By practically memorizing its contents, the code solver learns what words to look for. A word which would occur at least once and which would fit in a given place in search through the "Bible" would very often result in a solution. On the other hand a word not found there would probably be rejected unless there was reason to think that the type of code used changed, for the same way the "Bible" served as a guide to the number of groups to be expected for each message the code

22

A sample sheet is attached to this report, as Exhibit 4.

Assuming that a solution for the group KFA had been found, it was then entered on the K sheet of the triptic, in the proper space.

The placing of a question mark after the solution, indicated, as in the case of the charts or record books, that it was doubtful or unconfirmed.

After the use of the initial letters S, and A began, the sheets of the triptics were continued for each letter as before, but they were not fastened together, as it was difficult to handle five sheets conveniently.

Another use of triptics was made when only the encoding half of a code book for one of the codes for which text was available was captured. All of the groups in the code book were entered on a set of triptics and thus could be referred to very readily ~~(Exhibit 7)~~. The same these took the place of the decoding method was also used with the record books. book.

VI. "EXTRACTS".

Aside from the systems referred to above, a means of studying the characteristics of the more frequent groups and the groups which preceded or followed them in the various messages in which they occurred, without having to run through all the text, was deemed advisable. The plan of making "extracts" of telegrams in which these groups appeared, was adopted.

As soon as sufficient text had been stencilled and indexed the frequent groups, (that is those which had appeared five or more times), were taken, and extracts made. These were kept up to date by adding to them each day as new text became available.

A typical extract is shown herewith. ~~in Exhibit 8.~~

EXPLANATION:

The number of the messages was placed at the left edge of the page, and the group "extracted" in the center of the page. Groups which preceded and followed were written in their proper positions. The asterisk (*) indicated the beginning and end of the message. If alternate groups were given in the text they were placed underneath the groups for which they were alternates.

EXTRACT OF GROUP "KME"

REF ID:A2458117

ALBERT CODE NO. 17 — Start August 22, 1918.

4H-14:00				*RRT RAE	AFM KFM	KME	UDF	SZG ULG	UUF	SRT	UYS	UAJ SAJ	
6A-13:32			*RLN	KWH	UPH	KME	---	---	RPZ	ROC	ADC	AWF*	
6J-17:45	RGD	UIM	ANL	SAZ	ASQ	KME	ABT	SGA	KUD	SYG	RBT	AZS	
11H-18:25	AKJ	RCC	RKO	UKO KGO	AGF	KNE KME	UAP*						
12C-10:42	REV	STE UTE	UKR	AVH UVH	ASQ	KME	KRG	AHZ	RDT	RBT	RXB	AJD* RJD	
16B-08:55	*UBJ	RDH	RNI	AVJ	RHG RHQ	KME	UNM UDM	RBT	ACO*				
20D-15:30					*	KME	RYS	UXD	SRZ	KOD	AYM	KOD	KXS
20E-15:30	USJ	AXJ	KOM	RWC	AMD	KME	KOD	UXD	RLZ	APZ	RBA	AEM	
20F-15:30		*SOM SOK	SNY	AYH AOH	SIW	KME	RYS RIS	RLZ SLZ	HKZ SKZ	SWA	SNY SMY	KOD	
21A-15:30					*	KME	UXD KXD	AXV	UKZ	SFD	REC	UKD	
21A-15:30	UZA	KLN	AKB	RSU	RPU	KME	RYS	SGA	SRZ	KOD	USC	ADR	
21E-18:55					*	KME	UXD	AXV	UKZ	SFD	REC	UYD	
25H.					*	KME	UXD	ADU	ASK	SFC	SWV	UBS	
47G.11,15	UGJ	AQW	AEL	RJV	SWF	KME	UEJ	KDB	RKZ	RKA	RGV	AAW	RVE
54F.17.45	RGD	UIM	ANL	SAZ	ASQ	KME	ABT	SGA	KUD	SYG	RBT	AYS	AUD*
56L- 03.05					"SDV SDN	UMZZ KME	UAD UAH	SWF	UTT	UVY	RPH	URW	UYF
67K- 16.27	"RDT	STE	UWN	RBB	USN	KME	ABT	SAZ	RDE	RZZ	SGA	AJD"	
69C- 21.00			"AJD	REI		KME	KDB	AQI	RGR	KXJ	KLN	RXK	
69C-21.00			*AJD	REI		KME	KDB	AQI	RGR	KXJ	KLN	RXK	
78B-14.00	RRK	ADC	RXU	RDS	UGR	KME	KYE	AQI*					
80F-11.15	UGJ	AQW	AER	RJV	SWF	KME	UEJ	KDE	RHZ	RKA	RGV	AAW	
80L-09.42					*RZI	KME	AFD	RGH	USN	AXU	AYH	APV	
85F-18.21					*AOD	KME UME	RHQ	SRZ	PKD RUD	RTO	RUS	UJD	
102K21.00				*AJD	REI	KME	KDB	AQI AQM	RGR	KXJ	KLN	RXU	

EXHIBIT 8

HEADQUARTERS AMERICAN EXPEDITIONARY FORCES.

FRITZ NO. 14. JAN. 24, 1918.

A. FROIDOS 16.00 600m BW v R4

17.45 GR-13 UZM RLA KKI UMM RIN ROP KKI UMM RIN KKI KOV RIN KWQ R4 UM

B. LANDRECOURT 16.00 600m WQ v MP

16.45 CHI-13 UER UEK RBR KKB KMO RTC ROV ROB RIJ RIC UMN KOY KDE NF MP

C. FROIDOS 16.03 600m 8B v GA

16.40 ZI-7 RLH UXS UAS UUD KFQ UFT UJP KJJ GA UM

D. FROIDOS 16.06 600m 8B v CZ

ZI-6 KMB RDS UQC KOR UTS UCO (or UCS) MF CZ UM

E. LANDRECOURT 16.18 600m -- v VC

11-GR UOK UQL KPR KQL KDU RET UNT REP UTW KJC KBV VC UM

F. LANDRECOURT 16.10 600m D4 v HF

17-GR RJP --- RQO KPC RNC KID UJU RLL KNT RRF KWI RWH UMM KSQ KVB --- --N HF UM

G. LANDRECOURT 16.12 600m 8B v GA

16.40 ZI-7 RZH UXS (or UPS) UAS UUD KFQ UFT KJP GA UM

H. LANDRECOURT 16.16 600m 8B v CZ

ZI-6 KMB RDS UQC KOR UTS UCO CZ UM

I. FROIDOS 16.15 600m OE v 5Ä

17.20 CHI-18 KQZ --- KAM KCX --- UKO RFJ RTZ RQU UWH KSN UKS (or UKH) UTT KQN UKH ULY (or URY) RLL REA --- UAT REU --- 5Ä UM

23

Groups which appeared more than once in the extracts were underlined in colored pencil, a different color being used for each separate group which so occurred. In the extracts shown in the exhibit several groups are underlined in such a manner. This work was done by clerks. It was found important to keep the extracts always up-to-date.

METHODS OF SOLVING THE THREE-LETTER CODE

We will consider first the Three-Letter Code, beginning with its original or simplest form and following it in the development to the most complex, noting the first methods of solution, and the improvements in those methods which were necessitated by the development in complexity of the code.

At the outset it must be stated that this development proceeded simultaneously with the advances made in the various methods of "camouflaging liaison", a subject which would require a long, detailed report in itself, but which is treated briefly subsequently (see Pages--) and also in the report of the Goniometric Department.

(79)

The date on which the very first messages in code were sent on the Western Front marked the beginning of a new era in cryptography as far as the use of secret means of communication in warfare are concerned. Up until this time cipher had been used almost exclusively, and much information had been secured therefrom. But with the sudden introduction of code as a means of daily communication on the battle front, approximately January 1917, new problems, and apparently grave ones, presented themselves to the experts in the code offices of the Allies. Heretofore, while it is true that methods of solving the ordinary, small, dictionary-type of code, wherein each code group represents a whole word, no more and no less, and where these words follow each other in alphabetical sequence (the simplest form of type 1, page --) were known, still the solution of a code message set up by means of a code-book wherein a single group may represent a letter, syllable, group of letters, word, phrase or even an entire sentence was regarded as extremely difficult, if not impossible.

(9)

24 It was not long, however, before these messages were being read, either in part of completely. There is no doubt but that two of the factors which were of the greatest assistance in giving the clues leading tothe discovery of these methods were first, the general lack of knowledge of the weak~~esses~~points of code as a system of secret communication, and second, the methodicalness and the almost slavish adherence to set form, that is characteristic of the German mind.

The German Three-Letter Code, which they called the SATZBUCH (literally, sentence-book) was a comparatively small code, specialized to meet the requirements of the field; i.e., either positional or open warfare. ~~(Exhibit 9)~~.

(3) As stated above, this code, as shown in the chart discussed on page --, was not supposed to be taken within three kilometers of the front line trenches, the danger zone, and therefore it was not available for infantry battalions in line, trench mortar batteries, artillery observers, forward intelligence and liaison officers and the like. The code designations took the form of combinations of three letters of which the initial letter was one of a limited number of letters, the other two being any letters of the alphabet. In the first codes, these initial letters were K, R, or U. Later the letters S and A were added, as further groups were made a portion of the code. With three initial letters, the total number of code groups possible equals 3 x ~~28~~ 26 x 26, or 2028 groups; with five initial letters it is 5 x 26 x 26, or 3380 groups. The last development was the inclusion of the three umlauted letters Ä, Ö, and Ü, for the second and third letters of groups, making the total possible number 5 x 29 x 29 or ~~3389~~ 4205 groups. In setting up a new edition, not all of these possible groups were used, as many places were left to be filled in at Army Headquarters for the names of towns, code names of units, artillery groups, observation posts, etc., at the discretion of the particular units concerned.

The SATZBUCH was based, as stated above, upon the two-part type, and therefore consisted of a VERZIFFERUNGSBUCH, or the encoding book, and an ENTZIFFERUNGSBUCH, or the decoding book.

25

25

The encoding book was prefaced by some general remarks and precautions to be taken, and it will be interesting to read them, then to compare the early editions with the last in regard to these instructions. The following is a translation of these instructions given in a code-book captured in the fall of 1917:

TRANSLATION

TO BE READ BEFORE USING THE BOOK.

PRELIMINARY REMARKS.

1. All reports and orders must be encoded by means of the code-book. Clear text may be sent by wireless only in case of extreme necessity. The mixing of clear text and code text is prohibited.
2. The code-book consists of an encoding book and a decoding book, and contains three-letter groups of which the first letter is K, R or U.

   a) the encoding book is composed of the following parts:

   IMPORTANT REPORTS
   GENERAL REPORTS
   STATION AND SERVICE REPORTS
   MILITARY NAMES
   PLACE NAMES
   NUMBERS
   PUNCTUATION
   LETTERS AND SYLLABLES
   AUXILIARY SIGNALS AND BLIND SIGNALS
   VOCABULARY

After each part, as well as in the vocabulary, space has been left for the insertion by hand of supplements.

Military names (Staffs, Formations) and Place names must be inserted by the Wireless Detachment itself according to its needs, and must be provided with code groups.

The groups which have been provided for these supplements are to be taken from the decoding book.

The Auxiliary Signals are placed immediately after the groups whose meaning is to be changed. For example, if it is desired to encode ANGEFORDERT, the signal MITTELWORT DER VERGANGENHEIT is placed after the group for ANFORDERN; thus:

26

RGS RMR

The Auxiliary Signals will be used only when necessary in order to avoid an error.

The Blind Signals must be inserted at random in very frequent, recurring, similar or stereotyped reports and orders.

In decoding they are simply disregarded.

The vocabulary is arranged alphabetically; Ä, Ö and Ü are treated as A, O, and U. In adjectives, the group for the uninflected form applies also for the inflected forms; for example, the group for GROSS applies equally for GROSSE, GROSSER, GROSSES, etc. The group for DIESER applies likewise for DIESE, DIESES, DIESEM, DIESEN. The group for the infinitive applies also for the other forms of the present tense; for example, ABFLAUEN, for FLAUT AB; NEHMEN for NIMMT. Compound verbs are arranged alphabetically under the preposition; for example, FLAUT AB, under ABFLAUEN, GREIFT AN under ANGREIFEN. Reflexive verbs are to be sought under the verb; for example, SICH AUSDEHNEN, under AUSDEHNEN, SICH; SICH EIN GRABEN, under EINGRABEN, SICH. Phrases such as AUF DEM RECHTEN FLÜGEL , UNTER FEUER NEHMEN, EIGENE ARTILLERIE, HAT AUFGEHÖRT, ZU SPÄT are inserted once alphabetically under their first word (AUF, UNTER, EIGENE, HAT, ZU), and then also under the succeeding noun, verb, etd. (FLÜGEL, FEUER, ARTILLERIE, AUFHÖREN, SPÄT). In a similar manner the frequently recurring forms of the auxiliary verbs and verbs such as IST, WAR, WIRD, KANN, GENOMMEN are to be found once under these forms and then also under the infinitive to which they belong (SEIN, WERDEN, KÖNNEN, NEHMEN).

For the spelling of words and names which are not contained in the code-book, individual letters, double-letters, and syllables are set forth under the section LETTERS AND SYLLABLES.

26

27

If there are several code-groups for a word or a group of words, these groups must be chosen at random.

b. The decoding book contains first the three-letter groups with the initial letter K, then those with the initial letter R, and finally those with the initial letter U.

3. In a CHANGE IN CODE-GROUPS it is necessary to pay particular attention that:

1) The change is made in the encoding and in the decoding book.

2) Those groups, whose significance appears in several places (see above: AUF DEM RECHTEN FLUEGEL, UNTER FEUER NEHMEN, ZU SPÄT, IST, WAR, KANN, etc.), are changed in all the places.

For simplifying this work, these groups whenever they appear twice, are indicated with an asterisk.

The first edition of the Three-Letter Code was really very simple compared with the latest. But since it will be impossible to give a clear idea of the methods of solving the more complex types without first giving a detailed exposition of the methods by means of which it was possible to solve the simple types, we will proceed first to discuss in detail the solution of what we shall call the KRU Codes, a name derived from the fact that the early editions employed as initial letters only K, R, and U. Then we will take up, step by step, the evolution through which these codes and the methods for their reconstruction passed, until finally the KRUSA Codes came into use and represented the most developed type.

Serious work on the code began only after a fair amount of text had accumulated and been recorded. For the first day or two, therefore, it was necessary to examine the messages with a view to familiarizing oneself with the new code groups. Too much stress cannot be laid upon the importance of training the eye and the memory in this regard. A man with a poor memory will never make a code expert, for he must be able to recognize groups, or sets of groups at a glance; and he must be able to keep in mind the relative positions occupied by these gouprs, so that as soon as his

eye meets them in new messages it calls up at once the various theories which he has formed with respect to the groups in question; and the juxtaposition of groups which he recognizes in new positions must be consistent with the theories he has formed previously concerning them.

K-R-U-CODES

In a code of the type to be discussed, the whole of the text was divided into six main parts, or sets of groups, which, although they were very closely inter-related, really had to be attacked separately. If even only a few solutions were found in each of these sets, these solutions enabled us ultimately to rebuild or reconstruct the code either completely, or at least sufficiently so to be of value. These sets of groups, all having their own peculiarities and characteristics by means of which they were susceptible of being discovered were as follows:

(1) NUMBERS
(2) WORDS AND PHRASES
(3) SPELLING GROUPS
(4) AUXILIARY SIGNALS
(5) PUNCTUATION
(6) BLIND GROUPS

The analysis which ultimately led to the individual solutions for the members of these groups, went through two stages, a proper and thorough understanding of which is absolutely essential. They were:

(1) CLASSIFICATION
(2) IDENTIFICATION

When the code solver first began his study of the text, he was confronted with a body of completely unintelligible "sentences" to which he had to apply various tests more or less equivalent to the reagents of chemical analysis. By means of these tests he was enabled to break up the text into these six main sets of groups of which the code text was composed, as stated above. This, then, is what is meant by the process of classification. After this, the identification, of the individual members of each set followed by a

29

different series of tests. In a word, the process was somewhat analogous to that in qualitative analysis; first, the chemist applies tests by means of which he breaks up a complex substance into its several classes, then he proceeds, by another series of ~~facts~~ tests to identify the members in each class. When classification had proceeded upon a solid foundation far enough, each set of groups was indicated in some distinctive manner. For example, spelling groups were underlined in green pencil; numbers, in red; words, in purple; military units were set off by a red square; etc. In case of doubt, such underlining or blocking-out was made by dotted, instead of continuous, lines. This had the result of setting forth clearly to the eye the parts of which each message was composed and was of the greatest aid in solution. Immediately after an identification had been made, the solution was written above the group each time it occurred. This was absolutely essential.

The two processes mentioned above will be referred to subsequently strictly in accordance with these definitions.

The principles by means of which these two steps in solution were accomplished were based directly upon the characteristics of these main classes resulting from the uses to which they were put. Only after an opening had been made into all of these six categories had there been built up a sure foundation for the complete solution of the code. We will therefore proceed to give them somewhat in detail.

Before proceeding, several definitions will be necessary.

Certain groups will often be designated as either STATIONARY or MOBILE. That is, certain groups remained unchanged either in form or position, while their accompanying groups varied in these two respects. For example, Military Units formed a set of stationary groups with numbers as mobile groups. That is the group standing for the word Regiment, when used in connection with numbers, remained constant or stationary, while the groups standing for numbers changed, or were mobile or varied. The words VON, FIS and UHR formed another set of stationary groups with numbers as the mobile groups.

29
30

Repetitions of two code groups, in the same order, are called BIGRAPHS; of three groups, TRIGRAPHS; of more than three, POLYGRAPHS.

THE USES AND CHARACTERISTICS OF THE MAIN CLASSES OF CODE GROUPS

I. NUMBERS.

A. Uses.

1. In designating Military Units. In referring to the various units, numbers naturally play a great part.
2. In giving dates and the hours of the day.
3. In giving "CHI" and"ZI" numbers. It was a usual custom to refer to messages according to thenumber of groups as given in the preamble to the message referred to; for example: "CHI 37 NICHT VERSTANDEN". Another way of referring to messages was to give the time stated in the preamble of the message referred to; for example: "CHI 1825 ERLEDIGT".
4. In giving the coordinates of a map square, or, as the Germans call it PLANQUADRAT; for example: "40 SCHUESSE AUF PLANQUADRAT 4425". In referring to points on a map; for example: "KARTENPUNKT A8".
5. In tabulated reports wherein the separate subheadings were referred to by consecutive numbers.
6. In setting forth number of shots, and casualties; requesting supplies, accessories, etc.

B. CHARACTERISTICS.

1. These groups were very frequent, numbers 1 and 2 being among the most frequent groups in the text.
2. These groups were found in connection with a set of groups which already had been classified as MILITARY UNITS.

Note: It should be borne in mind that the mental process which accompanied classification did not attempt to take up one of these sets of groups at a time and isolate that, for this impossible. In fact it may be said that the process of classification proceeded with respect to all the sets of groups more or less simultaneously.

3. These groups appeared frequently in sets of two's, three's and four's; rarely, in chains of more than four, the latter being occasioned infrequently by certain types of weather reports to be discussed later.

4. These chains showed extreme diversity in the arrangement of permutations of the constituent groups, i.e., there was no regularity of sequence of groups in such chains. For example, if A, B, C, D, E, F, G, H, represent a set of these frequent groups which conform to the first three principles enumerated above, they might have shown the following sequences in the various chains where they occurred:

AB; BA; BC; FA; EB; HA; etc.

ABC; CAF; GHA; DEF; GBD; etc.

ABCD; BAFE; EGFA; DFAC; etc.

The reason for stating that a chain of more than four of such suspected groups was rarely to be found is, of course, that the occasions for giving a number beyond four places was rather uncommon in these codes, except in weather reports as mentioned above; whereas in the case of spelling groups which also appeared in chains (see below), the proportion of long to short chains was the reverse of that in the case of numbers, since most words that had to be spelled out required several groups as a rule.

C. CLASSIFICATION AND IDENTIFICATION.

Having found some Military Units, a study of their extracts was made, with a view to classifying numbers, which were found to behave as mobile groups in connection with these military units, the stationary groups. Note the following extracts of two groups classified as Military Units:

21

32

Get all of these extracts on next page

		*RRC	RBK	KCB	UFP	RIO	KNT
	UAX	UUN	RBK	KCB	KPF	KNT*	
	*RRC	UVX	RBK	RIO	KPF	RCC	RIP
			RBK	KKN	RIO		
*RVL	RNV	ROP	RBK	UCQ	KCB	UON	UVK	KKX

			*RRC	RBK	UFP	KKN	KXX	UUO	UOK
			KOJ	RBK	KPF	KCB	KCB	KEA	
		*RRC	UVX	RBK	UFP	RIO	UFP	RZP	
	RYY	RCP	KNM	KII	RBK	KKN	UCQ	KNT*	
	*RRC	KCB	KKN	RIO	UXU	UOK	KUS	KTA	
UKS	UVV	KCB	KCB	KPF	UXU	KAE	KVD	RDS	RIB*
		*RRC	RIO	UCQ	UXU	RBB	UBQ		
	RYI	ROY	KPF	KCB	UXU	KNT*			
RSP	UXT	KCB	RIO	RIO	UXU	KNL	RLZ		
		*RRC	UCQ	KPF	UXU	RYY	UNA	UAM	

face

Note the behavior of the groups which have been underlined. In the first set of extracts these groups follow the stationary group RBK; in the secont set, they precede the stationary group UXU. If these mobile groups are numbers, and ~~so far,~~ we will assume that the evidence is good that this is the case, then their behavior with the stationary groups RBX and UXU is quite in accordance with the German method of designating the military units, REGIMENT and DIVISION, respectively; in the case of the former, the numbers follow; in the case of the latter, the numbers precede. In the case of ~~BATTALION,~~ BATAILLON the numbers follow; in the case of BRIGADE and KOMPAGNIE, the numbers precede. Of all of these Military Units, DIVISION and REGIMENT were by far the most frequent.

Having thus classified a few numbers, they were underlined in red throughout the text, and in a short time further study of the messages in which they occurred, and of the groups which preceded and followed them disclosed more numbers, and gradually, the classification process had isolated all of the important ones. For example, if an unclassified group was found between two red-underlined groups (already classified as numbers) the unknown group was traced throughout the text. If it behaved as a number, for example, if it was found in connection with Military Units, etc., the chances were it was a number also. It was underlined, and the process continued.

The process of identification then followed, by a detailed study of all the messages in which these groups occurred. If one were fortunate enough to find one or more long messages in the nature of reports, a careful study of such messages often disclosed the whole series of numbers from 1 to 10 (see sample stereotyped message on page --). (51) The numbers 1 and 2 were the most frequent, and they were identified often on the basis of frequency alone. By a study of the German "Order of Battle" Map, the "Daily Field Station List" and a reference to the two volumes "Index of the German Forces in the Field" further identification or confirmations were secured. For example, if the map showed in a given locality the following divisions:

251, 52, 121

and the aforementioned books, or the "Daily Field Station List" showed the following regiments, as parts of the divisions named:

251st Division	52d Division	121st Division
Regiment 73	Regiment 192	Regiment 243
" 129	" 71	" 96
" 37	" 42	" 56

almost positive identifications in the following cases may be made:

	RIO	UPF	UXU	:	RBK	UCQ	UPF		:	RBK	UPF	UCQ	KPF
UPF	RIO	KCB	UXU	:	RBK	KCB	RVR	UPF	:	RBK	RVR	UUA	
KCB	UPF	KCP	UXU	:	RBK	KCB	UPF	RVR	:	RBK	RIO	UUA	

II. SPELLING GROUPS.

cases → a. Uses.

1. It is obvious that the chief use of these groups was to spell out words which did not exist in the code book. Hence, when used at all, the majority of cases necessitated the use of a whole chain of spelling groups. However, in practice messages, many words were spelled out which really did exist in the code book, although rules are strictly against it.

13

34

2. Certain letters were very frequently used in abbreviations. Among the most frequent of these were the following:

K.T.K. (KOMMANDEUR DER KAMPF-TRUPPEN)

R.I.R. (RESERVE INFANTRIE REGIMENT)

R.I.D. (RESERVE INFANTRIE DIVISION)

L., LW., LD. (LANDWEHR)

A.V.O. (ARTILLERIE VERBINDUNGS OFFIZIER)

3. Certain letters were used as sub-indicators; examples,

PLANQUADRAT 4452 A3; KARTENPUNKT M3.

4. Single letters and combinations of single letters were frequently used in giving the call-sign of stations. Sometimes a call consisted of two letters, sometimes of a letter and a number (See ~~Section ——~~ Page 61). These were often of very great assistance in establishing tentative values and in finding new ones. For example, given a message in which the word STATION had been already identified, followed by two letters of which one is already known, the other letter identification could be made immediately by finding the call of the station concerned.

There are certain of these spelling groups which were used as words. The most important of these were the following:

AB	BIS	DES	ER	GEGEM	MIT	UNTER
AM	DA	DIE	ES	IM	NACH	VOR
AN	DEM	DURCH	FUER	IN	UBER	WIE
AUF	DER	EIN		IST	UM	ZU
AUS						
BEI						

The possibility of using these syllables as words resulted in the finding of messages in which a supposed spelling group occurred "isolated" and not in a chain of such groups. The point to be emphasized is the fact that the classification procedure as regards spelling groups consisted in the gradual building up of these chains, a process which was of the highest importance in breaking into a new code.

The method of building up these chains was as follows: Having classified a few of the most frequent groups as spelling groups, from color in the indexes, position, use in abbreviations, etc., they were underlined throughout the text in green. Suppose

35

that one or two unclassified groups were found between two green groups; these unknown groups were followed throughout the text, to see if they could be spelling groups, bearing in mind all of the characteristics of spelling grojps as outlined below. If they were found to behave in accordance with expectation, they were underlined green likewise. The process was continued in the same manner until many complete chains had been built up. It will also be recalled that spelling groups were occasionally used in connection with numbers and some in connection with military units. Therefore, the discovery of certain tentative spelling groups in the vicinity of such numbers or military units was of great assistance in the final identification of such letters.

The reader will understand by this time, if he has carefully examined the construction of these codes, and has considered the uses named above that the principles of the frequency of occurrence of individual letters in clear text, as applied to the solution of cipher, could not have been applied in the solution of these codes, without certain modifications, due to the causes which may be summarized as follows:

1) The use of syllables containing the most frequent combinations of single letters.
2) The frequent use of certain letters not in connection with the spelling of words; as abbreviations, sub-indicators, station calls, etc.
3) The use of certain syllables as words. Note those given above.
4) (The assignment of more than one value to the most frequently used single letters, and syllables. This applies only to the later codes).

The result of these causes is that certain single letters which are only of medium or low frequency in German clear text rose to a high frequency in these codes. These letters were B,D,F,G,H,K, L,M,P,W,Z. Single letters such as E, N, and I, which are always the highest in frequency in ordinary German text, were among the less frequent groups because they were incorporated in so many syllables,

each represented by a single group; and because each time there occurred syllables such as AD, AC, etc., i.e., combinations for which there were no spelling groups, etc., the individual letters had to be used, and hence these consonants mentioned above rose to a fairly high frequency.

B. The characteristics of spelling groups were therefore as follows:

1) Some of them were very frequent.

2) They were found in chains as a rule.

3) The sequences in these chains were very much more regular in nature than sequences of chains of numbers. The formation or construction of words of a language entails the building up of a chain of letters in a definite sequence; Long words are usually composed of the parts of shorter ones. The most frequently used syllables of a language will therefore follow each other in more or less definite sequences. The result of this condition is that spelling groups in these codes were found in chains of 4, 5, 6, or more groups, often in the same order, sometimes in minor variations of a given order; but these variations were nowhere so irregular and haphazard as was the case with numbers. This characteristic formed the basis of an important test by means of which spelling groups were classified as distinct from numbers, though, of course, such a test was never absolute, merely, relative in nature.

4. Whereas numbers were found in very short messages, spelling groups as a rule, except those which were used as abbreviations, were not found in short messages. Again, messages rarely began with a word that had to be spelled out. Also there are certain letters in every language which are rarely used as initial letters, others, rarely as final letters. The result of these conditions was that most of the spelling groups were of necessity restricted to the interior of messages; and the consequence of this condition was that the majority of spelling groups showed no color or little color in the indexes. It is true, however,

that certain of the very frequent spelling groups, such as R, D, etc., which were used as abbreviations in connection with Military Units, showed some color but always less color than was the case in numbers.

C. CLASSIFICATION AND IDENTIFICATION.

No definite procedure can be outlined as exemplifying the steps used in making the first break into the spelling groups, for here is really where the ingenuity, patience, and good-fortune, of the code-solver comes most into play. As a rule, in the early codes the first steps were to find the PUNKTS (to be discussed later) and they would almost invariably lead to the classification and identification of some of the most frequent letters such as R, I, D, L, K, and T. The coloring of the groups as shown by the indexes was a great aid in first classification. Following through several such groups and anderlining them in colored pencil as indicated above resulted in the building up of spelling group chains. ~~Repetition of code groups and underlining them in colored pencil as indicated above resulted in the building up of spelling group chains.~~ Repetition of code groups within chains was of course a great aid in assigning tentative values. In subsequent pages several actual cases will be given. Once having solved a few groups the values were immediately filled out wherever the groups in question appeared. Juxtaposition and new arrangements of them led to the solution of additional groups ~~in a somewhat like~~ in an endless chain until finally all or nearly all the spelling groups ~~are~~ were solved.

It should be added that in this whole process the part played by chance, by the happy coincidences which were always lurking everywhere for the watchful eye of the worker to note, by the mistakes of a foolish or a careless encoder, and by a fortunate "long shot" or guess by the decoder cannot be overestimated. Often the minutest and most insignificant of clues formed the starting point for the unravelling of a whole chain of groups. Later one or two examples will be shown.

37

III. WORDS AND PHRASES.

There are certain words that could be classified so easily that they were among the very first to yield to solution. These words may be classified into these four main sets:

1. Military Units
2. Interrogatives
3. Certain prepositions
4. Most commonly used words not included in the above

The characteristics of each of these classes were as follows:

1) Military Units.

a. These were naturally among the most frequent groups in the code.

b. On account of the common custom of beginning a message by addressing the unit to which the dispatch is sent, and ending it by the signature of the unit from which it is sent, these groups were among the most highly colored groups in the indexes, if not actually the most colored.

c. These groups were accompanied very frequently by numbers. It is important to note the standard form of giving Military-Unit designations in German. (See page--)

It was enough on first classification merely to designate the group as a military unit and draw a red square around it; later, from other sources the actual identification of the military unit, i.e., whether it was "division", "brigade", "battalion", "regiment", etc., followed. Such sources were either external, furnished by goniometric data, or internal, derived from a study of the messages themselves, the numbers identified together with their positions (see page--), and by reference to the map giving the German Order of Battle. For example, it was possible from goniometric data alone to determine from a study of the sending and receiving stations the higher and the lower units. A divisional station was usually further back, and was the receiver of reports from the battalion or regimental stations, which were more scattered and nearer the front.

2) Interrogatives: WO, WIE, WAS, WARUM.

a. These were of medium frequency.

b. They showed the predominant color green, then blue, in the indexes; rarely yellow, and never red.

c. They occurred in short messages, in the nature of questions. A great aid in determining the latter was to study the messages from the standpoint of time of sending, and the stations concerned. Note these two messages:

RX v P2 Chi-5 0830

KAB RUA UAB RIC KNB

P2 v RX Chi-2 0835

UAB RTF

It is not hard to imagine that these two stations have exchanged "question and answer". On account of the importance of locating these interrogatives, all the messages of each day were studied and "question and answer" messages indicated. A careful examination of all such messages soon disclosed many important groups. Classification of the interrogatives almost immediately led to the identification of the verb IST, which was of very great importance. Consider thefollowing messages, arranged in the form of an extract of the group KNB; the final group in five of them:

WO	IST	REGT.	1	3	5	=?=
*RTF	RUA	UAA	KRI	UFS	UTS	KNB*
		WIE	IST	LAGE	DORT	=?=
		*KAB	RUA	UAB	RIC	KNB
*AN	W	EN	IST	FUNKSP.	0	7	2	5	=?=
*RCX	KOP	KZR	RUA	RYP	UPX	KVU	KIL	UTS	KNB*
			IST	P	0	ST	DORT	=?=	
			*RUA	UXR	RRU	RVI	RIC	KNB*	
			W	ER	IST	STA-TION	P	2	=?=	UN	BE-KANNT
			*KOP	ROO	RUA	KZK	RNO	KIL	KNB	KAO	RSV*
IST	ABEND	MELDUNG	UNTER	WEG	=?=	SOFORT	ANTWORT				
*RUA	KKR	RIL	UUO	ULT	KNB	RZK	RVV*				
WO	BLEIBEN	GEGWT.	MORGEN	MELD.	=?=						
*RTF	RFF	UFX	UXP	RIL	KNB*						

(These messages must link up in KNB as the contacted group)

Note that the verb IST often came second in a short message preceded by an interrogative, and often first in a short message ending with an interrogation point. In short, the interrogatives WO, WIE, WAS, WARUM, were found to be bound up very closely with the verb IST and its various allied forms SIND, WAR, SEID, etc.

Once having classified the interrogatives, the identification of WO, and WIE were made rather easily by reference to the colors in the index and a study of the position occupied by the groups representing these suspected interrogatives. In German the interrogative WIE can also be used in the sense that our word "as" is used and hence this word was found in the interior of messages having nothing to do with questions; on the other hand, the interrogative WO is rarely used except in questions. The result, therefore, was that the group representing WIE was usually somewhat higher in frequency and showed less green and blue color in the index than did the group WO, which was almost invariably green.

These "questions and answers" were veritable mines of information because they led to the classification and identification of some of the commonest nouns and verbs. Questions as a rule were found to assume a stereotyped form, such as those given on page---, which are typical.

(38)

3). Prepositions.

The most important prepositions AN, VON, BIS, ZWISCHEN, and AUF, will be considered only, because of the important chains which they initiated, and because they were usually among the first identifications made.

a. AN

Of all the code groups, this was usually among the easiest to classify and to identify, because of the constancy of its position: very frequently the first word in a message. By looking through the index the predominant color, green was usually so apparent, and the phenomena exhibited by the groups which followed it, (Military Units with numbers either in front of it or after it, ~~see page 4~~) were so clear that it was noticed very quickly. Furthermore, it could never end a message, and could rarely come near the end, say second or third from the end, except in such comparatively rare cases as messages concluding with "...ANTWORT AN REGIMENT".

40
71

In addition to its importance as a preposition, the syllable

AN was found to be a very important spelling group. Once having located the AN, this group was found sometimes in a chain of say five spelling groups; an important clue to the whole word was of course furnished by the syllable, AN. It was frequently found in words such as LAND, KRANK, MANNSCHAFT, ANRUFEN, DANK, etc.

It was also of great importance in classifying Military Units and such words as STATION, GRUPPE, etc. Often a message intended for several stations began thus: AN ALLE STATION-EN. Notice that the important word ALLE, and the very frequent spelling group EN were very apparent there.

b). VON, BIS and ZWISCHEN.

These three prepositions were usually so closely bound up with the word UHR, and with numbers, that they may be said to have formed a more or less definite set of groups, which were solved simultaneously. Consider the following series of messages arranged in the form of an extract of what may be called the STATIONARY GROUP, SHA, because it is always surrounded by groups which change around, or are MOBILE. ~~The groups which are underlined have already been classified as numbers, and we are now trying to locate these prepositions.~~

A	RRU	KII	SVB	ALU	SHA	SJB	UAY	UID	
					SHA	SJB			
B	RSP	UNS	RPS	UZF	SHA	UAS	KWN		
					SHA	SSK	RIO		
C	RPS	SYN	UAE	AMB	SHA	UAY	RPS	AMB	
					SHA	UKN			
		UAY	RPS	AMB	SHA	SBW	UNT	KUU	SNT	UNS
D	SVB	UID	UAY	SYN	SHA	KKS	RVI	AST	SSI	KKI
E		KII	RPS	ALU	SHA	AWJ	UAE	UID		
					SHA	AWJ				
F		ROI	RPS	SWV	SHA	~~KOW~~	KKS	SIT	AHS	SIN
G		RIC	SVB	KWN	SHA	SJB	UAY	ALU	AWJ	KIP
H		RXO	RPS	UID	SHA	SSK	UNR	STP	AXF	UIT

41

42

Note the group RPS which so often precedes the MOBILE groups; and also the group SVB, which is often found preceding the group SHA with one or two intervening mobile groups. It does not take much imagination to see that we have here the prepositions VON, BIS, and ZWISCHEN, together with the word UHR and numbers, in accordance with the usual formula of giving time in German:

"VON 2 UHR 30 BIS 3 UHR 45"

"VON 3 BIS 5 UHR"

"VON 3 UHR 15 BIS 4 UHR UND VON 5 UHR 25 BIS 6 UHR"

"ZWISCHEN 6 UHR 30 UND 7 UHR"

c) AUF.

This preposition was often located in the following type of phrases, which were of rather frequent occurrence:

"ANTWORT AUF FUNKSPRUCH 1725"

"50 SCHUESSE AUF PLANQUADRAT 4215"

In other words the two stationary groups preceding sets of four mobile groups which had been classified as numbers, were studied with a view to ascertain whether they were not the commonly used words given above, preceded by the preposition AUF.

4) Very frequently used words not included in the preceding. Among these were the following:

MORGEN	LINKS	HIER	SONST
ABEND	SENDEN	HEUTE	GESTERN
NACHT	EMPFANGEN	NACH	KOMMEN
MELDUNG	SOFORT	NICHT	HABEN
LAGE	MANN	UND	SCHICKEN
RECHTS	AKKUMULATOR	NEU	ERHALTEN

The words MORGEN, and ABEND, formed a set of alternate groups with the word MELDUNG, because of the frequent occurrence of messages beginning MORGEN MELDUNG or ABEND MELDUNG. Often a tentative interrogative WO and the interrogation point were confirmed by finding a message such as the following:

WO BLEIBEN GEGENWART ABEND MELDUNG?

42

43

RECHTS and LINKS formed another set of alternate groups with such words as REGIMENT, KTK, ABSCHNITT. This was best determined by noting the bigraphs throughout the text, especially those obviously connected with groups which had been classified as military units.

The word LAGE was a very frequent one in short messages such as WIE IST LAGE DORT? Often the answer comes back somewhat in this form: LAGE UNVERAENDERT, or HIER NICHT-S NEUES. It is now clear why the classification and identification of the interrogatives and the interrogation point were so important because they led to the identification of so many common words.

The important verbs SENDEN, EMPFANGEN , and SCHICKEN were often easily identified in such stereotyped messages as the following:

"2 CHI EMPFANGEN 3 ZI SCHICKEN"

"SENDEN 3 T-A-K-T ERHALTEN 4 CHI"

Such messages were in the nature of station reports and were transmitted to the central station at least once every day. Not only because they were so easy to identify, but also because they were veritable mines of information (note the spelling groups above), these messages were of the utmost importance and they will be treated more in detail subsequently.

Two other very frequent short messages were the following:

SOFORT 1 MANN NACH HIER SENDEN

BRAUCHEN SOFORT 2 AKKUMULATOR-EN

Note the appearance of the very important words NACH, HIER and SOFORT in the preceding messages. The preposition NACH was in fact very important.

The conjunction UND was fairly easy to locate from the various clues given herewith:

1) It was the very obvious connecting link between two sets of groups which were externally evident as being coordinate. For example, note the following messages.

KPR UNS UVK RIF KVS KPR UNS RSQ UPW

KVO RIS KVS KVO KPU

ROB RXT; ROB KAS; ROB RXT KVS KAS

43

44

2) Sometimes this group was used between two "foreign" groups, i.e., groups which were evidently not errors but which did have the initial letter K, R or U, or which sometimes had one of the umlauted vowels. Such groups were frequently used to designate the names of places and the code names of military units, a subject which will be discussed later. Examples of such a usage, which was soon prohibited, are the following:

BAN KVS BAP

RBÄ KVS RBÖ

IV. PUNCTUATION. (Satz-zeichen).

Instead of being as might be thought at first hand, mere refinements and really unnecessary additions to the meaning of the sentences, in these codes the punctuation signs were of paramount importance in solution, and their identification was an indispensable part of the solution. For example, it may be said that the identification of the PUNKT (.) was probably the most important factor in the preliminary steps toward solution. At the beginning when the would-be-decoder was working with wholly unintelligible "sentences" the mere ability to block out a single sentence into its parts, if it was a fairly long one, was of greatest value; and the various uses to which the Germans put the important punctuation signs furnished the most surprising and valuable clues. Their discovery may be attributed more or less to the unintelligent pedantry of the German operators, who in the beginning varied only unconsciously a procedure once established, i.e. their tendency was slavish adherence to a regular form. However, it must not be supposed that the uses given herewith were subject to no variation whatsoever. They are only generalizations after all, and just as we in writing clear text do not invariably use the same punctuation in exactly the same manner and in exactly the same places, so the Germans likewise varied their procedure now and then.

The characteristics by means of which the most important of these signs were classified and identified followed from their uses just exactly as was the case in all that has gone before.

44

45

1. PUNKT (period)

A. Uses.

1) Normal use in separating sentences within a long message.

2) Separating the various headings of tabulated messages in the nature of reports. Example: 1 PUNKT NICHTS PUNKT 2 PUNKT SICHT GUT PUNKT 3 PUNKT NICHTS...etc.

3) At the end of short, single-sentence messages.

4) In abbreviations, probably the most important use, and thus the most fruitful source of identifications, because single letters ~~may~~ could be found. Examples:

K PUNKT T PUNKT K PUNKT (KAMPFTRUPPEN KOMMANDEUR)

A PUNKT V PUNKT O PUNKT (ARTILLERIE-VERVINDUNGSOFFICIER)

R PUNKT I PUNKT R PUNKT (RESERVE INFANTERIE REGIMENT)

R PUNKT I PUNKT D PUNKT (RESERVE INFANTERIE DIVISION)

LT-PUNKT M PUNKT (LEUTNANT M.)

In the earliest codes these groups were particularly easy to identify because there were no alternates for any of the letters nor for the PUNKT so that the repetitions of the latter in the form shown above were clear indicators of the presence of such abbreviations.

5) In setting off addresses and signatures either accompanied by numbers or not accompanied.

Example:

(a) REGIMENT PUNKT WARUM IST etc., etc. R PUNKT 61 PUNKT

(b) DIVISION PUNKT FEIND IN DIE MITTE EIN GE DRUNGEN PUNKT BRIGAN

(c) ~~BRIGADE~~ AN 25 RESERVE DIVISION PUNKT SOFORT .... PUNKT

(d) AN 12 PUNKT RESERVE DIVISION

(e) 3 PUNKT KOMPAGNIE

6) In dates: 11 PUNKT 4 PUNKT 17 PUNKT

7) Often used to replace the word UHR: 2 PUNKT 30 (2:30)

8) In decimals

B. The result of all these uses led to the characteristics by means of which the PUNKT could be identified very early. These characteristics were as follows:

45

46

1) It was one of the most frequent groups, if not in fact the most frequent one.

2) It was highly colored red and yellow, never green, occasionally blue.

3) It was repeated several times within long messages.

2. KOMMA (comma)

This group was not nearly so frequent as PUNKT and its main use was in separating the parts of a sentence. Occasionally it was used in the place of a PUNKT, as for example in the following "VON 2 UHR 30 BIS 3 KOMMA 45":

At one time it used to be very frequent in the following:

KOMMA N-D-O

3. DOPPELPUNKT (colon)

The use of this group was the same as in English and it often would overlap with the dash (TRENNUNGSSTRICH). Example:

VERLUSTE DOPPELPUNKT (=Verluste:)

ANFORDERUNG DOPPELPUNKT (=Anforderung:)

4. FRAGEZEICHEN (Interrogation point)

This group was of the greatest importance in that it was bound up with the identification of the main interrogatives and of the verb IST as explained ~~in section~~ on pages ---. On account of its almost invariable stationary position at the end of messages, chiefly short ones, its frequency and red color in the index was sufficient to enable the solver to find it very early in his studies, especially if "question and answer" messages were indicated throughout the text. Note the following messages:

37 c 38

PV v RS 1520 CHI-5 KAB RST ROB KNS UAF
RS v PV 1525 CHI-3 KNS RIN RBQ

S2 v KN 0910 CHI-7 KUN RIF UFT RCS KSU UAF
KN v S2 0920 CHI-3 RIF UBS

AX v PR 1205 CCHI-5 KUN RCA KSO UBK UAF
PR v AX 1208 CHI-2 KZR UXB

A4 v KB 1635 CHI-7 KSU KVP KUN UFT RCA KSU UAF
KB v A4 1642 CHI-4 RCA KSU RCA RIY

5. AUSRUFUNGSZEICHEN (Exclamation Point)

This group was commonly used in practice messages and after

short commands. It was not very important, but its identification aided one of the finishing touches to solution.

6. BINDESTRICH.(Hyphen)

a) Its normal use was that of a hyphen. Example:

ERD-TEL STATION.

b) It was also equivalent to the word BIS. Example:

VON 20-25 SCHUESSE.

c) In separating coordinates in tabulated messages. Example:

5 PUNKT-8 PUNKT NICHTS.

d) In giving the strength of units. Example:

5 TE KOMPAGNIE: 1-4̄4̄0, which meant that the strength of the 5th Company was one officer, 4 N.C.O's and 40 men.

7. BRUCHSTRUCH (Diagonal stroke)

This had a particular use as a rule in the following cases only: 8 / 112, which equalled REGIMENT 112 COMPANY 8.

8. TRENNUNGSSTRICH (dash)

a) This group was often used in the same way as the BINDESTRICH, separating address and signature from the main body of the text, for example:

REGIMENT - WARUM ... .. ? - BRIGADE.

b) As a dash in English - separating an "afterthought" or further explanation.

c) As the equivalent of BIS.

9. KLAMMER (parenthesis)

A very rare group and difficult to identify. It was sometimes used to enclose an explanation or an identification, example:

PLANQUADRAT 4452(1: 20000).

V. AUXILIARY SIGNS (Hilf-signale)

The uses of these auxiliary signs in these codes were very definite and the identification of the important ones was necessary to the completion of the reconstruction of the code. These signs were placed immediately after certain words to alter, modify, or to make more definite their meaning wherever doubt existed concerning their significance in the particular position they occupied. On this account, namely, that they always immediately followed a certain

few groups, their position was fairly constant. Furthermore, they never showed green color in the indexes, and, in fact, little color of any sort. When several sets of bigraphs were found, in each of which the second group was the same, the latter group was usually one of thes auxiliary signs. Therefore, when beginning the study of the code text, it was important to find and to note all groups which had a tendency to occur in pairs, or bigraphs, on account of the aforesaid constancy of position of these signs. Immediately after identifying any of these groups they were filled out through the entire text, and the nature of the preceding group thus indicated. This was of great assistance in forming an assumption regarding the meaning of an entire sentence. Continuing the chain, above each occurrence of these preceding groups which had thus been classified was indicated its nature, i.e., NOUN, VERB, etc., even though it was not followed by the auxiliary sign which had led to its classification.

The chief ~~characteristics~~ uses of the auxiliary signs were as follows:

1. HAUPTWORT and ZEITWORT. (noun and verb)

The first of these two groups was used to change a verb into a noun in case the latter was not in the code book, and vice versa in the case of the second of these groups. Example: DIE VERTEILEN HAUPTWORT WIRD etc. (Equals - DIE VERTEILUNG WIRD, etc.); "ANDERUNG ZEITWORT (equals - ÄNDERN).

2. EINZAHL and MEHRZAHL (singular and plural)

These groups were used to convert a noun which was found only in the singular or the plural form respectively in the code book into the desired form. Examples:

DIE GRANATEN EINZAHL (equals - DIE GRANATE)

48 60 SCHUSS MEHRZAHL (equals - 60 SCHUESSE)

3. ERSTE STEIGERUNGSFORM and ZWEITE STEIGERUNGSFORM

49 These signs were used to indicate the degree of comparison which an adjective was meant to signify. Examples:

GUT ERSTE STEIFRUNGSFORM AUFPAS EN (equals - BESSER AUFPASSEN)

HOCH ZWEITE STEIGERUNGSFORM ANTENNE (equals - HOECHSTE ANTENNE)

4. TENSES OF THE VERB

4. TENSES OF THE VERB

GEGENWART (present tense)

VERGANGENHEIT (past tense)

ZUKUNFT (future tense)

MITTELWORT DER VERGANGENHEIT (past participle)

These groups are all self-explanatory and were fairly frequent. They were first found in short messages usually and from there on the path was clear. The first one together with MEHRZAHL were the most frequent, and thus had a tendency to form bigraphs more than most of the groups. A careful hunt for bigraphs, therefore, usually disclosed these groups.

5. BUCHSTABIER GRUPPE (spelling signal)

This sign was used to indicate that spelling groups began or ended. It was only used in the earlier editions of this code, inasmuch as later it was found to be unnecessary.

As stated above the manner in which these groups were found was by noting all bigrams and by studying the context of the messages wherein they appeared for further identification. Often the sense was clear but the intervening group which was present had to be given a meaning, and therefore the decoder had to determine whether or not he had there an auxiliary or possibly a punctuation sign.

VI. BLIND GROUPS

In the period covered by the above, the use of blind groups was so relatively infrequent that they could have been omitted from consideration entirely, inasmuch as they did not interfere with the solution to any appreciable degree. The code book contained only a few of such groups, all localized at the bottom of one page of the code book, and not enough stress was laid upon their use to keep them in the mind of the operators, who as a consequence disregarded them entirely.

In the later stages, however, the procedure with respect to these groups had been modified so much that they became of increasingly greater importance as time went on. They will be discussed in a further section. (see page --).

The uses and characteristics of the six main sets of groups have been discussed, and indications have been given how solutions in each were made. Too much stress cannot be laid upon the fact that at no time was it possible to confine all attempts to the solution of one set first, then proceed to another, and so on. The work of solution and reconstruction proceeded in all of the classes simultaneously solutions in one set leading to solutions in another in a never ending chain. It must be emphasized that the preliminary steps necessitated the classification of the most important groups of each set of these six main classes. After a few solutions had been made in each, and all work rested upon a sure foundation, the road to completion was clear. It was possible in those early days, after considerable progress had been made, and as long as the code continued to be in effec to decode the enemy messages as rapidly and alm as completely as ~~it~~ was done by the enemy himself.

Messages dealing with plans for raids, local attacks or counte attacks, reliefs, etc., were frequently solved in time to be of great value.

SOLUTION BY ANALOGY

As stated above, the Germans, in the Spring of 1917, were the first to employ code on the Western Front. The British and the French soon followed their example. There seems to be no reason for doubting that the German Code Office was able to solve the codes of the Allies, and thus discover~~ing~~ed the ~~weakness~~ weak points of code as a general system of secret communication in warfare. 59 There is also no doubt but that the liaison between the German "Enemy-Code-Section" and their own code-producing section was good, for it was not long before improvements and developments set in with respect to their own code, together with a gradual improvement in code discipline and personnel, which continued steadily until the fall of 1918, when their code reached a very high degree of complexity and safety. 51

Before proceeding to a discussion of these developments it is necessary to bring up a subject to which only an allusion here and there has been made in all the preceding discussion, namely, the importance of ANALOGY in the solution of codes. In fact, it may be

said that there are two ways of solving codes; (1) by the method of "First Principles", and (2) by the Method of Analogy. In brief, the distinction between these two methods is this: the solution of a code by "First Principles" involves a long, laborious and detailed analysis of all groups, with the aid of indexes, record-books, charts, extracts and all the various helps by means of which the code-solver can bring the most important features of the code-groups before him in order to form a basis for the assignment of clear-text values to the code-groups; the solution by "Analogy" simply involves the study of a series of unsolved messages the usual form and general contents of which are known to the code-solver from previously decoded messages and all he has to do is to find the groups and sets of groups in the unsolved messages which are analogous with the groups and sets of groups in the previously solved messages in order to form a basis for the assignment of clear-text values.

The Analogy Method, naturally, can be applied only after a solution by First Principles has disclosed the nature of the messages sent by a given set of stations. As long as the personnel of these stations remains unchanged, and as long as they continue to adhere to a definite procedure, to a set or stereotyped phraseology, the Analogy Method is invaluable, and may result in a break being made into a new code when the amount of text is still very small. When this no longer continues to be the case naturally the Analogy Method cannot be applied and solution must be attained by a recourse to First Principles.

52

In the early days, each station had to send daily reports, and these took the form of stereotyped messages, which were even sent at definite hours. A thorough study and acquaintance with the decoded text of messages passing between the stations whose new text was to be solved was, therefore, necessary and was indeed a prerequisite to solution by analogy. The decoder had to be familiar with the form of these reports, their contents, their variations and peculiarities. The location of but a few of the characteristic "landmarks" in the text of a new code was all, then, that was necessary: solution proceeded very rapidly.

Note the following examples of typical reports such as ~~might have been~~ were sent during the summer of 1917:

PQ v RT 04.30 4 TLE 1 TL CHI-4~~5~~4

AN·5·2· RESERVE·DIVISION·PUNKT· MORGEN·MELDUNG·PUNKT·1·PUNKT·INFAN-TERIE·KOMMA·EIGEN·M·G·TAETIGKEIT· SEHR· LEBHAFT·PUNKT·2·PUNKT·VON·1· UHR·BIS·2·KOMMA·30· MORGEN·S·SEHR·LEBHAFT·EN·FEUER·AUF·UNSER·E·VOR· DER·E·GRABEN·MEHRZAHL·PUNKT·

PQ v RT 04.30 4 TLE 2 TL CHI-31

3·PUNKT·VON·1·8·UHR·15· BIS·20·PUNKT·30·UND·VON·22·UHR·BIS·3·3· KOMMA·15·HUNDERT·SCHUSS·MEHRZAHL·AUF·ERSTE· UND· VIERTE·STELLUNG·EN· PUNKT·

PQ v RT 04.30 4 TLE 3 TL CHI-21

4·PUNKT·NICHT· S·ZU·MELDEN·PUNKT· 5· PUNKT·WETTER·GUT· KOMMA·SICHT· UN·KLAR·KOMMA·NICHT· VIELFLIEGER·TAETIGKEIT·PUNKT·

PQ v RT 04.30 4 TLE 4 TL CHI-43

WEITER·PUNKT·6·PUNKT· NICHT· S·7·PUNKT·VERPFLEGUNG·ANKOMMEN·MITTEL-WORT DER VERGANGENHEIT·PUNKT·8·PUNKT· VERLUSTE· DOPPELPUNKT·10·MANN· SCHWER·VERWUNDET·KOMMA·15·MANN·LEICHT·VERWUNDET· PUNKT·9·UND·10·PUNKT· NICHT·S·PUNKT· 2·4·5·TF·R·PUNKT·I·PUNKT· R·PUNKT·

Knowledge of the form and contents of reports like these and the careful study of a few messages in a new code was sufficient to

The importance of the Analogy Method may be illustrated best by giving somewhat at length the various steps in the solution of the Fritz Codes, which were studied by this office. The writer takes pleasure in acknowledging his indebtedness to a preliminary report on the "Fritz Codes" by Second Lieut. Lee W. Sellers, Inf. for most of the material discussed under this heading.

The "Fritz Codes" were used by the Fifth German Army up to the spring of 1918. With the exception of the Emergency Signal System (~~see Part VI, Section--~~), and a special code for aeroplane registration, these codes, at the time of their employment, constituted the only matter transmitted by wireless on the front of the aforementioned Army throughout the period stated. It must be remembered also that at this time the callpletters of the various stations remained comparatively fixed, (~~see Part--, Page--~~), so that the procedure of every station could be studied from day to day.

In the Verdun Sector at that time it was the invariable procedure, occasioned by a General Ofder, in fact, for lower units to transmit short, routine reports to higher units by wireless at definite times during the day. The first step was therefore to search for these reports. Usually they began with either MORGEN MELDUNG, or ABEND MELDUNG, depending naturally upon the time of the day at which sent. Therefore, after separating out all the messages sent during the entire day into two classes, viz., those sent from 00.01 to 12.00 and those from 12.01 to 24.00, a search was made for a set of three groups which would be found to behave in accordance with the requirements of the words MORGEN , ABEND, and MELDUNG. That is, if these words be fepresented by the letters A, B, and C respectively, then the messsges of the morning hours should show among them several beginning AC, and those of the afternoon hours should show among them several beginning with BC.

Series of such messages were not hard to find. Now these reports ordinarily referred to the messages of different kinds sent by a station during the last twelve hours.

Here are several examples :

1) MORGEN MELDUNG 1 CH/I 2 SCH/I SENDEN 4 CH/I EMPFANGEN
2) ABEND MELDUNG ERHALTEN 3 CH/I 4 Z/I GEBEN
3) ABEND MELDUNG ALLE/S IN ORDNUNG
4) ABEND MELDUNG IN ORDNUNG
5) MORGEN MELDUNG WIE SONST
6) ABEND MELDUNG NICHT/S NEU/ES

Note the repetition of the code group for the single letter I in messages one and two. From this group the other spelling groups CH, SCH and Z were soon located, together with the verbs SENDEN and EMPFANGEN.

At this time the operators were in the habit of expressing their approval or disapproval of messages received by sending a message consisting of the code groups for GUT or NEIN repeated two or more times. Such messages, which consisted therefore of two or three repetitions of the same group, were watched. There would be

sure to be one or more messages beginning with a set of three groups of which the third was MORGEN, the second unknown, and the first, one of these groups which was repeated as stated above in other messages. Here then was a clear indication that we had the phrase GUT-EN MORGEN, thus giving the important spelling group EN.

As soon as a few solutions had been made, the custom was to send out a "First List" to the French Code Office. As more solutions were made, subsequent lists were issued.

So invariable were the reports mentioned above that practically all "First Lists" of solutions for the Fritz Codes were identical and consisted of some or all of the following:

MELDUNG	CH	IN ORDNUNG
MORGEN	Z	GUT
ABEND	SCH	UND
SENDEN	I	1,2.3.4.5.
EMPFANGEN	EN	

Once an opening was made, further progress was very rapid. During those days, when "camouflage of liaison" was yet in its infancy, the sending of practice messages by the German operators was a boon to this code office. For a detailed discussion of the necessity for and importance of practice messages, reference is made to Part [illegible] page [illegible] --, of this report. At this point we will only discuss the nature of the practice messages sent by the German operators at this time.

Owing perhaps to lack of imagination they were in the habit of repeating short aphorisms as practice messages. They did this so constantly that in at least one instance it was possible to know in advance what "aphorismus" a particular station would send. Its favorite was:

MORGEN STUNDE HAT GOLD IN MUNDE

Sometimes before a code was three days old a thirteen group message beginning with the word MORGEN and having certain characteristic repetitions would prove to be this proverb, spelled out as follows:

MORGEN ST-UND-E HAT G-O-L-D IN M-UND-E

Note the repetition of the UND-E in this message.

Frequently the group for UND would be located already and would thus aid inthe finding of this proverb.

Having identified a few spelling groups further progress was made by continuing the chains which they initiated. Whole words would now be solved. The auxiliary signals and punctuations would manifest themselves, and progress would be very rapid.

Having given, from the proverb mentioned above perhaps, the following:

KKA	RUC	RLN	UVK	KUZ	UVA
		O	ST		-?-

it was soon possible usually to complete the message without any difficulty as follows:

KKA	RUC	RLN	UVK	KUZ	UVA
IST	P	- O	- ST	DA	-?-

The word IST was used very frequently as a syllable in the words L-IST-E, or HE-IST, and very often the whole message

WO BLEIBEN GEGENWART VERPFLEGUNGS L-IST-E?

would be solved as a result.

Among the messages which furnished a great deal in the way of solution by analogy, and this applied not only to the Fritz Codes, but also to the very latest codes, were those dealing with the issuing and recalling of the SATZBUCH, or code-book. It is a rather curious fact that the code-book itself did not contain in its first editions the word SATZBUCH nor was it among the many words added subsequently. As a consequence, whenever mention was made of it, the word had to be spelled out. Now when a new code-book went into effect, among the messages of the first day's traffic would be found almost invariably one or more messages calling in the old code-books. They ususlly began with the words ALTES SATZBUCH or ALTE SATZBUECHER.

The appearance of such messages was so regular that a hunt for them would be made immediatelyafter a few spelling groups had been classified. Let us assume that we have found a message in which we have underlined a chain of spelling groups and which we suspect to contain the word SATZBUCH. The question then arises as to how to distribute or assign the values in the chain.

From the various previous solutions, the following distributions are possible:

AL T-ES S-A-TZ-B-U-CH ....

AL T-E$\ddot{E}$ S-A-TZ-B-U-E-CH-ER ....

ALTE$\ddot{E}$ S-A-TZ-B-$\ddot{U}$-CH-ER ....

~~ALTE$\ddot{E}$ S-A-TZ-B-$\ddot{U}$-CHER ...~~

The guiding clues for the distribution would be furnished by the indexes. It is obvious that the groups representing the parts of this word should show the following characteristics:

S-High frequency, some color, of which yellow and red predominate

A-High frequency, little color, sometimes standing alone, or even in the company of numbers. This arises from the use of this letter in designating the subdivision of a PLANQUADRAT square, for example: PLANQUADRAT 4528A.

TZ-Low frequency, little color, sometimes standing alone, or even in the company of numbers for the same reason as given under letter A.

U-Medium frequency, no color, seldom found except with other spelling groups.

$\ddot{U}$-Medium frequency, no color. At one time the enemy had been sending a peculiar type of report somewhat as follows:

T-2-15-2-$\ddot{U}$-2-15-2. The nature of this report was undiscovered. For this reason the letter $\ddot{U}$ might sometimes appear between numbers.

E-Very high frequency, if colored, red or yellow, seldom green, Often standing alone because of its frequent use in connection with the inflection of nouns and of such adjectives as ALT, NEU, SCHWER, etc.

CH-Low in frequency, very little color, sometimes green or blue occasioned by the sending of such messages as :

CH-I 1307 ER-LE-D-IG-T

2 CH-I GESCHICKT, 3CH-I EMPFANGEN

FR-Fairly high in frequency, colors, red and yellow, seldom green, perhaps two or three times blue, occasioned by such a message as

W-ER HAT FUNKSPRUCH 2000 GE-GEBEN?

This group (ER) may be found alone frequently, that is in juxtaposition with groups evidently not spelling groups. This is occasioned by the use of this group in connection with the inflection of nouns and of such adjectives as STARK, SCHWER, ALT, etc.

(insert new) → These brief descriptions will suffice to emphasize the point that not only could the decoder find no aid from the normal frequency tables for the language, but also that he had to be familiar with the various uses to which the individual letters and syllables were put in such a code. In this, the knowledge and experience gained in previous codes was indispensable.

37

In these codes numbers were solved without much difficulty. In the first place, the most important ones, from 1 to 6 or 7 were classified very early, by the station reports which were the basis of the analogies leading to the first solutions. Numbers were used in all the situations mentioned on page --, especially frequent was their use in connection with call-signs of stations, and since in these days the call-signs remained fairly constant, many identifications were secured or corroborated by their means.

The solution of complete words and phrases was the most difficult part in solution and naturally followed only after a fairly large amount of work on spelling groups and numbers had been done. However, it must be added that phrases and WICHTIGE MELDUNGEN (important ~~messages~~ reports) presented difficulties normally insurmountable because the groups standing for such messages were of such infrequent occurrence that certainty or corroboration of solution was usually impossible. Perhaps if a close liaison between the intelligence officers in the front line and the code office a hundred or more kilometers back were possible, such solutions could have been achieved. But as a matter of fact, while such solutions were important they were of great interest only at the particular hour when they were sent. Messages dealing with the tactical situation, preparations, and intentions were of much greater importance and their solution was always within the realm of possibility. The identifying of such short and frequently used phrases as

IN ORDNUNG
LEICHT VERWUNDET
SCHWER VERWUNDET
LAGE UNVERAENDERT

was a comparatively easy matter, but at the same time that represented the limit of success in solving of such phrases.

The Fritz Codes continued to yield to solution along these lines until late in the spring of 1918 when this office discontinued their study and concentrated all attention upon the Albert Codes in use by the German unit "Detachment "C" ~~opposite the American First Army.~~ [illegible]

As stated before, code was introduced on the Western Front sometime around the month of January, 1917.. After it was found that code could be used with advantage under such conditions, wireless activity suddenly increased very greatly in amount. This is illustrated in a striking way by noting the great increase in the number of enemy wireless stations: in January 1917 there were approximately 125 on the Western Front; in August of the same year the number had increased to almost 700.

Wireless traffic thus began to assume a very great importance and it was but natural that developments and changes should take place. On account of the information that could be secured by merely studying the radio traffic in its external aspects above, it became necessary to adopt measures to prevent the enemy from securing such information. This was the beginning of the "Camouflage of Liaison", a subject which is discussed in detail subsequently (see Pages --). For the moment we will not break the continuity of thought, by going into that phase of the subject, but will continue with the KRUSA Codes.

K R U S A CODES

It was but natural that with the development of methods of camouflaging liaison, and, also of methods of solving codes, that the trench codes should increase in complexity. As time went on, it became more and more difficult to reconstruct the enemy codes, and the various additions and complications which arose will be taken up herewith.

The first change (towards the early part of Fall, 1917) was an increase in the number of representatives or code-groups for the the most frequently used groups, i.e., the adoption of "variants." Whereas up until this time such highly important and frequently used groups as PUNKT, numbers, and spelling groups such as the important consonants B, C, D, G, K, etc., and even the vowels O and U, were without alternates whatsoever, the enemy soon found that these groups became so conspicuous by their high frequency that most of the important groups were increased to two representatives, and some to three.

The effect of these additions was not to cause any change to be made in the methods of classification and identification, as explained in the preceding sections, but to render these processes more difficult at the start, because of the reduced frequency of the main groups, and the disappearance of certain invaluable clues which were the result of the absence of alternates or variants for the important groups. Consider for example, the single case of locating the abbreviations KTK and RIR. In the early days, these abbreviations could be represented in one of two, and only two forms:

A B A or A X B X A X
C D C or C X D X C X

in which A stands for the group representing letter K; B, the group for the letter T; C, ~~the one~~ for R; D, ~~the one~~ for I, and the ~~one~~ X for PUNKT.

Therefore, after PUNKT had been identified (and this was done very quickly), as soon as such sequences ~~such~~ as those shown had been found, it was soon easy to determine them to be either KTK; K PUNKT T PUNKT K PUNKT; or RIR; R PUNKT I PUNKT R PUNKT. It was easy to determine which of these two was correct.

But with the adoption of two and three variants for these frequent groups K, T, R, I and PUNKT, each of these abbreviations could appear in any of the large variety of forms resulting from the great number of combinations possible as a consequence of this increase in the number of code-equivalents for each group.

The method, then, of locating such a series was to study all the bigraphs, trigraphs and polygraphs with a view to the estab-

lishment of equivalency of code-groups. When two code-groups were found to exchange places in chains of groups, or when two or three groups were found to occupy the same relative positions in messages indifferently, it could be assumed that these groups were equivalents OR variants for the same group.

60
61

Having found, for example, a polygraph repeated three times as

E F G H I J K

and twice as E F P H M J K

it was not hard to imagine that the groups represented by the letters G and P, I and M were equivalents. By a study of such cases the alternates and variants for the most frequent groups were classified and later identified.

To illustrate the enormous increase in difficulty of locating such a phrase as MORGEN MELDUNG, which formerly had been so easily identified, it may be stated that whereas at first there was but one group to represent MELDUNG and one each to represent the various parts of the day, at the end of a year there were in the code-book the following groups for the same expression, each having three variants.

ABEND	MITTAG
MORGEN	VORMITTAG
MELDUNG	NACHMITTAG
ABENDMELDUNG	VORMITTAGSMELDUNG
MORGENMELDUNG	MITTAGSMELDUNG
	NACHMITTAGSMELDUNG

Despite this increase in the number of variants, code messages could still be solved, though not so readily, because of the carelessness and ignorance of the operators responsible for encoding the messages, a fault of which the German operators were on the whole much less guilty than our own as time went on. Though the use of the variants was recommended time and again, the operators failed to do so and it was only after a long period of inspection and strict regulation that the rules for the indiscriminate use of variants were followed. At first, the German operators had the idea that the variants were to be used only in case the group were repeated in a single message: i.e., if the group had to be used three times the first time he would choose the first of the

the series of three variants, the second time, the second one, etc. As a result, the first group in each set of variants was ~~used~~ by far the most frequent and a great deal was detracted thus from the value of the alternates. Later, however, and possibly ~~after~~ as a ~~the~~ result of regular instruction in special schools, the German operators improved vastly and the repetition of a group within a message became indeed a rare phenomenon; also all three values were used indiscriminately. Another important factor was that the rule prohibiting the spelling out of a word, the equivalent for which existed in the code book, was not strictly followed. The most flagrant violation of these rules was encountered in one message sent during the month of Sept-ember 1918, which was as follows:

DSZ v DHR (H40 v ---) T-3.09.18. 10.10 CHI-10

H	O	CH	A	N	T	E	N	N	E
UAR	KUE	SHN	ALV	RZN	ASN	SAX	RZN	RZN	SAX

This message, after we had decoded it (by means of a cap-tured code book) caused us much chagrin, for had we not hesitated to follow through to its completion the clues offered by the re-peated groups, we might have broken into this code in the early part of its life. This case also emphasized to us that one must not hesitate to assume such an occurrence as the spelling out of a word or a phrase which is already present in the code book, even under the best controlled conditions; for the word ANTENNE was among those which suggested themselves to us, but because of what we regarded as its high degree of improbability, it was not tested very thoroughly. The next important changes were as follows:

1) The compound numbers from 10 to 20 were added. This nat-urally resulted in increasing the difficulty in locating numbers, especially military unit numbers. Whereas formerly in order to indicate the 125th Regiment, for example, it was necessary to give the groups for 1, 2 and 5, the same could now be represented by two groups, 12 and 5. This also tended to reduce the frequency of the number 1 very greatly.

2) Various frequently used words which formerly had to be spelled out were added. For example, a case which was rich in its harvest of spelling groups was the following:

D-IST-I-LL-IE-R-TE-S-WASSER

65

Now, the whole phrase DISTILLIERTES WASSER was represented by one group. Other additions of much importance were the groups representing the words TELEFON, RUFNAMEN, SCHLUESSELHEFT, etc., which formerly had to be spelled out.

3) A table of the hours of the day was added, giving for each hourly and half hourly period of the day three variants and also having two complete sets, one for the morning hours, the other for the afternoon hours. Thus at one stroke, the entire set of groups by means of which it was possible to locate very quickly the prepositions VON, BIS, ZWISCHEN, the word UHR and also the very important numbers from one to twelve, was destroyed, and from then on such identifications became very difficult. The enemy also added a smaller table giving two alternate equivalents for periods of time from five minutes up to 55 minutes.

4) The entire procedure with respect to nulls or blind groups was changed. The nulls increased in number from 12 to 50 and were distributed in sets of 4 at the bottom of nearly every page in the code book. The instructions were to use them very liberally and especially in messages consisting of only two or three groups. The first code in which their use in such a manner was discovered was in Albert Code No. 10. Long after the break was made into this code, in fact weeks after the code went out of effect, continued study of this code brought to light the fact that the high frequency groups for which no values could be found, and the presence of which nevertheless did not seem to interfere with the sense of most messages were nothing else but blind groups. Three ~~of~~ four of such groups having been identified in perfectly legitimate places, such as between spelling groups, these groups were traced throughout the text, when it was noted that here and there an entire message consisted of nothing but a series of these blind groups accompanied by the groups for UEBUNGSFUNKSPRUCH. Following up this clue it soon became apparent that the enemy was sending as practice messages chains of blind groups with perhaps one or two "real" groups in the whole message. By following out this clue, the entire series of about 50 blind groups was identified.

63

64

Now a little thought will show that such a method of employing blind group put new difficulties in the way of the code solver, for the blind groups, if used with discretion, would behave exactly like numbers as regards first, their irregularity of interchange and second, their coloring in the indexes, since they could be placed anywhere in a message.

It became necessary, therefore, to find some method of distinguishing numbers from blind groups, for at the beginning when the code-solver has hardly any guiding points at hand, once having started out on a false track, he might readily classify and build up as a whole series of numbers what really was nothing but a series of blind groups.

The clues for distinguishing them were found not in any particular characteristics of blind groups themselves, but in the characteristics of the blind groups as used by the Germans: they carried a good thing too far. The operators got into the habit of turning to a page and transmitting the series of blind groups in the order in which they stood on the page. The result was that as the text accumulated, and the blind groups stood out because of the frequency and ubiquity of their positions; the finding of individual messages with a chain of such groups soon confirmed their identification as blind groups. Very often, furthermore, a blind group would be found between two groups which in other places formed a bigraph, a very clear confirmation, therefore, when several cases like this were found.

It should be added, however, that when there was really important traffic going on, the operators seemed to forget all about blind groups. In other words, the lavish use of these was confined to practice messages and to messages coming from a quiet sector.

The addition of all the groups mentioned above, together with an increase in the number of variants for the important groups necessitated the addition of the letter S to the series of initial letters raising the total number of possible combinations from 2,038 to 2,704 combinations.

The final additions and changes to the code were even more radical.

1) More spelling groups were added, this time (a) for infrequent combinations in German, (b) for frequent combinations of letters found in the French names of towns, such as AIN, AGNE, ANCE, AUX, BOIS, etc., etc.

2) The adoption of an enciphering table containing cipher equivalents for pairs of letters; this table was to be used in spelling out place names. The following is a translation of the directions for the employment of this system, as contained in the code-book itself (see pages ~~73~~ 70-77 of Exhibits ~~10~~ 5 and ~~11~~ 6):

SYSTEM FOR THE SPELLING OUT OF WORDS.

The Encipherment.

1). Write the word to be spelled out, writing the letter 'Ä' as 'AE', 'Ö', as 'OE', 'Ü' as 'UE'; for example, Düsseldorf - Duesseldorf. Divide the word into pairs of letters. If after this an unpaired letter remains at the end, add to it a recognizably dummy letter, for example J, X, y or I.

Example: The word DUESSELDORF would give: DU-ES-SE-LD-OR-FX

2) Encipher ~~ent~~ the pairs of letters thus formed by means of the Enciphering Table. This is done by finding the pair of letters and setting down the pair of letters standing beside them in the table.

Example: DU=LZ; ES=AT; SE=CH; LD=SE; OR=BV; FX=WD.

3) In front of every enciphered pair thus found place as the third letter A, K, R, S or U.

Example: KLZ AJT UCH SSE RBV SWD.

4) Count the three-letter groups formed in this manner, find the SPELLING SIGNAL corresponding to this number, and set it before these groups.

The Spelling Signal indicates to the decoder how many groups following it are not to be found in the code-book but were built up by means of the Enciphering Table.

Example: KLZ AJT UCH SSE RBV SWD.

There are 6 groups. The Spelling Signal for "six encipher pairs of letters follow" is UPF. It is set before the groups.

UPF KLZ AJT UCH SSE RBV SWD

Prudent

SYSTEM FOR SPELLING

Deciphering.

If one finds in decoding a message the following meaning for a group:

"There follow (number) enciphered pairs of letters", then as many of the code groups following this signal as are indicated by the number are not to be sought in the "Decoding" part but are to be treated as follows:

1) Strike out the first letter of every group, so that pairs of letters remain.

Example: The message reads:

space > UMS UEC AUQ KNU RCV SRY SHZ UQS SFI
UMS = STATION
UEC = There follow 6 enciphered pairs of letters.

The initial letters, therefore, of the succeeding six groups are stricken out:

~~A~~UQ ~~K~~NU ~~R~~CV ~~S~~RY ~~S~~HZ ~~U~~QS

2) Decipher the pairs of letters thus formed by means of the "Deciphering Table". This is done by seeking the pair of letters and writing the pair of letters standing opposite in the table. By writing together the pairs of letters thus found, the clear text results.

LC 67

Example:

UQ = DU, NU = ES, CV = SE, RY = LD, HZ = OR, QS = FX.

DUESSELFORFX = DÜSSELDORF

3) The code groups then following in the message are looked up in the "Decoding" part.

Example; The group SFI follows. SFI - ANRUFEN (call up). The decoded message reads: STATION DÜSSELDORF ANRUFEN.

No further explanation of this system is necessary. The Enciphering Table changed with each code, and the equivalents were at random, there being no system whatsoever to the construction of the table.

A study was made to determine whether such enciphered spel-

'ling groups could be detected in the new code text, whether the Germans were actually making use of this table, and if so, to what extent. A large chart, 26 x 26 was made. Each one of the 676 smaller squares was divided into five parts and the text was recorded in the following manner:

Suppose the group RAB were to be recorded in this chart. The group belonged in the large square determined by the letters A and B, and on the line reserved for the letter R, a check mark was placed. A group UAB would go in the same square but on the line opposite the letter U a check ~~was~~ would be placed. Thus:

	A	B	C	D	E	etc.
A	K- R- U-1 S- A-	K-111 R-11 U-11/1 S-111 A-11/1	K- R-1 U-1 S- A-			
B			K-1 R-(11/1 11/1 11/1 11/1) U-11 S- A-			
C				K-11/1 R-- U-(11/1 11/1 11/1 11/1) S- A-		
D						
etc.						

Now the theory was that since any one of the letters K, R, U, S or A could be prefixed to these encipherments, a square which showed a diversity of prefixes might well indicate one of these spelling groups, whereas a square showing a high degree of constancy as regards initial letters would be likely to be a code group. On this basis, the group AB as shown in the diagram might well be an enciphered spelling group, whereas RBC and UCD are probably code groups. To check this up, supposing that the groups ending AB were found in the following chains:

ATK	RAX	KUN	RAB	SAV	RIV	UCT
RCV	KAX	KUN	UAB	RAV	KIV	AUK
ATK	UAX	RUN	KAB	SAV	UIV	RIP
RCV	SAX	UUN	SAB	KAV	AIV	KUB
ATK	AAX	AUN	KAB	RAV	SIV	KOL

The finding of such sequences would be a complete confirmation of th theory that we have here an enciphered word of five digraphs which begins with the group AX and ends with the group IV. The constancy of the groups ATR and RCV shows them to be the spelling-group signal for five groups whereas the inconstancy of the groups following the enciphered spelling groups shows that miscellaneous text follows.

A fairly exhaustive study of the text of one code failed to disclose such phenomena, whereupon we were led to conclude that the enemy was making very little use of this table. This conclusion was completely substantiated when a copy of the very next code was captured and it was found that the use of this table was indeed rare. ——— draw line & leave space

3) The extensive use of and change in procedure as regards DECKNAMEN.

This was probably one of the most important changes in the entire development of the code, because of the stumbling blocks it put in the way of the solution.

It was only after listening-set stations were established on the Western Front, and their possibilities discovered that all the warring forces found it necessary to adopt a whole system of conventional or code names to designate the various Military Units, artillery-groups, support-groups, observation-posts, geographical points, etc., all along the whole front. The Germans called them DECKNAMEN (literally "cover-names or disguise-names"). Up until the winter of 1917, and early spring of 1918, when a DECKNAMEN was used in a code message, it had to be spelled out. The result was then that such a practice aided very considerably in the solution of spelling groups. By the end of spring 1918, however, a most radical change took place in this respect, as a result of the very simple expedient of applying code-groups to the DECKNAMEN, and changing not only the latter every few weeks, but also changing the code-groups with each new change of code. The very earliest code-books had pages assigned for code-groups of DECKNAMEN and ORTSNAMEN or place-names, but ther were not made use of to any great extent.

But later, when their importance became understood, with the issue of each new code, a list of DECKNAMEN equivalents for each sector was provided by Divisional Headquarters, who secured them from a larger list made up at either Corps or Army Headquarters. These were written in by hand, or the typewritten sheet was pasted inside the book, at the proper place, by each unit receiving a copy of the code-book. Note pages 21-24 in the photostat copy of Albert Code No. 17 (Exhibit 6) ~~and the captured book of DECKNAMEN, shown as Exhibit 15~~.

It is obvious that, as a result of these changes,

a) A marked reduction in the use of spelling groups and of numbers was thus effected;

b) Even if such code groups were solved no actual identification of Military Units or of positions could possibly follow except by circumstantial evidence.

It should be added that the greatest effectiveness of DECKNAMEN was during positional warfare, since in warfare of movement, most of the units and groups shifted places. At the beginning of their employment, the custom was regularly to begin the message with the DECKNAMEN of the unit addressed and to end with that of the unit sending. As a consequence it was very easy to locate these DECKNAMEN and upon some occasions certain deductions were possible with regard to reliefs and changes in battle order; namely, when a unit bearing a given DECKNAMEN was found to disappear from one position and suddenly reappear in another position, indicating that a unit had moved and failed to take the DECKNAMEN of the unit whose place it was taking, a procedure which was absolutely against regulations. However, later even this method of using the DECKNAMEN, which resulted in their becoming conspicuous, was amended, so that they could not be distinguished from the names of Military Units, such as regiment, brigade, etc., or at least only with great difficulty in a quiet sector.

In addition to these DECKNAMEN arranged in alphabetical order there was a special table in the last codes by means of which the code-groups representing, let us say, the DECKNAMEN of a given artillery group, changed with every ten-minute period. ~~(A sample of this table will be found on pages 25-7 of Exhibit 10).~~

Supposing the time given by the German operator was 12.25, and the message was addressed to group MARS, the code name was ROR. If this same group was addressed at 10.32 its DECKNAMEN would be represented by AZI. At 6.55 it would be addressed as RYI, etc. In other words, the DECKNAMEN would be chosen according to the column under which the minute-period for the particular message fell. It is not known to what extent the Germans made use of this table in every sector, but in certain ones, it was used a great deal, and with good effect.

4. DISTORTION.

In order to make clear the nature of the change which is to be described now it will be necessary to recall to the reader that the first process of solution of a code, namely the process which has been termed classification above, was dependent upon the external characteristics of the main sets of groups in these codes as determined by their uses. Spelling groups, for example, had the chief characteristics of appearing in chains, in more or less definite positions. Supposing now that the code groups of which a messa~~is~~ge ~~was~~ composed ~~were~~ be shifted about so that all constancy or regularity of position of any code group ~~was~~ is absolutely broken up; it is easy to see that the greatest of all stumbling blocks ~~had been~~ would be placed in the path of the would-be-code-solver.

Supposing even that classification of spelling groups could be made, it is clear that the difficulties in the way of building up a word whose parts were scattered and mixed about within a message would be enormous. This ~~is~~ was exactly what the Germans did as regards their practice messages, by means of an apparently random distortion which resulted in a complete transposition of the groups comprising the messages. This phenomenon was first encountered in the Three-Number Code and, of course, evidence was soon found in the Three-Letter Code that the same practice was being followed. It was not until the capture of the code-book applying to Albert 17 (Exhibit ~~15~~ 6) enabled us to decode completely the text, that full confirmation of this procedure was found. A few attempts to determine the nature of the transposition were unsuccessful and it would seem that it was intended to be more or less of a test or a puzzle for the receiving station to put together the distorted messages, aside from confusing the enemy code experts.

As signals for distorted messages, the enemy had a table ~~(see Page 81 of Exhibit 10)~~, which changed with the code. These signals changed ~~with the date~~ daily. Examples of such messages are given subsequently on pages ---.

As stated above, such tricks were used almost exclusively in practice messages; consequently, in an inactive sector, where very little real traffic was necessary, by fall of 1918, the text presented a rather hopeless case to the code-solver and it must be admitted that hardly any information of value was or could have been secured therefrom. As soon, however, as the sector began to be active the entire complexion of the code changed and took on the regular appearance of real code text, and it became possible once more to dig in and to extract useful information.

LENGTH OF TIME CODES WERE IN USE

In all that has preceded no mention has been made of the factor which was of the highest importance in the solution of a code, i.e., the "life" of the code, or in other words the length of time it continued to be in effect. Below is given a table showing this information.

G - Sector

Type	Name	No.	Commenced	Ended	No. days.	
KRU	Fritz	3	Aug.29,'17	Oct.30	63	Average
	"	6	Oct.30,	Nov.26	28	
	"	11	Nov.27,	Dec.26	30	
	"	14	Dec.27,	Jan.28,'18	33	-- 36 days
	"	19	Jan.29,'18	Feb.28,	31	
	"	23	Mar.1,	Apr.4,	35	
	"	28	Apr.5,	May 5,	31	
KRUS	Jean	1	May 6,	May 23,	18	-- 23
	"	2	May 24,	June 20,	28	
KRUSA	Andre	3	June 21,	July 14,	24	
	"	7	July 15,	July 21,	17	
	"	8	Aug.1,	Aug.14,	14	-- 16
	"	9	Aug.15,	Aug. 21,	7	
KRUSA	Marcel	1	Aug. 22,	Sept. 22,	32	
	"	2	Sept. 23,	Oct. 3,	11	
	"	3	Oct. 4,	Oct. 12,	9	-- 16
	"	4	Oct.13,	Nov. 3,	22	
	"	5	Nov. 4,	Nov. 11,	8	

H - Sector (Albert Code)

Type	No.	Commenced	Ended	No. days	
KRU	6*	Dec.28,1917.	Jan.25,1918.	29	
	7*	Jan.26,1918.	Feb.21,	27	
	8*	Feb.22,	Mar.21,	28	-- 25
	9**	Mar.22,	Apr. 4,	14	
	10	Apr. 5,	Apr.29,	25	
KRUS	11	Apr.30,1918.	May 19,1918.	20	
	12	May 20,1	June 6,	18	-- 21
	13	June 7,	June 30,	24	
	~~14~~	~~June 1,~~	~~July 14,~~	~~15~~	
KRUSA	14	July 1,	July 14,	15	
	15	July 15,	Aug. 6,	23	-- 18
	16	Aug. 7,	Aug. 21,	15	
KRUSA	17	Aug.22,	Sept.16,	26	
	18***	Sept.17,	Oct. 21,	35	-- 27
	19	Oct. 22,	Nov. 11,	21	

* Albert Codes #6, 7, and 8 were called Nancy Code #1, 2, and 3, until the French Code Office informed us that they had applied the name "Albert" to this code.

** Sometimes a code changed at the beginning of an offensive.

*** This code ran longer than any other ~~one~~ KRUSA known. It was at the time of the St. Mihiel operation, when the German organization was completely disrupted evidently.

12
13

It will be noted that the average life of the early codes was much longer as compared with that of the latest codes. The reader will understand by this time the importance of this fact; for the ease of breaking into a code varied directly with the amount of material. In the early codes, when no great difficulties were encountered, the text of one week was sufficient to enable a break to be made into a new code, and by the end of three weeks, messages were being read by us as quickly and almost as completely by the code-office as by the enemy. But when the codes became more and more difficult, and at the same time the life of each one was made shorter and shorter, the amount of information that was received was very greatly reduced.

The question may be raised "how was it determined when the code had changed?" This was not a difficult matter at all, and sometimes was determined even to the exact hour from external evidence alone.

The expert soon acquires a highly trained visual memory without which he is lost in code work. As stated before he must be able to recognize on sight the frequent groups and he should be able to remember their relative positions in messages, even their preceding and succeeding groups, what bigraphs, trigraphs, and polygraphs they form. Certain sequences are familiar to him, and his memory becomes so trained as to enable him even to remember in what message a certain polygraph occurs. Now when the text takes on an unfamiliar, wholly new appearance; when new groups suddenly spring into prominence, with a ~~swift~~ simultaneous disappearance of the old, familiar, frequent groups, together with their combinations, the code man becomes aware of it at once. The change in these codes could be determined to the very day, and it was usual to recognize it not later than the first day after the new code went into effect. The code officers, thereupon notified the chief recording clerk who had a set of new index books prepared and the recording of the new text began at once.

73
74

It should be added that at the end of the summer of 1918, the number of code groups in the trench code had increased so much that the Germans adopted the umlauted letters for use in the second and third letters in code-groups. However, the umlauted letters gave rise to so many errors that it is certain had the armistice not gone into effect so soon, the Germans would have discarded this procedure and would have added another initial letter to the series.

It will be interesting at this point to compare the "Preliminary Remarks" to the early code-books with those applying to the latest.

Compare the following "Preliminary Remarks" to KPUSA Code #153, ~~Exhibit 10~~ Captured September 26th 1918, with those of ~~Exhibit B~~, ~~given on pages~~ ~~---~~ of the ~~early~~ code captured about a year earlier which are given on pages — —

(indent)

PRELIMINARY REMARKS

1. All reports and orders must be encoded by means of the code-book. Clear text may be sent by wireless only in case of extreme necessity.

The mixing of clear text and coded text, as well as the insertion of uncoded numbers, time groups, hyphens or punctuation in the code text is forbidden. Phrases and sentences which may be tramsmitted by one group in the code-book must not be expressed by their individual parts; for example, "IN UNSERER HAND by IN-UNSER HAND.

Words and word-endings which are not absolutely necessary for the understanding are to be omitted in encoding; for example, encode BEI FEIND instead of BEI-M FEIND-E, etc.

2. The code-book consists of the part "Encoding" and the part "Decoding", and contains three-letter groups of which the initial letter is A, K, R, S or U.

a) The part "Encoding" contains the following sections:

IMPORTANT REPORTS
GENERAL REPORTS
STATION AND SERVICE REPORTS
WEATHER REPORTS
PLACE NAMES
MILITARY CODE NAMES
NUMBERS
HOURS OF THE DAY
LETTERS AND SYLLABLES
AUXILIARY SIGNALS
PUNCTUATION
VOCABULARY AND BLIND SIGNALS
SPELLING SYSTEM

77
75

After each section, as well as in the vocabulary, space has been left for the insertion by hand of supplements.

For the military names (Staffs, Formations) only the code names under the "Military Code Names" are to be used, not the real designations. The numbers of the lines in which the code-names for divisions, brigades, regiments and battalions are to be inserted will be determined by the Grukonach (Corps Signal Commander); the remaining code-names will be inserted in places where desired.

In the part "Decoding" the conventional name is to be inserted by hand opposite the six code groups which belong to it. For simplifying this work these are indicated by a pair of crossed

daggers. The use of other code groups for the designation of conventional names and the use of the code groups indicated by the crossed daggers for the designation of other meanings is forbidden.

The names of places must be inserted and provided with code groups by the wireless detachment itself according to its needs. The code-groups which have been provided for such supplements are to be taken from the part "Decoding". The employment of other code-groups by a recourse to groups with new initial letters is forbidden

Such military names and place names as are not provided for in the complete filling in of the code-book are to be transmitted by means of the "System for Spelling out Words", which is found at the end of the part "Encoding".

The Auxiliary Signals are placed immediately after the groups whose meaning is to be changed. For example, if it is desired to encode ANGEFORDERT, the signal for MITTELWORT DER VERGANGENHEIT is placed after the group ANFORDERN; thus, SOA UID.

The Auxiliary Signals will be used only when necessary in order to avoid an error.

Blind Signals are inserted at the foot of every page. Liberal use is to be made of them. Above all they must be inserted at random in frequently recurring, similar or stereotyped reports and orders.

Short messages which consist of only one or very few groups are to be disguised by the addition of several blind groups.

In decoding, these blind groups are merely omitted.

The vocabulary is arranged alphabetically. The umlauted vowels Ä and Ü are also contained in the vocabulary; Ö is treated as O. In adjectives, the group for the uninflected form applies also for the inflected forms; for example, the group for GROSS applies equally for GROSSE, GROSSER, GROSSES, etc. The group for DIESER applies likewise for DIESE, DIESES, DIESEM, DIESEN. The group for the infinitive applies also for example, ABFLAUEN, for FLAUT AB; NEHMEN for NIMMT. Reflexive verbs are to be sought under the verb; for example, SICH, AUSDEHNEN under AUSDEHNEN SICH; SICH EINGRABEN under EINGRABEN SICH. Phrases like AUF DEM RECHTEN FLÜGEL, UNTER FEUER NEHMEN, EIGENE ARTILLERIE, HAT AUFGEHÖRT ZU

indent

SPÄT, are inserted once in the alphabet according to their first word (AUF, UNTER, EIGENE, HAT, ZU), and then again under the succeeding noun, verb, etc. (FLÜGEL, FEUER, ARTILLERIE, AUFHÖREN, SPÄT). In similar manner the frequently recurring forms of the auxiliary verbs and verbs such as IST, WAR, WIRD, KANN, GENOMMEN are to be found once under these forms and then also under the infinitive to which they belong (SEIN, WERDEN, KÖNNEN, NEHMEN).

For the spelling of words which are not contained in the code book individual letters, double letters, and syllables are set forth under the section LETTERS AND SYLLABLES.

The SPELLING of words which are contained in the code-book is forbidden.

16
17

If there are several code groups for a word or a phrase, these groups must be used at random, for example even if the word occurs only once in the message, the group which stands in the first position in the code-book is not to be chosen invariably.

b) The part "Decoding" contains first the three-letter groups with the initial letter A, then those with the initial letter K, R, S and finally with the initial letter U.

At the end of the part "Decoding" there is the Enciphering Table of the "System for Spelling.

3. In a change in Code-Groups it is necessary to pay particular attention that:

1) The change is made in the part "Coding" and the part "Decoding".

2) Those groups whose significance appears in several places (see above; AUF DEM RECHTEM FLÜGEL, UNTER FEUER NEHMEN, ZU SPÄT, IST, WAR, KANN, ETC.) are changed in all the places.

For simplifying this work, these groups whenever they appear twice, are indicated with an asterisk.

As an example of the method of breaking into one of these highly complex codes the following brief description of the steps actually used in the first solutions of the spelling groups in

Albert Code #18 are given. This description was given in a report by the writer under date of Oct. 39, 1918.

The procedure involved the application of no new principles. The steps may be outlined briefly as follows:

1) Determination of Military Units, DECKNAMEN, and PUNKT. The groups representing these were fairly easy to detect from the coloring of the occurrences, in accordance with the scheme previously described. Two probable PUNKTS were located, KDV and KAF.

77
75

2) Determination of the interrogation points and allied groups.

Among the groups studied above there appeared two groups, SZA and AQY, which showed mainly red and yellow, and which were often found in a brief message, often followed shortly thereafter by what appeared to be the answer to the preceding dispatch. The messages containing these groups, moreover, came from various stations, eliminating at once a supposition that the groups concerned were signatures or DECKNAMEN. Accordingly the two groups SZA and AQY were assumed to be "interrogation point". This assumption was corroborated further by a study of the initial groups of the messages concerned; there were found several groups which might well be the interrogatives WO, WIE and WAS, not only from the color as shown in the indexes (green) but also from the fact that they appeared most often in these short messages terminated by the groups SZA or AQY interchangeably. A study of these suspected interrogatives resulted in the identification of the groups for WIE and WO; and these soon led to the identification of AWP as the verb IST. The latter was corroborated by the frequency and color of the group as shown in the index, and also by the fact that several of the short messages mentioned above commenced with the group AWP and terminated with either SZA or AQY.

3) Identification of spelling groups.

The first group sought was AN. In the "Albert" Codes this group does not manifest itself as clearly as in other codes, but it was possible to isolate two groups which looked fair, KIG and AIM, of which the former was the more frequent, with the formula

(18) (see Page--) 38-11-4-4-0-18-1. Both of these groups were followed occasionally, but not frequently, by groups previously determined as Military Units.

78
79
32 33

An attempt was then made to classify by means of the indexes alone some spelling groups without, of course, endeavoring to make any definite identifications. Following the principles elucidated on page---, many were found and these were underlined in green throughout the text. The following message was noted:

xxxxxxxxxxxxxxxxxxxx

1)

		IST			REGT.	=?=
UHW	USK	AWP	UCX	REV	KJZ	AQY

The word W-ER suggested itself for trial for the first two groups. The group USK (formula 27-1-1-5-2-18-0) seemed excellent for ER; and there was nothing to contradict the assumption that the group UHW (formula 14-3-1-0-0-13-2) was W.

Among the messages containing longer chains of spelling groups there were the following:

2) From station GKP to station LNQ time .. 07:30

						ER		IST		WO	
ABL	REB	KJO	KTU	AJV	RGG	USK	KRU	RQQ	AWP	SMN	AGB	KA

SLA AXN

3) From station LNQ to station GKP time ... 08.00

IST		AN	DIV							ER	-?-
AWP	KOM	AIM	APC	UZA	ABL	REB	KJO	KTU	AJV	RGG	USK	SZA

4) From station GKP to station LNQ Time ... 08.25

	AN							
KOM	KIG	SXO	SYU	KJO	KTU	AJV	RGG	KMV	UIJ	AZF

The following suggestions presented themselves:

Message #2 is addressed to some person whose name is spelled out; message #3, directs a question to the sender of message #2, inquiring whether the message is for that person or for ~~some Military Unit~~ Division; message #4, answers the question saying that message #2 is for that person. It seemed therefore that the group KOM might well be FUNKSPRUCH. This group was found in the following message:

5)

AN			IST		-?-
KIG	UFF	URB	AWP	KOM	------SZA

Since UFW appeared only twice throughout the text, and since the two letters F and H may be confused easily (F equals ..-. and H equals ....) it was not too much to assume that this group was really UHW (= W), whereupon it seemed safe to assume URB to equal EN, making the message read "AN-W-EN-IST-FUNKSPRUCH ----?" It may be well to note here that such corrections are often necessary and the assumption of an error in the text on the ground of probabilities alone should not be regarded as gratuitous.

Attention was then directed to the spelling groups forming the name of the person addressed in message #8. First of all it seemed best to try to determine the length of the name. From a consideration of messages #2 and #3 it will be seen that the name certainly ends with the group USK (=ER) and begins either with ABL or REB. It will be recalled that a copy of the code book applying to the text of the preceding "Albert" Code had been captured. In the text decoded by means of it, there occurred the name P*U-TT K-AM-ER, also P-U-T-K-AM-ER and BUTTE-K-AM-ER. This seemed to offer a good clew to the name concerned in the messages under discussion and a trial was therefore made upon this basis. It also seemed best, on consideration of frequency, to split up the groups as follows:

6)	P	U	T(T)	K	AM	ER	
	ABL	REB	KJO	KTU	AJV	RGG	USK

It remained then to attempt a corroboration of these values in other portions of the text. Here are several of the spelling-group chains:

7)	UYU	SJU"	UKB	SUI	RSE	KTP	U KJO	ROR	UFU"		
8)	*	*	*	UKB	SUI	RSE	KTP	U KJO	ART	*	*	*
9)	W UHW	AMA	UIA	=.= KDV	U KJO	UQG	UVV	U KJO	KTP	*	*	*
10)	*	*	*	UKD	AAC	ER USK	UMI	P REB	SUI	AAC	EN URB	
11)	IST AWP	P REB	RKA	UBY	RZE	-?- SZA						
12)	*	*	*	UGU	UBY	RKA	UQG	UKD	AUR			
13)	IST AWP	UFU	FUNKS. KOM	RAP	SUI	K AJV	T(T) KTU	RRQ	-?- AQY			

Message #7 was sent on the 2d day of the life of the code; and if it be supposed that the enemy was following the usual custom of calling in the old code books it seemed that such a message ought to appear in the early text. It may seem perhaps far fetched to have imagined the word S-A-TZ-B-U-CH, given only the assumed and as yet uncorroborated value of KJO as U, but such was nevertheless the case; and the values for the parts of this word were therefore distributed in this message on the basis of frequency and probability, (see page--) thus:

7)

		S	A	TZ	B	U	CH	
UYU	SJU	UKP	SUI	RSE	KTP	KJO	ROR	UFU

Filling in these values in other messages, samples of which are given above, corroboration of most of the assumed identifications were found. Using the preceding examples, some of the steps may be illustrated as follows:

9)

W			-?-	U			U	B		
UHW	AMA	UIA	KDV	KJO	UQG	UVV	KJO	KTP	*	*	*

AMA = I UIA = LL UQG = R UVV = LA

10)

					ER		P	A		EN
*	*	*	UKD	AAC	USK	UMI	REB	SUI	AAC	URB

UKD = BE AAC = SS UMI = AUF

11)

					-?-
IST	P				
AWP	REB	RKA	UBY	RZE	SZA

RKA = O UBY = ST RZE = (DORT?)

12)

				ST	O	R	BE	
*	*	*	UGM	UBY	RKA	UQG	UKD	AUR

UGM = GE AUR = N

15)

								-?-
IST		FUNKS.		A	K	T		
AWP	UWU	KOM	RAD	SUI	AJV	RTU	RRQ	AQY

UWU = ? RAD = T RRQ = (ISCH?)

Once the start was made and the foundation corroborated, additional spelling groups were identified and more words were built up. But it goes without saying that the process of breaking into the code did not go as fast as that described in brief above.

CAMOUFLAGE OF LIAISON.

CAMOUFLAGE OF LIAISON.

It is safe to say that in the early days almost as valuable information was secured from merely an external study of the enemy's wireless traffic as from the actual decipherment and decodement of his messages. It is also safe to say that had the Germans improved and complicated their code without adopting the various measures to be discussed below, information of the highest value could still have been secured without solving a single one of his messages.

A clear idea of the nature of the dangers in connection with an unlimited and unsupervised radio liaison may be gained by reading the documents and extracts which are given at the end of this report.

By a careful study of the weekly reports of the Goniometric Department, beginning with the one for the week ending January 28, 1918, one can gain a good idea of the progressive developments. The whole series of weekly reports form part of the records going with the report of the Goniometric Department.

The important steps by means of which the enemy succeeded in disguising his wireless traffic may be summarized under the following headings:

1) Changes in procedure as regards call signs.
2) Regulations as regards the number and contents and direction, of messages sent each day by means of practice messages, and spurious activity.
3) Regulation and complete standardization of methods.

These will be discussed in order.

---

1) Changes in procedure as regards call signs.

In the early days call signs consisted of combinations of two letters, or a letter and a figure. These call signs were relatively stable; in some cases a station retained the same call sign for more than a month.

Moreover, the German Signal Service was organized upon a somewhat different basis then, the DIFUAS being assigned to divisional areas instead of the divisions themselves, and moving with the latter as was later the case.

It is clear therefore, that once having located a station by goniometry, as long as its call sign remained unchanged, no further bearings needed to be taken. In other words, the location of station was a relatively easy matter. Furthermore, by paying ~~good~~ attention, an observant intercept operator soon learned all the pecualiarities of the stations under surveillance, and could later draw many valuable deductions from any change in procedure, for example, the appearance of new operators.

When all the stations along the front had been charted, as long as no changes in call sign occurred it could be concluded that no change in the distribution of forces was taking place. On the other hand, the appearance of a new callsign, and the prompt location of the station using it as being between two stations previously located would mean that a new unit had been interposed, or a change in distribution of forces had occurred. No comment upon the importance of this information is necessary.

82

The necessity for frequently changing the call-signs becomes apparent, therefore, in order to make it more difficult to determine the location and order of stations. The Germans soon realized this necessity and by the fall of 1917 changes began to take place.

Now when a change in call-sign occurred, it was more or less a general and progressive phenomenon all along the front, the changes being made in succession, and not simultaneously. Therefore, when a general change was made it was easy to follow up the individual stations and note the new calls. Sometimes a warning of a change would be furnished by the enemy himself. For example, this note is found in the weekly report of February 4, 1918, by our Gonio Department:

"A message intercepted on January 27, in Group G-40 man indicate that a change of call signs is being contemplated".

The system of monthly change of call-signs lasted until March, 1918, then the calls began to be changed more frequently. In some places the calls were changed as often as twice a week, and beginning on March 8, a daily change in signs was adopted by the German Fifth Army and Detachment "C".

The following extract from the report for the week ending March 21, 1918, is of interest:

"GENERAL. In connection with the present German offensive we may reasonably assume the following facts to have a direct bearing on it.

During the two weeks preceding the offensive an entirely new system of changing calls daily (see report for week ending March 14th) was adopted by the Germans on the entire Western Front. The adoption of the new scheme on the entire front was calculated to confuse our locations and at the same time to prevent our attention from being attracted to any one certain sector".

On May 11th, 1918, all enemy radio stations adopted three-letter call-signs, with the initial letters D and G for field stations, and W and M for aeroplane-artillery stations. Later other initial letters were added.

On August 1, 1918, a new system of call signs was introduced on the whole front. In addition to the old system of three-letter calls beginning with D, G, M and W, introduced on May 1st, new calls beginning with L, P and T were inaugurated. From a captured document it was found that each station, including power buzzers, was allotted one of these initial letters and a number; the initial letter remained unchanged for a period of ten days; the two final letters of the call changed every day and were obtained from lists which gave a series of pairs of letters for each number. New tables came in force on the 1st, 11th and 21st days of the month. It was so arranged that two station calls with the same pair of final letters could not occur in adjacent armies, and that when such calls did appear in armies not adjacent, the same stations would have the same final two-letter combinations throughout the 10-day period.

Sometimes a station would use several call-signs daily, and it would change wave-length, or tone when giving alternate call-signs; all this was designed to confuse the enemy.

With the daily change in signs, it became necessary to improve all the work in connection with goniometry; and it also became necessary to get out a daily list of field stations, and to adopt new schemes for designating locations.

2) Regulations as regards the number, direction and contents of messages.

This subject is closely bound up with three apparently unrelated things, viz., (a) The details of organization of the German Signal Service, (b) The deductions which can be made merely from the amount of traffic, and (c) The subject of practice messages.

a) It was stated above that at first wireless groups were assigned to divisional areas, and later assigned to the divisions themselves. Now a wireless station is usually located in the vicinity of the post of command which it serves. Since each DIFUA acted as a unit, with the divisional station in charge, by drawing lines between the stations whose locations have been ascertained by goniometry and studying closely the number of messages passing between stations the whole "radio net" of the DIFUA would be ascertained. Thus, the arrangement and location of the units within a division would be disclosed.

A particularly fruitful source of information in the early day lay in a close watch for "General Calls". It used to be the custom when the commanding station had a message to be communicated to all stations in its jurisdiction to send out a general call sign (equivalent to CQ, in international wireless traffic, meaning "Attention! all stations". Immediately after, every station in the net would flash out in turn its call sign, indicating that it was ready to receive. Naturally, by listing each call in turn, the entire radio net would be disclosed. The calling-up by a general call sign was soon strictly prohibited.

Further, since in the early days, communication between DIFUAS was restricted only by the needs of the situation, by observing the imaginary lines across which messages were not sent or only occasionally sent, the boundaries of divisions could be ascertained, also the depth of formation, units in reserve or rest, etc. Likewise Army boundarie

could be ascertained. In other words, the entire enemy Order of Battle could be secured from goniometric date alone. No comment upon the importance of this information is necessary.

In order to destroy this source of information obviously the thing to do was to order messages to be sent across these boundaries. This gave rise to what is called "lateral communication", or"lateral liaison", a phenomenon which began to come into prominence in the Spring of 1918 and continued to be of increasing importance until the end of the war. The nature of the messages which were sent will be taken up later.

84 85 b) As to the second point, regarding the deductions which can be made merely from the amount of traffic, it is easy to see that unless regulative measures be taken, the number of stations and the amount of traffic will be greater in the region where an attack is being prepared than in one where no change is being contemplated; vice versa, in a sector which has just been active and settles down to "rest", the traffic will die down. This is almost elementary in nature and it was not long before the Germans recognized the danger. It became necessary therefore to regulate the amount of traffic which could take place on every portion of the front. This led naturally to the attempts to deceive the enemy by spurious activity; to draw his attention away from the point where an attack was really to take place and center it upon a point of no importance.

This statement which may appear at first thought easy to do, calls for the highest skill and foresight by the director of wireless camouflage operations, and it must be said that on the whole no very successful plan was made by either side because of the very numerous other sources of information outside the control of the director of operations.

The best that could be expected was to maintain activity on a perfectly even level so that an active sector could not be distinguished from an inactive one, nor could one where preparations were in progress for an attack be distinguished from one where no preparations were being made. This could be done best, and was done, by requiring each station to send not more nor less than a given number of messages each day.

c) As to the third point, regarding the nature and importance of practice messages many pages could be devoted to the subject.

THE NATURE AND IMPORTANCE OF PRACTICE MESSAGES

The problem of keeping the station apparatus in good working order and the operators in practice, so that in case of emergency the station can be relied upon to transact business with despatch and with certainty, is a most serious one. In the first place, in order to insure accuracy in the reception and transmission of code messages, operators must be kept in training constantly; and in the second place, in order to insure speed in encoding and decoding, the code personnel must also be kept in training. There is another point which cannot be over-emphasized with respect to the personnel of the coding office: it must realize and be aware of all the dangers to which their code is subject unless all the proper precautions in encoding are closely followed. The only way in which the encoder can avoid making the unnecessary errors which allow an opening for the enemy code expert, is constant practice and a familiarity with his own code. For this reason it is advisable that all of the business of a wireless station be transacted in code by competent experts.

To combine now the requirements necessitated by these three conditions discussed above, viz., that:

1) Messages must be sent across boundaries,
2) " " " limited in number,
3) " " " sent for practice,

a whole system of well regulated wireless activity was maintained by means of practice messages. It is obvious that unless these messages be in the current code in all cases, the purpose for which they were sent would be defeated, since the code experts would be able to tell spurious messages from real ones by their external appearance alone if they were not in the code in effect at the time.

Stations, therefore, were required to send messages to the right and left across boundaries, the number of messages which could be sent was limited, and had to be made up by practice messages in case there were not sufficient real messages to make up the required number,

and these messages had to be in the current code, in the nature of practice messages.

Let us now take up the nature of the practice messages. They may be divided into six types:

(1) Practice tactical or station operation messages.

As this heading indicates, these messages were put up exactly the same as though they were real tactical messages, there was added some group designating the message to be "practice". Such designations were usually:

DIES IST EIN UEBUNG FUNKSPRUCH OHNE SINN	(1 code group)
OHNE S-IN-N	(4-5 code groups)
UEBUNG FUNKSPRUCH	(2 code groups)
Ü FUNKSPRUCH	(2 code groups)
UEBUNK G	(1 code group)
O-S	(2 code groups)

2) Proverbs, greetings, jokes and the like.

Without question, the sending of proverbs as practice messages was of the greatest aid in the early days to the solution of a code, because most of the material in such messages had to be spelled out. In fact such messages formed veritable mines of information. Added to this, the fact that the Germans had a predilection for repeating certain proverbs many times, as stated above, the establishment of a single letter often resulted in locating these proverbs and thus in turn, the solution of a whole series of important spelling groups in a new code was effected.

In these proverbs and greetings the operators were at times either careless about spelling, or purposely jocular, affording us some amusement on occasions such as these:

WAS M*8 DIE....	KAUM-ER-AD
R-U-F-MAH-MEN	8-UNG
UHR-LA-U-B	K-UN-HEIT
DIE-CH	etc. etc.
H-UHR-A	

Another great aid found not only in these practice messages but also in real tactical messages was the spelling out of words

containing
~~using~~ commonly used short words in combination with spelling groups. Such practice was beneficial to us, therefore, from the standpoint of aiding in the solution of not only spelling groups but also many important short words. A few examples of this are the following:

AUF-P-A-SS-EN	UEBER*HAUPT	UM-GEHEN-D
AB-GE-SCH-LAGE-N	HE-IST	MIT-WO-CH
DEUTCH-L-AN-D	NIE-MANN-D	GE-S-UND
K-R-AN-K	JE-DEN	M-UNTER
ER-S-A-TZ	K-AM-ER-A-D	FEST-UNG
AM-ER-I-KANN-ER	SCH-MIT	ALLE-S
GE-WO-R-DEN	M-A-SCH-IN-E	BE-H-ALT-ET
	N-O-T-VER-FAHREN	WO-H-L

3) Fictitious messages.

By such a message is meant one which is composed of bona-fide code groups, belonging to the code, but which were simply chosen at random. The messages never made any sense. Two examples are the following:

LA HAIE L'EVE QUE	PRÜ- FUNG	(BLANK CODE GROUP)	(BLANK CODE GROUP	13 UHR NACHTS	VOR- DERE LINIE	U	CK	BE- TREFFS					
KFO	KIC	RCI	RKA	UND	KOE	URJ	UCB	RZB					
	BE		WETTER VOR-			RE-		WO	(BLANK CODE				
" UBER	MERK EN	AB LOSUNG	HER- SAGE	REGR. G1	LI- BELLE	MIERES WALD	UNG	STEHT IHR?	GROUP)				
RVC	ADO	AKZ	RMK	AAY	RXD	KMW	KHQ	KWP	PKE				

A lazy operator (or perhaps a crafty one!) would sometimes open the code book at a given page and send a series of code groups chosen at random. Three examples of such messages found in Albert Code #17, which were decoded by means of a captured code book, are as follows:

	N	NK	NT	OIS	NEU	NES	ND	HT	ME	11	ON	OE	NIE	*
1)	RZN	SEP	UZO	RLR	RMZ	RGP	RSH	RKI	KSF	RKF	AMW	AAK	ARU	SE

* DIES IST EIN UEBUNG FUNKSPRUCH OHNE SINN

	=.=	=,=	=:=	=?=	=!=	=-=	=/=	=_=	=()=
2)	ALC	AJQ	SMZ	STT	UOQ	SOX	ASQ	AOG	ASM

T-9

	AB- SCHWA CHEN	AB- WECHS- ELND			BE- LEUCH- TUNGS				BE- WEG-	BI- VA
3)	KAP	UEY	ÜBUNG RJB	BEIDE STY	MATERIAL KQQ	BRENN- PUNKT RAV	CHAUS- SEE UDO	BRIEF- TAUBEN KHK	UNG AWR	IFRE SI

4) Artificial Messages.

These are simply drawn up without reference to the code book at all and made to resemble bonafide code groups. A good example of an artificial message found in Albert Code 17, is the following, i which it will be noted that the letter B, is the middle letter of nearl every group:

RIE KBI KBL KBX KNQ RBV ABR SBX RII

Various other peculiarities of a similar nature were encountered. Such messages always have a peculiar appearance and are not hard to isolate.

5) Distorted messages.

Mention has been made above concerning the transposition of code-groups within a message and the great difficulties which such procedure set in the way of solution. Example of such distorted messages are as follows:

*	VER	DIE	NACHT	IE	ZIEM- LUCH	1	F	RUHIG	MANN	3
	RCC	SLO	UUD	KQU	SIH	UPV	AGF	KPJ	ATW	UCM	UGZ

UND	LEICHT VERWUNDET	SCHWER VERWUNDET	6	*
AYM	RXE	STX	SGA	SHY

* Distortion signal?

The reconstructed message reads as follows:

* DIE NACHT VERLIEF ZIEMLICH RUHIG. 3 MANN LEICHT VERWUNDET UND 6 SCHWER VERWUNDET *

INF. BRIG.T	(BLANK CODE GROUP) RBT	(BLANK CODE GROUP KHC	HIN- TER GEL- ANDE	STELL- UNG	BEN	O	
AAX	FEIND- LICHER FLIE-		ACO	UFW	SWB	KUE	
NACHT	GER	HEUTE	M	UND	(BLANK CODE GROUP	AUF	B
KQU	AKH	SER	KLO	AYM	REV	UCZ	REC

Infantry Brigade G. HEUTE NACHT, BOMBEN UND FEINDLICHER FLIEGER AUF eaps HINTERGELANDE STELLUNG.

001

90

DIV.G	GE	BLIND GROUP	SIND	BLIND GROUP	TRUPPE	TZ	N
AAV	UYL	RGD	KCX	UKR	SPH	AMA	RZN
BLIND GROUP	UNSER	SE	E	T	IN	BLIND GROUP	MARSCH
AKP	UUN	AWZ	SAX	ASN	SWF	RGH	

DIV.G. UNSER-E TRUPPE-N SIND IN MARSCH GE-SE-TZ-T

DER	BLANK GROUP	WASSER	W	BRAU-CHEN	SS	DRING-END
ADS	REZ	RAI	RGB	UAU	SZY	KEV
PUMPE	EIN	ENT	ZUM	ER	BLIND GROUP	
AJB	RVE	KEO	KOW	UQT	UKL	

STOL-LEN	N	(BLANK CODE GROUP)	A
SJY	RZN	RJV	RQU

ERAUCHEN DRINGEND EIN WASSER PUMPE ZUM ENTWAESSERN DER STOLLEN

6) Blind Group Chains.

(61) These have been taken up before. (See Page--) Toward the end of October such messages were never encountered, and it would seem that the practice was prohibited.

The third point in regard to the camouflage of liaison deals with the regulation and complete standardization of methods on the whole front. The purpose of this was to prevent deductions being made from variations in procedure which may have been characteristic of certain units; whole movements were often traced by means of them. It is easy to see that the constant sending of stereotyped messages, or messages signed by a name allowed the enemy to follow the unit to which the station was attached from place to place. Illuminating examples may be found in the documents attached.

Especially regulated was the procedure attendant upon the relief of a unit. Care was taken not only before a relief, but long after, so that no indications of it be given. This was accomplished by retaining all conventional names, by retaining the station personnel for a certain length of time after the relief had been completed, and by continuing all procedure exactly as before. The Germans were rather successful in this particular on account of the complete standardization and strict supervision of methods.

Among the documents captured during an attack was a record book in which the messages sent and received by a radio station between August 25 and September 11, 1918, are given in order. It happened that a code-book was also captured and it will be interesting to see the sort of traffic that was carried on by this station which, during the period mentioned, was located in a very quiet sector. We will give only the messages handled by this station during one day, and in the form in which they appeared on the sheet. Of course, the decodements were not on the sheet.

Were it not for the fact that three of the messages make sense one would be justified in questioning whether the correct code had been applied, so great was the number of spurious messages.
Note that touch of "reality" is added to the fictitious messages by prefixing and suffixing what are apparently code groups for conventional names. GNW, the receiving station was located in H-40, and the locations of the sending stations are added in parenthesis after the signature.

11/9 Ub. Funksp. Empfang 0125

GNW - 01.05 - CHI-18

DECK-NAMEN	5.30 P.M.	AUS-SERE	DECK-NAMEN	STADT	30	GEG-NER	DECK-NAMEN		
RJB	SLL	RUK	RBB	UFV	AKG	KMT	RDH	GAM	

(Station in H-40)

Ub. Funksp. Empfang 0959

GNW 0930 CHI-10

SE AWZ	GENEH-MIG-UNG KIT	BLIND GROUP KMV	DECK-NAMEN RCI	AU AAB	DRAHT SHZ	AUF-SAK SCHIE-BER UIK	DECK-NAMEN REB	76 SAT	BLIND GROUP AGX	DSÄ

(Station in H

11

Ub. Funksp. Befördert 1003

92 DSÄ 0950 CHI-10

WANN ALM	VU IST AKK KBQ	UB. MELD. SOV	K RBI	DECK-BLIND ET KQO	GROUP RDH	ABS- 1:2500 CHNITT : KDS	AVW	SXO	DECK-NAMEN RCI	GNW

"Ub. Funksp. Empfangen 1512

GNW 1510 CHI-9

B	L	ØE	D	S	I	NN	BLIND GROUP	DECK-NAMEN	
ATH	AGF	AAK	ANF	AAG	AAR	ANO	AEP	RBB	DOK

(Station in H-40)

"Ub. Funksp. Befördert 19:20

GAM 1900 CHI-10

DECK-NAMEN	FEUER-UEBER-FALL	Ø	4:30 A.M.	MELDE GÄNGER	RAD FAHRER	RAD FAHRER	SP. 16	EIN-ZEHN	DECK-NAMEN	
RCI	KCQ	KHT	RFA	SLV	SKS	UFU	AVJ	AST	RDH	GNW

"Ub. Funksp. Befördert 1923

DOK 1915 CHI-8

DECK-NAMEN	DECK-NAMEN	TREN-NUNGS-STRICH	KA-NONE	VER	4:30 A.M.	SIG-NALE WERFER	TRINK-WASSER	
RDJ	RCI	USD	AVJ	SLO	KVI	RIM	AGI	GNW

"Ub. Funksp. Empfang 1923

GNW 1920 CHI-11

U	DAG-EGEN	HABEN	BLIND GROUP	S	GE	SCH	A	F	T	DECK-NAMEN	
URJ	AMV	AOF	RCI	AAG	UYL	RKY	ALV	UYZ	ASN	RBB	DOK

"Ub. Funksp. Empfang 2102

GNW

DECK-NAMEN	KARTE	SIE-BENTE	BAT-TERIE	BLIND GROUP	EIN	FRGE-NEIS	STEIL-FEUER	FAST	GASAN-GRIFF	KRAF-TIG	BLIND GROUP
RCI	KAL	SAT	UHR	KQX	ALP	ARM	RIT	AFT	AET	RRD	KST

DSA

12
13

"Ub. Funksp. Befördert 22.48

DSA

DECK-NAMEN	SIND	DIE	6	M	AR	K	GUT	AN	KOM-MEN	DECK-NAMEN	
RJB	KCX	RZY	SGA	UDW	SZA	APL	UUQ	AXT	UWS	RBB	GNW

CONCLUSION

It is difficult for the writer to make a good estimate of the Three-Letter Code as a system of secret communication. At first, whe the codes were simple, and no artificial difficulties were put in the way of decodement the amount of valuable material which was secured from a study of the text was only limited by the life of the code. The longer it lasted, the more information was secured. Later, when the dangers of unrestricted and unsupervised wireless traffic were recognized; when messages were made shorter, and greater care was taken to prevent loopholes for the decoder, the amount of information which was secured depended a great deal upon whether the text was coming from an active or a quiet sector. In the former case it was difficult to disguise real traffic; urgent moments arose when rules were forgotten; spurious activity was discarded and every message was a real one. It was always possible to break into such a code, notwithstanding the large number of variants, etc., because the characteristics of the most important groups would manifest themselves despite all regulation and carefulness.

In the latter case, in a quiet sector, the text was of a totally different complexion. Here spurious activity, tricks, fake messages, etc. were rampant. Such text presented a rather hopeless case.

Now it happened that the activities of this section were restricted, ffrom May to September 1918, to the text coming from a quiet sector. ~~Xxr We~~ were always waiting for the "big show" to take place, for then we knew that the case would present greater possibilitits. Immediately after the St. Mihiel offensive began the text took on a new appearance. Messages at once became longer, groups began to stand out and the attack on the code was begun with high hopes of success. These hopes were soon dispelled, for the whole affair was over very shortly, and the Germans returned to their old tricks of camouflaging wireless traffic. Then came the armistice, and the end of all activity.

In the light of this limited experience it is impossible to say absolutely what the degree of security offered by such a highly developed system really is. There is no doubt but that it is

very great. There is no doubt but that with the proper precautions, careful supervision and control the employment of such a code by trained men offers the highest possible security for secret communication on the field of battle.

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

94

95

THE THREE-NUMBER CODE

For most of the material forming the basis of the following exposition, the writer is indebted to Second Lt. J. F. Gunster, Infantry, who made a preliminary report on the subject. Many valuable suggestions were added by Capt. P. B. Whitehead, F. A. I take pleasure in acknowledging indebtedness to these two officers for their aid.

As stated in Section ___, the Three-Number Code was intended for use in all forms of communication within or to and from the three kilometer Danger Zone; it was designed, in other words, to meet the requirements for communication in the region from which the Three-Letter Code and all other means of liaison were specifically excluded.

Although this code was not put into use until March, the plans for its employment were fully completed by the German General Staff before January 22, 1918, and were published in Part 10 of their MANUAL OF POSITION WARFARE FOR ALL ARMS, under the heading SIGNAL SERVICE TRAFFIC REGULATIONS, a translation of which is attached to this report, as Exhibit 7. In this document, the last ten pages were devoted to a description of the SCHLUESSELHEFT, the name which the Germans applied to the book which forms the basis of what we have called the Three-Number Code. A captured copy is attached to the report, as Exhibit 8.

It will be well to set forth this description inasmuch as it explains in detail very clearly how the code-book was to be used.

TRANSLATION

"Directions for the Use of the ~~Three-Number Code-Book~~ SCHLUESSELHEFT.

~~(German: SCHLUESSELHEFT)~~*

The ~~Three-Number Code-Book~~ SCHLUESSELHEFT contains a list of sentences, words, letters, numbers, etc., for the construction of the messages necessary on the battle-field. The transmission of messages is

done by means of letter or figure designations.

Fundamental changes of the code-book are forbidden.

The employment of the code-book for encoding without the use of the Secret Key consists in the following:

a) Replacing the text arranged under the headings of "General Traffic Signals" and "Signals for Aeroplane Service" by the letters opposite them.

Example:

INFANTERIE IN MARSCHKOLONNE - IM

b) Transmitting the combinations of three figures which in the code-book represent the words and sentences of the other signals that may be sent.

Example:

GEGNER GEHT ZURUECK - 153

The transmitter sets down in front of the encoded message the syllable "GR" (Groups) and the number of three-figure groups of which the message consists. Thus "GR.7" means that the message consists of seven three-figure groups.

The employment of the code-book for decoding, without use of the Secret Key is as follows:

a) In place of the letters received, the text corresponding to the combination in the code-book is set down.

Example:

153 - GEGNER GEHT ZURUECK

In order to render the transmission of important messages during the exigencies of the moment more safe than is the case with the system given above under b, the basic signals of the code-book can be re-enciphered. Decision in this regard concerns the sending station. This encipherment is accomplished with the aid of a Secret Key (GEHEIMKLAPPE, literally, secret-flap", or "secret fly-leaf") provided on the last page of the code-book. The message enciphered in this manner still offer security as regards keeping the contents secret from the enemy even after the loss of a code-book, as soon as a new Secret Key is inserted in the place of the lost key.

97

The use of the code-book without the Secret Key represents not a secret writing, but merely an abbreviated writing.

The Secret Key consists of two tables of numbers. The upper table serves for the enciphering; the lower one for deciphering.

Words which are not contained in the code-book may be built by putting together the letters and syllables found on pages 22 and 23 of the code-book.

Only the designations consisting of numbers can be enciphered. This is done in the following manner:

First the words or sentences are replaced by the three-figure groups standing opposite them, as explained above.

Example:

GEGNER GEHT ZURUECK - 153

Then one applies the following system:

In the Secret Key, on the left hand margin of the upper numerical table, one looks for the first figure of the number to be enciphered, that is the figure 1.

Next, one looks for the second figure of the number to be enciphered in the upper margin of the upper table, that is, the figure 5.

	0	1	2	3	4	5	etc.
0							
1							
etc.							

If one proceeds toward the right, carrying the finger along the row beginning with 1, until one finds oneself under the number 5, one arrives at a number (04), which is written down:

	0	1	2	3	4	5	etc:
0							
1						04	
etc:							

To this number (04) is added the last figure of the number to be enciphered; that is, in the preceding example, 3. The number thus found (043) is then transmitted.

In order to indicate to the receiver that the message following is enciphered, the transmitter places before the enciphered contents the syllable "CHI" (that is, CHIFFRIERT). Thus, for example, CHI GR 13 indicates that the message contains 13 enciphered three-figure groups.

If messages with the prefix CHI are to be read, for example the number 043, then one proceeds as follows:

One seeks in the lower table of numbers:

a) On the left hand margin the first figure of the number to be deciphered, i.e., 0.

b) On the upper margin the second figure of the number to be deciphered, i.e., 4.

	0	1	2	3	4	etc:
0						
etc:						

If one proceeds with the finger along the line determined by 0 to the right, then one finds under 4, a number (15) which is written down:

	0	1	2	3	4	etc:
0					15	
etc:						

79

To this number, one adds the last figure of the number to be deciphered (043), that is 3. The number thus found ($15\overset{3}{\wedge}$) is then sought in the code-book, and the corresponding text is taken:

153 - GEGNER GEHT ZURUECK

PRODUCTION OF THE SECRET KEY

The Secret Keys are produced by an authority of the Higher Command--as a rule, the Division--and are issued to the authorities of the subordinate commands and the troops. For the simplification of the production, printed Secret Key blanks are kept in readiness at the Army Signal Service Parks; before issuing to troops it is only necessary to fill out the 100 inner squares of the tables of numbers.

a) Upper table (Enciphering Table)

First, the numbers 0 to 9 are written on the left margin of the table, from the top toward the bottom; on the upper margin of the table from left to right.

Next, the numbers from 00 to 99 are written at random within the 100 squares of the table.

b) Lower table (Deciphering Table).

First, the numbers 0 to 9 are written on the left margin of the table from the top toward the bottom;
on the upper margin of the table from left to right.

Next, the numbers from 00 to 99 corresponding in their position in the upper table (the enciphering table) are inserted in the 100 squares of the lower table.

Example:

If in the upper table the number 06 is located at the intersection of the horizontal row determined by 2 and the vertical column determined by 7,

.	1	2	3	4	5	6	7	etc:
0								
1								
2							06	
etc.								

then in the lower table, the number 27 is to be written at the intersection of the horizontal row determined by 0 and the vertical column determined by 6.

.	0	1	2	3	4	5	6	etc:
0							27	
1								
etc:								

In order to allow for the quickest possible transmission of a message consisting of numbers, where the connection is working well, it is permissible to send in abbreviated Morse Signals, since transmission by means of the latter saves much time. For details, see Page 4 of the code-book.

In order to indicate openly that the abbreviated Morse Signals have been used, the prefix Z is necessary at the beginning of the message; for example, in an enciphered message CHI GR 9 Z, or in an unenciphered one, GR 5 Z.

The time at which the transmitted message was drawn up is indicated at the beginning of the message by prefixing a "time-group".

This time-group is a four-place number. The first two figures indicate the hours from 0 to 23, counting from midnight to midnight; the last two figures, the minutes. If the hours or minutes are single figures, the first and the third figures become a zero.

101

Examples:

Time of despatch from the post of Command

AT TOP OF TELEGRAPH BLANK	TIME-GROUP
12.25 Morning	00.25
09.05 A.M.	09.05
13.38 P.M.	13.38
03.00 P.M.	15.00
10.03 Evening	22.03

If the message is not of the same day, then the date is placed in parenthesis before the time-group. For example:

(9) 22.30 CHI 15, etc.

So much for the directions as given by the Germans themselves. No further explanation of the method of using the first and second parts of the code book ("General Traffic Signals" and "Signals for Aeroplane Service") is necessary, and they do not concern us further. They can hardly be said to pertain to code or cipher work.

We will therefore turn our attention immediately to the code part proper of this system.

To review what has been said previously, the outstanding features which distinguish the Three-Number Code from the Three-Letter Code are these:

1) In the former, the code-book contents run alphabetically and numerically, thus conforming to the type of code requiring but one book, which serves both for encoding and decoding;

2) The form and contents of the code book remain constant, and secrecy is attained by an enciphering process which makes use of a variable, enciphering table. The Three-Number Code, therefore, represents in its most complete form, a good example of enciphered code. Although a copy of the code-book itself was soon captured, the form and contents of the book remained unchanged since its introduction, and have therefore been termed the BASE. Various inserted typewritten or handwritten supplements were pre-

pared by the different divisions to cover the names of units and places, and these supplements naturally varied for each division and changed from time to time.

Whereas the solution of the Three-Letter Code involved the reconstruction of the code-book, the solution of the Three-Number Code involved only the reconstruction of the enciphering table, and was therefore a deciphering process in reality, since the code contents, immediately after the capture of a single copy, became in the nature of clear text.

It will be noted that the instructions as published by the High Command, with regard to the use of this code-book permitted the sending of messages without the use of the Secret Key, where special secrecy was not necessary. As a result many messages were sent unenciphered, and, therefore, in what we shall designate as the "base" that is, the unchanging part of the system. It happened occasionally, too, that a careless or an ignorant operator would send a message in the base and later repeat the message in the enciphered form, or vice versa. Often, too, an operator would, after sending an enciphered message in one key, repeat it in another Secret Key. All these blunders were of great aid to us.

Messages, both when in the base, or when enciphered sometimes underwent a further simple encipherment in which letters were substituted for figures, according to the following key:

0 1 2 3 4 5 6 7 8 9
T A U V R E S B D N

This simple key came into use about the same time as this code, but offered no difficulty because it never changed and because often the same message would be sent both by letters and numbers.

The first break made into this code was remarkable for its almost dramatic illustration how the carelessness and ignorance of a single individual responsible for the coding of communications may jeopardize the lives of hundreds of men by committing the inexcusable blunder of cryptography: repeating a message in almost its exact form, but in another system.

12
103

Here are the facts and the telegrams:

The messages of an obviously new system appeared along the entire Western Front on March 10 and 11, 1918. The intercepted despatches of the first day's traffic along the Verdun Front, March 11, were turned over to one of our officers and a short study proved the new text to be code. The main factor in this, of course, was the finding of groups which appeared as three-figure combinations many times, and in analogous positions.

Among these first messages, which were being studied from the original telegraph blanks, there appeared the following despatch:

ÄN v X2 (Souilly 0040) 0035 CHI-13

845 422 373 782 240 245 068 652 781 245 659 659 504

On the same telegram there also appeared the following:

X2 v ÄN (Souilly 0052) 0035 CHI-13

OS RGV KZD

The second message was recognized as containing two groups which belonged to the Three-Letter Code, while the combinations OS was the German abbreviation for OHNE SINN. The officer immediately referred to the current Three-Letter Code text to see whether the two groups RGV and KZD had been solved. He found that the former represented the word ALT, but no meaning had yet been found for the second group.

These were the mental steps which he took: Here is a message in a new code sent by station X2 to Station ÄN. About 10 minutes later (shown by the time of interception given by the station at Souilly) ÄN sends a message to X2, saying substantially the following:

"Your 0035 CHI-13 is without sense". Then he adds, in another code: "Old -----" What could the unknown group, KZD, mean? Clearly, it referred to some other system of communication. The word VERZIFFERUNG suggested itself almost immediately. The group KZD occurred in only one other place in the entire Three-Letter Code text, but in that place it fitted in well with the context.

103
104

It seemed then, that station ĀN had told X3 that his message in the new code could not be decoded and asked that he send it in the old code.

A search was made immediately among the messages of the Three-Letter Code text that day, and it seemed almost too good to be true that the following message should have been intercepted:

ĀN v X2 (Souilly 0057) 0025 CHI-14

UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB KUU UQX UFQ RQK

Note particularly the correspondence between the hours as given in these three telegrams. Now the Three-Letter Code to which this message belonged was already partially solved and this message was at once decoded insofar as it was then possible. Fortunately it contained mostly spelling groups. It was as follows:

AN		U.M.	2		H	I	R	SCH	=.=	W	I	TT	E
UYC	REM	KUL	RHI	KWZ	RLF	RNQ	KRD	RVJ	UOB	KUU	UQX	UFQ	RQK

Again it seemed almost too good to be true that the message in the new code should be almost exactly the same in form as this decoded message. Still such was the case. Note below the internal evidences in the messages; the repetition of the group 659, which stands for T; the equivalent in the other code is the group UFQ, which stands for TT. Note the repetition of the group 245, which stands for I. The message in the new code was therefore tentatively solved as shown below, in comparison with the other message:

AN		U.M.	2		H	I	R	SCH	=.=	W	I	TT	E
UYC	REM	KUL	RHI	KWZ	RLF	RNQ	KRD	RVJ	UDB	KUU	UQX	UFQ	RQK

AN		U.M.	2		H	I	R	SCH		W	I	T	T	E
845	422	373	792		240	245	068	652		781	245	659	659	504

These solutions were telegraphed immediately to the French Code Office. We had not as yet adopted a method of secret communication by telegraph with the British Code Office, and it may be interesting to note that to add to the dramatic situation, these solutions were despatched to the British by a special aeroplane.

This first break was sufficient. The new code was attacked at once, using the same principles as those concerned in

the solving of the Three-Letter Code. The principal classes of groups soon manifested themselves and it was speedily recognized that the arrangement in the code book was systematic and mostly alphabetical. For example, it was first noted that the third figure in code groups representing numbers was always the same as the number itself, though the first two figures in each combination varied with different keys. Thus, for example, in one key the various code groups were as follows:

790 = 0
791 = 1
792 = 2
793 = 3
794 = 4
etc.

The spelling groups "alphabetically related" also showed a consecutive arrangement. For example:

DEN	= 360		H	= 480	
DER	= 361		HE	= 481	
DES	= 362		HEIT	= 482	
DIE	= 363		I	= 485	
E	= 364		ICH	= 486	
EI	= 366		IST	= 488	etc., etc.

Words likewise exhibited similar relations:

BAHN = 708
BATALLION = 709
BATTERIE = 620
BEFEHL = 621
BEI = 622 etc., etc.

It was readily apparent, after the same phenomena had been discovered in what were clearly other "keys", that as regards the enciphering process, each code group may be considered as being divided into two parts; the first part consisting of a variable two-figure number, and the second part, of an invariable digit.

This naturally led to the conclusion that the system consisted of a basic code of three-figure groups applied consecutively to the contents of the book, the latter being arranged strictly alphabetically; that, furthermore, in the enciphering process, only the first two numbers (the variable two-place numbers) were enciphered, while the third remained unchanged.

From all these clues the nature of the system was quickly comprehended, and when on the 25th of March the French captured a copy of the code-book full confirmation of these various theories was at hand. To the French really belongs the credit of being the first to recognize these clues pointed out above. It now became desirable to develop the best system for the attack of messages in new keys. That was thenceforth our only real problem. The first thing done was the stencilling of the Base, with the exception of the words and phrases, on three large sheets of paper with all of the groups represented by the same two-place number, or "radical" in a horizontal line as, e.g.,

	0	1	2	3	
25	A	A	AM	AN	etc
26	C	CH	CHE	CHEN	

These sheets (samples attached) were fastened on a triptic and set in front of each worker, where they could be consulted without the need of any page-turning or other delay or inconvenience.

This was simply a more convenient arrangement from a deciphering and decoding point of view. The columns represented then the invariable portion of the code-book, while the two-place numbers, or "radicals" represented the variable, or enciphered portion. Solution would involve merely the finding of the correct equivalent for each of the one hundred radicals.

All numbers above 12 except the round numbers 15, 20, 25, 30, 40, 45, 50, 60, 70, 80, 90, 100 and 1000 had to be put together from the digits.

METHODS OF SOLUTION.

Following along the lines indicated in the methods of solving the Three-Letter Code we may divide the entire body of text in this code into three main sets of groups, which are:

1) Numbers
2) Spelling groups
3) Words, phrases and sentences.

Solution consists in the same two steps:

1) Classification
2) Identification.

NUMBERS

The classification of numbers was exceedingly simple. The most frequently used numbers being 0 to 9, and having the same

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES
GENERAL STAFF, SECOND SECTION (G.2,A.6) (asm)

(DISTRIBUTION "A") July 31, 1918.

BASE.	0	1	2	3	4	5	6	7	8	9
25	A	Ä	AM	AN	AR	AU	AUS	B	BE	BEN
26	C	CH	CHE	CHEN	CHT	D	DA	DASS	DE	DEM
27	DEN	DER	DES	DIE	E	E'	EI	EIN	EL	EN
28	ENT	ER	ES	EU	F	FÜR	G	GR	GEGEN	GEN
29	H	HE	HEIT	HER	HIN	I	ICH	IS	IST	J
30	K	KEIT	L	LE	M	N	NACH	ND	NE	NEN
31	NS	NU	O	Ö	OB	P	Q	QU	R	RE
32	RÜCK	S	SCH	SE	SEIT	SEN	SICH	SO	ST	T
33	TEL	TEN	U	Ü	UM	UN	UNG	UNS	V	VER
34	VOR	W	WEG	WIE	WIR	WO	X	Y	Z	ZER
35	0	1	2	3	4	5	6	7	8	9
36	10	11	12	15	20	25	30	40	45	50
37	60	70	80	90	100	1000	MAL	TER TE TES	ROMISCH	12 UHR NACHTS
38	1 UHR V.M.T.	3 UHR V.M.T.	3 UHR V.M.T.	4 UHR V.M.T.	5 UHR V.M.T.	6 UHR V.M.T.	7 UHR V.M.T.	8 UHR V.M.T.	9 UHR V.M.T.	10 UHR V.M.T.
	11 UHR V.M.T.	13 UHR MITTAG	1 UHR N.M.T.	2 UHR N.M.T.	3 UHR N.M.T.	4 UHR N.M.T.	5 UHR N.M.T.	6 UHR N.M.T.	7 UHR N.M.T.	8 UHR N.M.T.

BASE	0	1	2	3	4	5	6	7	8	9
40	9 UHR N.M.T.	10 UHR N.M.T.	11 UHR N.M.T.	AB	ABBRE-CHEN	ABEND	ABFEU-ERN	ABSCH-LAGEN	AB-LÖSEN	ABLOS-UNG
41	ABSCH-NITT	ABTEIL-UNG	ALARM	ALLEIN	ALL-GEMEIN	AN AM	ANGREI-FEN	AN-GRIFF	ANSCH-LUSS	ARTIL-LERIE
42	A.GR.	A.KDR.	A.M.	A.U.GR	AUF	AUF-SATZS.	AUF-SCHLAG	A.Z.	AUS-LADUNG	
43										
44								BAGA-GEN	BAHN	BATAIL-LON
45	BAT.	BEFEHL	BEI BEIM	BEOB-ACHTEN	BEOB-ACHTER	BEOB. GUT	BEOB. UNMÖG.	BEOB. STELLE	BEREIT-SCHAFT	B.T.K.
46	BESCHÄ-DIGT	BESCH-IESSEN	BE-SETZEN	BEWEG-UNG	- - - -	BIS	BLAU	BLAU-PUNKT	BLINDE GÄNGER	BOGEN-SCHUSS
47	BRENN-LÄNGE	B.Z.	BRIEF-TAUBE	BRIG.	BRÜCKE					
48										
49	CHIF.		DAUER-FEUER	DECK-UNG	DICHT	DIVI-SION	DRAHT-H'NIS	DRIN-GEND	1/3	DUNST
50	DURCH							EIGEN	EIN-SCHIES.	EINZEL FEUER
51	ENT-FERN'G	ER ES	ERBETEN	ER-HÖHUNG						
52			FALLEN	FEIND	FEIND-LICH	FELD-KÜCHE	FELD-WACHE	FERN-SPR-ER	F.SPR. LEIT.	F. SPRUCH
53	F.BAL	FEUER	FEUER-BEREICH	FEUER-BEREIT	FEUERN	FEUER PAUSE	" F.Ü.F.	FBSCH.	FLIE-GER	-?-
54	FRAG-LICH	FRONT	F.T.ST.	FÜHRER	FUNK-SPRUCH					
55			GANZ	G.AN-GRIFF	G.FLA.	G.G.	G.MINE	GEBEN	GEFANG-EN	GEF. STD.
56	GEGEN-STOSS	GELB	GESCHOS-SART	GE-" SCHUTZ	GESCH. FEUER	GESCH. WEISE	GES-TERN	GEWEHR	" GEWÖHN LICH	GEW. FEUER
57	GRABEN	GRABEN KANONE	GRAD	GRA-NATE	GR. WERFER	GROSS	GRUND-RICHT'G	" GRÜN	GRUPPE	GUT
58								HABEN	HALB	" HÄLFTE
59	HALTEN	HAND-GR.	HAUB. BAT.	HAUB.	HAUPTM.	HAPT-RICHT'G	HEUTE	HIER	HILF ZIEL	HINDER-NIS
60	HINTER HINTEN	H. GE-LÄNDE	HOCH	" HÖHE		" HÖHER				
61								IN IM	IM GANZEN	IM ZIEL
62	INF.	INF. FEUER	INF. FLIEGER	INF. MUN.	IST					
63			KALI-BER	K.T.K.	KANN	KANONE	K.BAT.	KARTE	KEIN	KLEIN
64	KL. QUAD.	KOMMA	KDR.	KOM-MANDO	KOM-MEN	KOM-PAGNIE	KRANK-ENTR.	KURZ KURZER		
65								LADEN	LADUNG	LAGE
66	LAGEN-WEISE	LAGER	LANG LÄNGE	L.GR.	LANG-SAM	LEBE	LEB-			

BASE	0	1	2	3	4	5	6	7	8	9
70	M.W.	MINUTE	MIT	MITTAG	MITTE	MITTER-NACHT	MITT-LERE	M.V.	MORGEN	MRS.
71	MUNI-TION	-								
72			NACH	NACH BAR	N-M-TAGS	NÄHER	NÄCHSTE LAGE	NACHT	NEBEL	NEHMEN
73	NEIN	N.Z.	NICHT	NÖRDL. NORDEN	NORD-NADEL					
74								ODER	OFF.	OHNE
75	O.V.	ÖSTL. OSTEN						PATR.	PION.	PLAN-QUAD.
76	POSTEN	PUNKT						Q.SCH.	QUAR-TIER	
77			RÄUMEN	RECHTS	REGI-MENT	REGLER	RE-SERVE	RICH-TIG	RICHT-KREIS	RICHT-UNG
78	R.N.S.	RIEGEL	ROHRE FREI	ROLL-SALVE	ROT	ROT PUNKT	RUHIG			
79								SALVE	SAPPE	SAUER-STOFF
80	SCH.AR. SCH.	SCH. ZEUG	SCHEI-TERN	SCHIE-SSEN	SCH-LECHT	SCHLÜS-SCH.	SCHNELL FEUER	SCHRAP-NELL	SCHUSS	SCHUSS RICHT'G
81	SCH-WACH	SCHWER	SEHR	SEIT	SEITE	S.RICH.	SEK-UNDE	SENDEN	SICH	SIE
82	SIGNAL	SIND	SOFORT	SOLL	SPÄT	SPERR-FEUER	SPREN-GEN	SPR.P. HEBEN	SPR.P. SENKEN	SPREN-GUNG
83	SPRUCH	STAB	STAF-FELN	STARK	STA-TION	STEL-LUNG	STOL-LEN	STOP-PEN	STÖR.F	STÖR. SUCHER
84	STOSS TRUPP	STRAS SE	STREU-EN	STUNDE	STURM	STÜTZ PUNKT	SÜDEN SUDL.			
85										
86						TAG	TANK	TEIL-RING	TEIL-STRICH	TIEF
87	TIEFER	TOT	TREF-FER	TROM.F						
88						ÜBER	UHR	UM	UND	UNS(ER)
89	UNTER UNTEN	UNT-NEHM.	U.OFF	UNTER-STAND	UNTER-STUTZ.	UNVER-ÄNDERT				
90						V.Z.	VER-BIND.	VER-KEHR	VER-LUST(E)	VER-MISSEN
91	VER-NICHEN	V-UNG	VERPF	V-SCH-UTTEN	V-STÄR-KEN	V-ST-UNG	V-WUN-DET	VON VOM	VOR	VORBEI
92	VORM.	VOR-POSTEN	V-VER-LEGEN							
93						WALD	WANN	WAR	WARUM	WASSER
94	WEG	WEISS	WEIT	W-ER	WEL-CHER	WENIG	WIRD	WERFER	WESTL. WESTEN	WIE
95	WIEDER	W-HOLEN	WIE-VIEL	WIR	W.S.	WO	WOLLEN	WM.		
96										
97						ZEIT	ZER-STÖRT	ZER-ST-UNG	ZER. FEUER	ZIEL
98	ZIEL-HÖHE	ZIEL-NAHE	ZIEL-RICHT	ZU	ZUG	ZUG-FÜHRER	ZUG WEISE	ZU-LEGEN	ZUR ZUM	ZURÜCK
99	Z.VERL.	ZWIS-CHEN								

radical, any chain of numbers such as may accompany a military unit, or follow a word like PLANQUADRAT could be spotted almost immediately because of the presence of a chain of groups with the same radical. Therefore, the finding of a group which occurred very frequently at the beginning or end of messages, followed by a chain of groups possessing the same radical could be taken to be REGIMENT with various numerical designations. Identification followed immediately, since the final digit in each group agreed with the clear-text number. Having found the most common numbers, the other numbers from 10 up could be found easily by their association with these already solved numbers. ~~All but the round numbers had to be put together from the digits.~~

SPELLING GROUPS

The code being very short, it was very frequently necessary to spell out words. There were only one hundred spelling groups available for this, with no alternates whatever, so that, in the case of any considerable number of words spelled out there ensued the repeated use of the same spelling groups. Moreover, since as regards spelling groups there could be but ten different radicals, repetitions of chains of groups containing these ten radicals, with variable final digits, was unavoidable in spelling out any considerable amount of text.

These last facts gave an easy clue to the classification of the spelling groups. They were, in general those groups which appeared in chains composed of a few, very frequently repeated radicals. The first clue to these chains would be given by finding a sequence such as the following:

420 572 432 572 425 425 174 425

Note the repeated radicals 42 and 57; the double letter represented by 425; the intimate relations between these repeated radicals. This chain manifests all the characteristics of a sequence of spelling groups.

In order to facilitate the solution of these chains, the spelling group columns just as they appear on the triptics were cut

apart and mounted upon cardboard strips. These formed the equivale to the sliding strips so often used in deciphering processes, and indeed they were used for exactly the same purposes, viz.; anagramming, to build up words. In order to show the details of the procedure an artificial example will be taken.

Suppose the word EI-G-EN had been spelled out. By referring to the triptic sheet it will be seen that the syllables EI and EN are on the same horizontal line; in encipherment, therefore, the groups representing them would have the same radical. The letter G, being in a different line, the code group representing it would have a different radical.

In the base, the word EI-G-EN would be represented by the combination 276, 286, 279. Let us suppose that in the Secret Key the number 27 was enciphered 52; the number 28 by 08. This word would therefore be represented as follows:

526 086 529

Now let us work this process backwards, using our sliding strips. Since the first and third groups have the same radical it means that the groups which they represent are on the same horizontal line in the triptic. Therefore, if we take the two strips, numbers 6 and 9, (determined by the final digits in the first and third groups) and lay them down so that the lines on both strips coincide (i.e., with the numbers at the top on the same horizontal line), then it is clear that the clear text groups represented by the first and third groups will be on the same line.

The two strips are in position as follows:

6	9
AUS	BEN
DA	DEM
EI	EN
G	GEN
ICH	J
NACH	NEN
Q	RE
SICH	T
UNG	VER
X	ZER

108

equivalents for the first and the third code-groups are on the same one

109

The clear text ~~is on one~~ of the ten horizontal lines; the problem is then to find the line. By employing another strip

number 6 (determined by the final digit of the second group of our chain) and sliding it between the two fixed strips we select tentatively the most probable syllable, combination of syllables, or word which presents itself. In other words, we apply the well-known process of anagramming columns of an ordinary transposition cipher to this problem.

You can get this all on one line

For example, we might place the middle strip as follows:

6	6	6
AUS	AUS	BEN
DA	DA	DEM
EI	EI	EN
G	G	GEN
ICH	ICH	J
NACH	NACH	NEW
Q	Q	RE
SICH	SICH	T
UNG	UNG	VER
X	X	ZER

No probable combination presents itself, so we move the middle strip one space further, Thus:

6		9
AUS		BEN
DA	6	DEM
EI	AUS	EN
G	DA	GEN
ICH	EI	J
NACH	G	NEN
Q	ICH	RE
SICH	NACH	T
UNG	Q	VER
X	SICH	ZER
	UNG	
	X	

Still no good combination is found. True, the word NACHT appears, but in the first place, this word appears in the code-book, and secondly, we are looking for one complete word made up of parts on each strip. We continue thus until we try the following position:

129

There must

	6	
6	AUS	9
AUS	DA	BEN
DA	EI	DEM
EI	G	EN
G	ICH	GEN
ICH	NACH	J
NACH	Q	NEN
Q	SICH	RE
SICH	UNG	T
UNG	X	VER
X		ZER

Not how clearly the good combination EI-G-EN presents itself.

Having determined the correct positions, we now have the equivalents for two numbers in the Secret Key. In the base the word EI-G-EN would be encoded:

276 286 279

In the encipherment we find it to be

526 086 529

It means therefore that 27 is enciphered by 52, and 28, by 08. We may proceed then to decipher all other groups with the radicals 52 and 08.

Once a start was made in the spelling groups, further progress was very rapid. Values in the new keys were recorded and added to as they were worked out from the incoming text. (over)

W O R D S

Generally in a new key, the attempt was made to solve the spelling groups and confirm them by several messages before trying to solve word groups. The word groups could be more or less completely solved according to the amount of text in the given key. They were attacked on ordinary code principles, with, however, this addition, that the results could be checked; first, by the similarity of their final figures with the final figures of the groups in the Base representing the same words; and second, by the similarity of their radicals, when they are taken to represent words having in the Base the same radicals, i.e., words from the same horizontal line on a page of the triptic. No very serious attempt was made by us to solve the groups which represented battle reports, i.e., whole phrases, there being no satisfactory way to check the results which might be obtained.

The spelling groups not only served to give us our first break into each new key, but also enabled us to recognize and identify messages in the same key. Incoming messages in an unknown key were scanned for repeated radicals. The repeated radicals and the radicals apparently tied up with them were then compared with

the radicals of the spelling groups of the solved keys. If they were the same as those of any particular key it was assumed that the message was in that key and the values in that key were applied to the new message. Usually they led to an intelligible decoded text, and so proved their applicability. If they gave a meaningless decodement it was assumed either that the message was not in the key applied, or that, if so, it had been garbled in transmission or intentionally distorted by the encoder, a trick to be discussed later. (over)

Occasionally it happened that a message came in with spelling radicals ranging from 25 to 35. The presumption in such a case was that the text had not been enciphered. The messages were tried out in the Base and usually made sense.

SPECIAL METHOD OF SOLUTION.

One method of solving a new key, which may have already suggested itself to the student, ~~is~~ was founded on the fact that the last numbers of the enciphered groups ~~do~~ did not change. Therefore, when a word ~~is~~ was spelled out, the sequence of final numbers ~~will~~ had to be the same in any key as it ~~is~~ was in the Base Code. A list of words frequently spelled out and of phrases with the sequences of final numbers used in spelling them was prepared and proved useful. This was called the "Simple Sequence List" and was revised several times. The numbers were arranged in order, as shown in ~~the attached sample.~~ Exhibit 9

111
112

A similar list was prepared for the more common place names in the St. Mihiel Salient, shortly before our attack there. It proved useful, but owing to the quickness with which the sector was taken it soon lost its usefulness.

Suppose a sequence of five spelling groups had been found, as follows:

746 084 746 084 179

By referring to the Sequence List under the series beginning with the number 6, we look for a sequence as follows:

6 - 4 - 6 - 4 - 9

¶ As soon as a key had been solved, the sector of the sending station was looked up and noted on the recording blank. Messages from the same divisional sector usually yielded to the same key. Thus it was generally possible to determine the key of short messages which did not contain spelling groups. These short messages proved very useful in solving word groups.

We find the word GEGEBEN will fit the sequence and if this word fits in the message, and can be checked elsewhere, three cipher equivalents have been determined.

From this Simple Sequence List it was not long before a more elaborate list was formed, called the "Sequence List Showing Repeated Radicals". Exhibit 10

In the example given above, note the repetitions of the radicals 74 and 08. By referring to this new list under the heading of repeated radicals ending in the invariable digit 6, we find the sequence

6 4 6 4 9, the underlining in which indicates that the radicals of the first and third groups are the same, and the word is GEGEBEN. A still further elaboration of such a list would be to indicate in each series more than one repeated radical if such occur. For example, the preceding sequence could be marked thus:

6 4 6 4 9

indicating that the radicals of the first and third, and of the second and fourth are similar.

Thus, by a careful hunt for such sequences and a reference to both the simple sequence list and the list of sequences showing repeated radicals, many groups could be solved in one operation. This actually occurred many times in the course of the work.

11a

113

SECRET KEYS AND SUPPLEMENTS

(1) Keys.

Each division supplied its own keys. In the first few months, a ~~simple~~ single key sometimes continued to be in effect for as long as a month; one, in fact, lasted for six weeks, but this was in a quiet sector. In time of active operations, as a rule, keys were changed more frequently than was the case in the time of comparative quiet. However, the length of time during which a key remained in effect gradually shortened, until by the end of the war some divisions changed keys daily. As soon as a key had been captured it was necessary to notify divisional headquarters, where there were

supposed to be two keys always on hand, the one in use and the one next to be used. On two occasions, however, a key continued to be in effect for several days after its capture by our troops; as a result much valuable information was secured.

Code books and keys were probably issued to all organizations in a division down to companies and batteries and to liaison stations and intelligence personnel. Neighboring division headquarters exchanged keys. Independently of this, flank regiments, battalions and companies of the neighboring divisions.

Messages sent to a unit of a neighboring division were enciphered, if at all, with the key of that division.

On August 18, 1918, the 18th German Corps issued an order that thenceforth keys should be issued by it for its entire Corps area, instead of by each division in the corps. It is thought that this was only a local departure from the general rule.

(2) Supplements.

A supplement to the code-book consisted of the code equivalents for military and place names (the ~~Decknamen~~ DECKNAMEN), the battle reports and the expressions to be inserted in the code-book opposite the blank spaces. Blank groups, even after the insertion of the supplements, were sometimes used as null or blind groups, i.e., they were inserted only to confuse the enemy code offices.

When the blank groups in the code-book were insufficient in number to represent all the words it was desired to insert, the excess words were represented by code groups of four letters, for examples:

Anfang	443
Anfordern	444
Angabe	445
Ankommen Anhobre-	4450
Ankunft	4451
Armee	446

In the case of a four-figure group, the regulations were to encipher only the second and third numbers, leaving the first and fourth unchanged.

The supplements were changed from time to time, at much longer intervals than the keys. Each division furnished its own

supplements. It is thought they were exchanged over the divisions boundary in the same manner as the keys. (Sample attached).

GENERAL REMARKS.

ACTUAL OPERATION OF, AND VARIATIONS FROM THE SYSTEM.

The Three-Number Code System was, on the whole, operated by the Germans exactly as designed. It is true, also, that such measures as were recommended for camouflaging liaison as regards the use of the Three-Letter Code were applied in the use of this code too. The sending of fictitious and practice messages was as normal in this code as in the other. Lateral communication was especially practiced after the spring of 1918. There were, however, certain features and sporadic variations from the normal procedure which deserve mention. These had to deal naturally, mainly with the method of using the Secret Key.

A special key or variation from the system used by a division in the Thiacourt Group Sector, July 1918, is interesting. The messages were first encoded in the Base, and then from each three figure group was subtracted a number determined as follows: from the 1st to the 9th of the month, the number of the day of the month; from the 11th to the 19th and from the 21st to the 29th, and on the 31st the last digit of the number of the day of the month; on the 10th, 20th and 30th, the first digit of the number of the day of the month, i.e., 1, 2, and 3 respectively.

Another more common "sport" was the use of the deciphering table of the Secret Key for enciphering, the enciphering table being then used to decipher. A division taken out of a sector after having used both its keys on hand and suddenly put into line in a new sector before it had time to obtain new keys, might, it has been suggested, resort to this practice, as an expedient, to avoid the continued use of a key already long in use. The great aid such practice furnished to us was, in that the solutions in each key gave, so soon as the practice was noted, an equal number of solutions in the converse key, for if 58 was used to encipher 32 on the enciphering table, then, when the deciphering table was used as suggested above, 32 was used to encipher 58.

A rather freakish development of the above was the use of the enciphering table to encipher the first half of a message, and of the deciphering table to encipher the second half.

It should be added that transpositions of code groups and distorted messages were first noted in the use of this code, and led to the discovery of the same procedure in the Three-Letter Code. But this was observed only in the case of practice messages and communications of only trivial importance. No case of a tactical message of any importance, in which transposition occurred, came to our notice.

ESTIMATE OF THE SYSTEM

In the 247 days from March 22 to November 11, 1918, there were intercepted opposite our fronts 952 stenciled pages of text, an average slightly under four pages per day. The majority of the messages were short, from two to fifteen groups.

During the first weeks of the Code about one half of the messages were sent in the Base. This proportion fell off steadily so that during the last months the number of messages in the Base constituted less than 5% of the total.

116

The messages in the Base were decoded as they came into our Radio Intelligence Offices at the First and Second Armies. Enciphered messages could be decoded only as keys in which they were enciphered were worked out. It is no exaggeration to say, however, that over fifty percent of the enciphered messages were deciphered and decoded, either in whole or in part.

The great majority of the messages were either practice messages sent to simulate activity or messages of a very trivial nature. The tactical messages of importance were, as a rule, sent during the first days of an advance made by either side. They were generally above the average in length.

Identifications, that is, for example, divisional and regimental numbers serving to locate units as being in certain sectors, were never very common in the Three-Number Code. By the fall of

1918, they had almost entirely disappeared. Messages were either unsigned and unaddressed or else use was made of shortened designations, such as division, regiment on the right, commander-of-the front-line-troops, etc., or of code names.

The outstanding fact in a study of the Three-Number Code wireless messages is that nothing of importance was sent by wireless when there was time to send it by messenger. It is, however, equally clear, that when there was not an opportunity to communicate by messenger, the most important messages could be sent in the Three-Number Code.

The Three-Number Code had many excellent features.

The Secret Key was a small slip of paper pasted into the back cover of the code-book by a narrow strip of edging on either the top or left hand side. When in use it projected from the code-book, so that both enciphering and deciphering tables showed clearly. When not in use it folded back, so that it was entirely within the book. There was no danger of it being lost. When capture was imminent, the key could be torn out and thrown away or destroyed. It could be burned in one hundredth the time it would have taken to burn the code book itself. If captured, it could easily be replaced. It could be changed just as often as deemed desirable.

117

The capture of the code book was foreseen when the system was adopted. The method of enciphering adopted was not sufficient to protect the contents of all the messages from decipherment. But the idea of a code-book with a key which can be frequently changed, easily destroyed when in danger of capture, and quickly replaced by a new key if captured, was excellent.

The uniformity of the system along the entire front was desirable. It minimized confusion. Further, the fact that the Base of every code-book was exactly the same as the Base of every other code-book together with the fact that every unit of any size was known to have a copy, enabled any unit to communicate with any other unit in a code, which, though simple, would nevertheless

115

prevent the contents of the message from being exploited by the enem troops opposite for at least several hours.

These advantages of uniformity were counterbalanced by too long an adherence to the same edition of the code. The captured books are uniformly marked "1 Ausgabe" (1st Edition) showing that it was not the original intention never to change the Base. If the Base had been slightly changed along the entire front once every month it would have added considerably to the cryptographic value of the system. Even after the current editions of the code-book had been captured the work would have had to be done without the aid of long and very helpful sequence lists.

The large number of code groups assigned to represent military and place names were an excellent feature of the little book. Filled in differently for each division, or in ame cases apparently for each divisional sector and occasionally changed, they were, even when not used in connection with DECKNAMEN or Code-Names, never thoroughly broken into by us. Similarly, though, to a far less extent with the blank groups in the vocabulary which were filled in by supplement. They were, however, repeatedly solved.

The "Battle Reports", consisting of short sentences and phrases proved to be good. They were very difficult for us to decode. Their disadvantage is this, that too much is made to depend on a single code group. A mistake in a single figure of the group, in encoding, in transmission, or in decoding, may entirely change the meaning of a very important message. This is true, however, of all code messages.

117
118

The selection of matter for the contents was excellent. The arrangement was good, with this possible exception, that the spelling groups should not have been given consecutive numbers. It was because they had been numbered consecutively that we were able to break into the code so easily. If they had been placed in the vocabulary in alphabetical order, they would have been much harder to solve, although, being solved they would then have involved the solution of all the words in the Base having the same radicals. That, of course, would have been objectionable almost equally.

116

The fundamental fault with the system ~~is~~ was not in the code-book itself, but in the system of enciphering the code. The encipherment did not sufficiently change the appearance of the group enciphered. The one ~~letter~~ figure of each group left unchanged by the process was fatal. All three figures of each group should have been changed. This could have been done by the addition of a short list of ten equations, like the TAUVRESBDN table, but using numbers, not letters, and changing the table for each new key. That would have destroyed not only the value of our sequence lists, but also to a considerable extent, the possibility of checking solutions with the Base.

A table giving values for the numbers from 000 to 999 would have been even better if it could have been made sufficiently small not to be awkward. There would then have been no check whatever on solutions, except that the words and spelling groups found in the code-book would have been the most likely ones to appear in the messages. Such a code would have been almost the equivalent of the Three-Letter Code.

The code was a little too short. If four figure groups had been used instead of three figure groups it could have been made longer and also it would not have been necessary to have ten consecutive code groups with the same radical. The groups could have been split in two and each half enciphered on a table similar to one of the tables of a Secret Key. It is believed that if such a code had been used for the same purposes as this code, very few of its messages would have been solved.

117

119

could

Many messages were received in the Three-Number and in the Three-Letter Codes with groups in transposed order. We know nothing of the system of transposition used. When used it was almost invariably a stumbling block. It is suggested that in the case of any code with changing keys, it is desirable that there be printed on each key one or two simple systems or orders of transpositions to be used with that key.

the safety of a code depends primarily on the way in which it is used.

Nevertheless when used intelligently, the code was very effective. In one sector (H-7) a fairly large number of messages were intercepted during a period of several months in the summer and fall of 1918. These messages were studied with great care and efforts to decipher every indication of being genuine messages sent out by spies like those detected. But it was found impossible to solve them. This was because the messages were kept short, old words were spelled out and repetitions were avoided and keys were changed frequently. This goes to illustrate what has already been said that

The Three-Number Code was a War-of-Position code. In War-of-Movement there is not so much need for a code to be used in communication between units so small as companies and battalions. Use can then be made of a code-book without the same apprehension as to the certainty of its early capture and exploitation by the enemy. And yet even in the War-of-Movement, a code similar to the Three-Number Code would be valuable, for use by patrols. advance units, observers, and the like; liaison being established by means of carrier pigeons, courier dogs, and greatly improved wireless and earth telegraph instruments.

120

EXTRACT FROM THE THREE-NUMBER CODE

This extract consisted of the most important words and phrases necessary for (1) Artillery Observation Planes (2) Infantry Contact Planes. They were printed upon a card, a sample of which is attached.

All of these words and expressions were taken directly from the SCHLÜSSELHEFT or Three-Number Code, and they were designated by two letters chosen from the word or expression, as will be seen on the sample. No encipherment was used.

MISCELLANEOUS SYSTEMS.

There were several special and perhaps purely local systems which deserve mention.

One of them called the FERNSPRECHSCHLUESSEL (Telephone-key) or SCHLUESSELSCHIEBER, ("secret sliding-rule") was for telephone communication in the danger zone. It consisted of a pasteboard divided into a right and a left hand section, between which a strip bearing numbers could be slid up and down. A sample portion of this sheet, which was mounted upon a thin board, is attached herewith; it is self-explanatory. After setting the sliding strip at the key number for the hour or day, the numbers opposite the words to be communicated were called off.

A more elaborate telephone code-book was captured by our troops on the Marne Front; a copy is attached. (Exhibit 11)

A message in this code would be sent in groups of four figures. For example, to send the word ARTILLERIEFEUER (which is in column A) the sliding strip on the left would be moved till the letter A appeared in the aperture. This brings the number 3 opposite the top line of the page, and the number 21 opposite the word ARTILLERIE-FEUER. The word would then be sent as 0321. A change in key consisted in the insertion of a strip with the aperture in a different position. ~~(Exhibit)~~

Another elaborate telephone code-book was used by the 14th Infantry Division ~~is attached herewith~~. Strips containing four-place numbers were posted in opposite the columns of clear-text, Evidently new strips were printed each time a change in code was made. ~~(Exhibit~~

A rather simple system especially adapted for hand grenade communication was based upon the same lines as the Emergency Signal Chart (Sample attached).

It is not known to what extent these special systems were used.

~~GEHEIM~~ FERNSPRECHSCHLUESSEL

7	11	15	19	23			
4	14	25	30				
5	9	21	28				
2	13	20	24	27	133	199	
1	10	18	26		134	200	
3	6	12	17	31	135	201	
8	16	23	29		136	202	
					137	203	
Maschinen-Gewehr					138	204	Strasse
Material holen					139	205	Stunde
Melder					140	206	Stuetzpunkt
Meldung					141	207	Streufeuer
Minenwerfer					142	208	Sueden
Minen					143	209	
mit Verzoegerung					144	210	Tank-Geschuetz
Mitte					145	211	Tanks im Anmarsch
Morgen					146	212	Teil
morgens					147	213	(b.Mitte,e.link Teilsperfeuer.a.rechts,
Munition					148	214	Teilring
					149	215	tief
Nachbar					150	216	tiefer
Nachtricht,benachrichtigen					151	217	tot
nachmittags					152	218	
nachts					153	219	Uebernahme
Nachkommando					154	220	Uebergabe
nahe, naeher					155	221	Uhr
Nebel					156	222	Unternehmung
Norden					157	223	Unterstand
					158	224	Unterstuetzung
Offizier					159	225	Unteroffizier
Osten					160	226	

Fernsprech-Schlüssel

für

Minenwerfer

Nr. 257 Deckwort: _____ ~~Geheim!~~

	Feuer-bereit machen	B.Stellen	weiter	1/1 s.W.M.	Kurzschuss	Stand ein-geschossen	feindl. Werfer	
	S. M. W.	Entfg.	kürzer	1/2 s.W.M.	Rohr-zerscheller	tot	feindl. Werfer schiesst	
	m. M. W.	l. M. W.	Schuss	m. W. M.	l. W. M.	verw.	feindl. M.W. Feuer auf Stand	
	Erhöh.	Ladung	Schuss ab	Treiblad	ldl. Artl. Feuer auf Stand	verschütt.	— mehr	
	Ziel	Zünder-stellung	Brenn-zünder	Zünder	Sperrfeuer	Schiessen beendet	weniger	
	Blau-punkte	Hilfszahl	Ver-zögerung	Reib-zündschr.	Ver-nichtungs-feuer	langsamer feuern	Uhr	
	Rot-punkte	Teilstrich	Feuer einstellen	Lade-hemmung	zum Schuss fertig	Minute	Gas	

Bemerkung:

Die Ablesung ist erst seitwärts dann oben zu machen.

Gebrauchsanweisung:

1. Sprich am Telephon nie von Schlüsseln (Deckworten).
2. Vermeide jeden Klartext, nenne nie Namen, nie Dienstgrade, nie Ortsbezeichnungen.
3. Verrate nicht Beginn und Beendigung des Schiessens.
4. Uebe Dich im Gebrauch umstehenden Schlüssels, dann wirst Du damit so leicht arbeiten wie mit Klartext.
5. Nenne nie Entfernungen.

—

Wenn Du nur noch mit diesem Schlüssel arbeitest, tust Du dem feindlichen Nachrichtendienst Abbruch und schonst das Leben Deiner Kameraden.

 SIGNAL SYSTEM. 122

This system was one of the various minor methods of communication employed by the various German Armies (First, Second, Fifth, Sixth) in the front line previous to the adoption of the Three-Number Code. It consisted in the application of two key-word alphabets, which were changed frequently, to a chart the various subdivisions of which were devoted to the letters of the alphabet, numbers, important words and phrases. (See sample).

The alphabets, the letters of which determined the coordinates of the smaller rectangles, were usually made up from either a single word, a name, or a phrase, in accordance with the well known custom. Since the original chart consisted of a square 18 x 18, these alphabets had only to be carried out to 18 places.

The message was sent in groups of three letters, of which the last two letters gave the coordinates, and the first letter was chosen at random, and which, of course, did not count. There were several modifications of this scheme of adding on the third letter to make a trigraph. One was to duplicate the second letter of each pair of coordinates, and thus each trigraph appeared as a set of letters in which the first and third were always identical. Sometimes the message was not sent in groups of three, but simply run together in a single chain of letters. Sometimes, to add greater confusion after the Three-Letter Trench Code was adopted, one of the three letters K, R, U, was used for the initial letter in each group, thus making a message look exactly like a three-letter trench code message.

These messages, however, were very easy to decipher, since most of the words used had to be built up letter by letter from the chart. A frequency table soon showed the equivalents of the high frequency letters E, N, etc., and the fact that Key-word Alphabets were used enabled the decipherer to complete the partially solved cipher alphabets in much less time than would have been the case had random-mixed alphabets been used.

After April, 1918, since the Three-Number Code replaced it, the use of this chart stopped.

Some good examples of the type of Key-word Alphabets that were used are:

HINDEBURGACFKLMOPQ	(Hindenburg)
LUDENORFABCGHIKMPQ	(Ludendorff)
SCHWERATILFUBDGKMN	(Schwer Artillerie Feuer)
MASCHINEGWRKOPBDFL	(Maschine Gewehr Kompagnie)

AVIATION CODES

Mention has been made ~~to~~ a special Three-Letter Code which the Germans employed solely for aviation. These were in reality three separate codes, each with special initial letters, GLF, GLFVX and GLFVZ.

One section of the Code Department was put to work on these codes, but after September 1918, so little information of any value was secured from their study by us that work was discontinued. These codes were used mainly by giant aeroplanes in bombing expeditions. However, the same principles by means of which the KRUSA were attacked could be applied to these codes inasmuch as they were constructed in exactly the same way, and in fact, with the exception of some phrases and words specially inserted for aviation activities, the contents of these codes was the same as the KRUSA Codes.

METEOROLOGICAL CODES

The importance of a knowledge of meteorological conditions in connection with both the Gas and the Artillery Service was soon recognized by the Germans.

At first they simply had observation posts where meteorological data were taken and these were transmitted by the Three-Letter or Three-Number Codes. A typical report ran as follows:

WETTER MELDUNG PUNKT 20 PUNKT 13 PUNKT ~~117~~ 17 PUNKT BODEN WIND HUNDERT KOMMA NULL VIER KOMMA ZWEI HUNDERT TRENNUNGSSTRICH NULL SECHS KOMMA DREI HUNDERT KOMMA NULL ZEHN PUNKT EINS FUENF NULL NULL BAROMETER NULL DREI KOMMA SECHS TEMPERATURE MINUS VIER PUNKT FEUCHTIGKEIT NEUN ZWEI PROZENT PUNKT LUFT GEWICHT EINS SIEBEN EINS DREI NULL PUNKT.

Later these reports were much shorter, and a typical example such as occurred in Fritz Code 23, was as follows:

REGIMENT PUNKT SIEBEN UHR ABEND P NULL VIER ZWEI EINS SECHS TAUSEND KOMMA ACHT UHR P NULL VIER ZWEI EINS SIEBEN TAUSEND NEUN UHR P NULL VIER ZWEI EINS ACHT TAUSEND FRONT WETTER -- BATAILLON.

Later, special codes were adopted, and no more reports of this nature were sent in the Three-Letter of the Three-Number Codes.

By July 1918, they had established about twenty-five meteorological stations along the Western Front, the locations of which are shown on the sheet attached. These stations were devoted exclusively to weather reports, and the enemy had great confidence in the value of such reports.

Several systems for transmitting the information were used. A memorandum of May 6, 1918, explains the method then in use, and no comments are necessary. Attached to this memorandum is a sample of the form in which the decoded messages were sent by us to the central office of G-2.

About July 1918, the enemy introduced a new procedure in transmitting these reports. Each group of four numbers was split into two parts, and each part encoded by three-letter KRUSA Code

groups. Each code book contained a whole section devoted exclusively to weather reports, and the code groups in this section were to be used for no other purposes. Since the enemy did not change the form of the reports, solutions were fairly easy, on Analogy Method principles.

About September 1918, the type of messages became very uniform on the whole front, on the introduction of what the enemy called the System of BALTASEKUNDEN. A copy of a German document shown herewith explains it.

In addition to these reports a special report was used for weather forecasts, and a memorandum explaining the system is attached.

Probably the most important information we secured from these stations was that entirely unrelated to the nature of their activity. It was noted that the movements of enemy meteorological stations furnished highly important information as to his intentions. A general withdrawal, for example, was often preceded by a movement of his meteorological stations further back. Indeed, in the later days, when information was very hard to get, a most fruitful source was in that furnished by the apparently innocent movements of the enemy's meteorological stations.

The codes were studied by Second Lt. John A. Graham, Infantry, with good results.

asm

GENERAL HEADQUARTERS , AMERICAN EXPEDITIONARY FORCES,
GENERAL STAFF, SECOND SECTION (G.2, A-6)

(DISTRIBUTION "I") May 6, 1918.

The following (furnished by the French) explains the contents of messages transmitted by enemy meteorological stations.

KEY	HHUU	BBTT	WWSS	WWSS(1)	WWSS(2) .....
EXAMPLE	0513	6511	0403	0605	0708

1 / - H H indicates the altitude of the meteorological observatory in decameters, example 05 = 50 meters.

2 / - U U indicates the hour from 0 to 23; for example, 13 = 1 p.m.

3 / - B B indicates barometric pressure in millimeters at the given altitude. (The figure designating hundreds is omitted) Example, 65 = 765 millimeters.

* * * *

4 / - T T indicates air temperature in degrees centigrade: example, 06 = 6° centigrade, 51 = -1° centigrade (1° below zero).

5 / - W W indicates direction of the wind at ground level in accordance with following table:

N by E	1	S by W	17
NNE	2	SSW	18
NE by N	3	SW by S	19
NE	4	SW	20
NE by E	5	SW by W	21
ENE	6	WSW	22
E by N	7	W by S	23
E	8	W	24
E by S	9	W by N	25
ESE	10	WNW	26
SE by E	11	NW by W	27
SE	12	NW	28
SE by S	13	NW by N	29
SSE	14	NNW	30
S by E	15	N by W	31
S	16	N	32

3 / - S S indicates velocity of wind in meters per second: example, 03 = 3 meters per second.

7 / - WWSS(1) indicates direction and velocity of wind at an altitude of 100 meters: example, 0605 = East Northeast, 5 meters per second.

8 / - WWSS(2) -do- altitude 200 meters etc., etc.

9 / - The last groups give additional data, for example the indication of the average temperature for the previous 24 hours for the determination of air density at the average altitudes of the trajectory of projectiles (over 500 meters): example,

average temperature 3° centigrade
barometric pressure 763 millimeters

following the daily table of correcti
density would therefore be 1.28

_____:

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES,
GENERAL STAFF, SECOND SECTION (G.2, A.6)

Intercepted by_____ _____1918.

GERMAN METEOROLOGICAL REPORT

Sent from:_____ at _____1918.

Height of observation station in meters:_____
Time of observation:_____
Barometer, in millimeters:_____
Temperature, in degrees Centigrade:_____
Humidity:_____
Density of air:_____

Direction and velocity of wind at various elevations:
(Elevation in meters, velocity in meters per second.)

Elevation:	000	100	200	300	400	500	600	700
Direction:								
Velocity:								
Elevation:	800	900	1000	1100	1200	1300	1400	1500
Direction:								
Velocity:								

Remarks:_____

Decoded by:_____

GENERAL HEADQUARTERS
AMERICAN EXPEDITIONARY FORCES
(G-2, A-6)

July 23, 1918.

MEMO FOR MAJOR MOORMAN:

According to the latest information, the following are the locations of the German METEOROLOGICAL stations:

Call	Location	Reference to larger city.
Z1	E. of TOURCOING,	N.E. of LILLE.
Z3	At HAUBOURDON,	S.W. of LILLE.
Z5	N. of ARLET,	S. of DOUAI.
Z6	At VALINCOURT,	S. of CAMBRAI.
Z7	At NESLE,	N.E. of ROYE.
Z8	W. of ST. SIMON,	S.W. of ST. QUENTIN.
Z9	W. of LAON,	
Z10	At BRAINE,	E. of SOISSONS.
Z11	At TAGNO,	E. of NEUFCHATEL
Z12	N.E. of VOUZIER,	
Z14	At STENAY,	S.W. of MONTMEDY.
Z16	S. of CONFLANS,	In the WOEVRE.
Z17	At POUILLY,	S. of METZ.
Z18	At DIEUZE,	In LORRAINE.
Z19	N.E. of SCHLESTADT,	In ALSACE.
Z20	S.E. of SARREBOURG.	
Z21	In COLMAR.	
WRG	At PERONNE.	
BP	At MARCHELLEPOT,	30 km W. of ST. QUENTIN.
MTR	At SERAINCOURT,	40 km N.N.W. of RHEIMS.
ABS	At MONT NOTRE DAME,	E.S.E. of SOISSONS.
MWD	At AUSSONCE,	23 km N.E. of RHEIMS.

E. H. FALK
1st Lt. F.A.U.S.R.

Officers decoding weather reports will please note location. If sent by stations not listed above, report call letters to Gonio Officer.

FRANK MOORMAN,
Major, G.S., American E.F.

Enemy Meteorological Reports. (Forecasts)

Enemy station Zl sending messages containing 5 figure groups, appears to be using the following procedure:

The precise import of the first 15 or so groups has not yet been determined.

The groups containing the weather forecast, when they occur, always do so after the break sign (B') in the latter part of the message. They are built up on the following formula:

FORMULA = K K O O O D C W W S S_h W_h V L T M I G Q Q

When K K = Index Group.
" O O O = Place or territory for which the weather-forecast is valid.
" D = Durability of weather condition.
" C = Character of wind on the ground.
" W W = Direction of wind on the ground.
" S = Velocity of wind on the ground.
" S_h = Velocity of wind up above.
" W_h = Direction of wind up above.
" V = Condition of clouds.
" L = Tendency toward a storm.
" T = Temperature.
" M = Precipitations.
" I = Visibility.
" G = Motion of the sea.
" Q Q = (Check figure, arrived at by adding all the other digits).

K K. 70 - Forecast for about 12 hours, the occurrence of which is very likely.
71 - Forecast for about 12 hours, the occurrence of which is to be expected to some extent.
72 - Forecast for about 12 hours, only with conditional reliability.
73 - Forecast for about 24 hours, the occurrence of which is probable to some extent.
74 - Forecast for about 24 hours, the occurrence of which is to be expected to some extent.
75 - Forecast for about 24 hours, only with conditional reliability.
76 - Forecast for about 36 hours, the occurrence of which is very likely.
77 - Forecast for about 36 hours, the occurrence of which is to be expected to some extent.
78 - Forecast for about 36 hours, only with conditional reliability.
79 - Weather-forecast.
80 - Weather-forecast impossible.

000 (Not known).

D. 0 - Continuation of prevailing weather probable for several days (2 - 3 days)
1 - For today, continuation of prevailing weather. Tomorrow, change to bad weather.
2 - Increasingly bad weather.
3 - Tommorrow, dangerously bad weather.
4 - Today, dangerously bad weather (stormy condition).
5 - After passing calmness, renewal of bad weather.
6 - Weather disturbance, probably of short duration (less than 1 day)
7 - Today, continuation; tomorrow, increasing calmness.
8 - Increasing calmness.
9 - Unable to state development of weather condition.

GENERAL HEADQUARTERS, AMERICAN EXPEDITIONARY FORCES
GENERAL STAFF, SECOND SECTION (G.2 A.6) (alp)

Oct. 29, 1918.

(Translation of a German Document)

18th Army G.H.Q., March 17, 1918.

18 Art. Kofluft W.Br. No. 1777.18.

Introduction of the System of

BALTASEKUNDEN

Meteorological reports hitherto sent by an Army meteorological station will in future be transmitted as Baltasekunden messages. ("Meldung ueber die ballistischen Tageseinflusse, gestaffelt nach Flugzeit Sekunden; i.e., "Report on Ballistic Influences of the Weather, Based on Duration in Seconds of the Flight of a Projectile").

Reports on Baltasekunden will be issued 7 times each day. Below are orders regarding the introduction of the new system, hours and the methods of their transmission by wireless.

Measurements and calculations required for registration of Baltasekunden will be made by the Army meteorological station. No mathematical computations whatever are to be undertaken by Balta sections. A reorganisation of this section is under consideration, and until its completion, Artillery Commanders will instruct detachments under their control and give them opportunities for practice about twice a week. Reports on the results of such instructions will be returned once each week in writing to the Army meteorological station.

Baltasekunden messages consist of a characteristic word followed by 11 groups of 5 ciphers. The words indicate hours, as;

temer.....	1st morning-message.....	(6 A.M.)
texor.....	2nd morning-message.....	(9 A.M.)
temit.....	1st afternoon-message....	(12 M.)
texit.....	2nd afternoon-message....	(15 P.M.)
temab.....	1st evening-message.....	(18 P.M.)
texab.....	2nd evening-message.....	(21 P.M.)
tenacht.....	night-message.....	(1 A.M.)

These groups are used respectively for flights of 10, 15, 20, 25, 30, 40, 50, 60, 70, and 80 seconds. The first two figures of each group indicate the ballistic weight of the air, the first two decimals thereof standing to the right of the comma. The next two figures indicate the direction of the wind according to the wind-card; thus, 08-East, 16-South, 24-West, 32-North, etc. The last figure shows the velocity of the wind in double metres per second (Doppelmeter, Doms). Particular attention is invited thereto, wind-velocity having previously been expressed in single meters per second, and most tables of atmospheric influences so giving it. If the velocity of the wind exceeds 9 Doms, the figures 50 are added to those representing the direction of the wind and only the second figure of the group which stands for its velocity will be put down. The group 0731 would thus be; weight of the air-1,20; direction of the wind, WSW (73-50 = 23); velocity of the wind, 11 Doms.

The eleventh and final group serves as a verification of the ten preceding ones, being their united total, with the figures for "exceeding" left out.

Example for a Baltasekunden message:

temit - 1st afternoon-message.

20302	-	for	10	seconds	flight,	weight	1,20	dir.	NNW.	velocity 2 Doms.
20322	-	"	15	"		"	1,20	"	N	" 2 "
20022	-	"	20	"		"	1,20	"	NNE	" 2 "
20043	-	"	25	"		"	1,20	"	NE	" 3 "
20034	-	"	30	"		"	1,20	"	NEN	" 4 "
20064	-	"	40	"		"	1,20	"	ENE	" 4 "
20067	-	"	50	"		"	1,20	"	ENE	" 7 "
21069	-	"	60	"		"	1,21	"	ENE	" 9 "
22570	-	"	70	"		"	1,22	"	EN	" 10 "
22581	-	"	80	"		"	1,22	"	E	" 11 "
07074	-	verification-group								

An addition of the cipher-groups gives 207074, which, omitting the first figure, gives 07074.

Battery-chiefs are asked to keep a file, arranged as follows, for the registration of Baltasekunden messages:

temit

Message for consideration.

Bal. air-weight in decimals	Wind Dir.	Velocity in Doms.	Duration in seconds	Bal. air-weight.	Wind Dir.	Actual velocity in Doms.
20	30	2	10	1.20	30 NNW	2
20	32	2	15	1.20	32 N	2
20	02	2	20	1.20	02 NNW	2
20	04	3	25	1.20	04 NW	3
20	03	4	30	1.20	03 NWN	4
20	06	4	40	1.20	06 NW	4
20	06	7	50	1.20	06 WNW	7
21	06	9	60	1.21	06 WNW	9
21	07	0	70	1.22	07 WN	10
22	08	1	80	1.22	08 W	11

This example is the same as that above.

The battery-Commander will determine the flight-duration of a given shot from his ranging-table. He will look in column 4 of the model above for a flight-duration approaching nearest to that in the ranging-table, and will find the figures for weight, direction and velocity of the wind, in a horizontal line therefrom. For example; for a flight of 12 seconds as given in the ranging-table, the figures of the model in a horizontal line from 10 seconds are taken. These figures serve for adjustments of distance for a given weight of air and direction of wind, as in the case of the tables of weather influences (Tageseinflusstafeln).

It is suggested that flight-durations be recorded daily, to supply any possible lacks in the tables.

General Staffs and Batteries will receive instructions later for use of Baltasekunden.

To be distributed down to Batteries.

Chief Quartermaster.

B R A U N
Colonel.

C.

0 - Uniform.
1 - Somewhat squally.
2 - Squally.
3 - Very squally.
4 - By about 2 full degrees.
5 - " " " " "
6 - " " 3 " "
7 - " " " " "
8 - Changing wind velocity.
9 - Air disturbances.

W W.

00 - Shifting
01 - N. E.
02 - E.
03 - S. E.
04 - S.
05 - S. W.
06 - W.
07 - N. W.
08 - N.

11 - Prevailing NNE - ENE
12 - " ENE - ESE
13 - " ESE - SSE
14 - " SSW - WSW
15 - " SSW - WSW
16 - " WSW - WNW
17 - " WNW - NNW
18 - " NNW - NNE

21 - In NE Directions.
22 - " NE - SE "
23 - " E - S "
24 - " SE - SW "
25 - From S - W "
26 - " SW - NW "
27 - " W - N "
28 - " NW - NE "

31 - N to E
32 - NE " SE
33 - E " S
34 - SE " SW
35 - S " W
36 - SW " NW
37 - S " N
38 - NW " NE

41 - NW by N to SE
42 - N " E " S
43 - NE " E " SW
44 - E " S " W
45 - SE " S " NW
46 - S " W " N
47 - SW " W " NE
48 - W " N " E

51 - From NE directions, later shifting to the right.
52 - " E " " " " " "
53 - " SE " " " " " "
54 - " S " " " " " "
55 - " SW " " " " " "
56 - " W " " " " " "
57 - " NW " " " " " "
58 - " N " " " " " "

61 - From NE directions, later shifting to the [illegible]
62 - " E " " " " " "
63 - " SE " " " " " "
64 - " S " " " " " "
65 - " SW " " " " " "
66 - " W " " " " " "
67 - " NW " " " " " "
68 - " N " " " " " "

Separate Statements.

80 - From varying directions.
81 - In the W of the territory from NW, in the E from SW directions.
82 - In the W of the territory from SW, in the E from SE directions.
83 - In the W of the territory from NE, in the E from SE directions.
84 - From the W shifting to S directions.
85 - " " W " to SW "
86 - " " W " " W "
87 - " " W " " NW "
88 - " " N of the territory shifting to SW.
89 - " " N " " " " " SSW.
90 - In the S of the territory from SW, in the N from SE directions.
91 - In the S of the territory from W, in the N from S directions.
92 - In the S of the territory from NW, in the N from NE directions.
93
94
95
99 - Nothing to state.

S. 0 - Quiet.
1 - Light.
2 - Light.
3 - Average - weak.
4 - " - moderate.
5 - " - fresh.
6 - " - strong.
7 - " - stiff.
8 - " - stormy.
9 - " - full storm.

S_h

0 - Upward, only slowly increasing, or decreasing.
1 - Up to 1000 meters slowly increasing, at greater elevations increasing more rapidly.
2 - Up to 500 meters moderate; above that level, slowly increasing or not at all.
3 - Up to greater elevations, moderately increasing.
4 - Moderate maximum in about 500 meters, above that level decreasing.
5 - Up to about 1000 meters moderately increasing; above that level remaining the same or decreasing.
6 - Up to about 500 meters strong, above that level slowly increasing.
7 - Up to higher elevations, strongly increasing.
8 - Up to about 500 meters strongly increasing, above that level decreasing.
9 - Unable to state.

W_h

0 - Upward, little change, or shifting to the [illegible]
1 - Above 500 meters, shifting toward N to NE
2 - " " " " " E
3 - " " " " " SE

4 - Above 500 meters, shifting toward S
5 - " " " " " SW
6 - " " " " " W
7 - " " " " " NW
8 - Above, shifting to the left.
9 - Unable to state.

V.

0 - Temporarily clearing up.
1 - Prevailingly clear.
2 - Cloudy.
3 - Overcast.
4 - Dense, heavy cloud covering.
5 - Decreasing cloudiness.
6 - Increasing cloudiness.
7 - Cloudy during day, clearing up during night.
8 - Changing cloudiness.
9 - Unable to state.

L.

0 - Storm not to be expected.
1 - Storm slightly probable.
2 - Storm not improbable.
3 - Storm probable.
4 - Here and there storm to be expected.
5 - Storm to be expected in many places.
6 - There will still be a storm today.
7 - Storm tomorrow.
8 - Strong storm activity to be expected.
9 - Unable to state.

T.

0 - Cold.
1 - cool.
3 - Warm.
3 - Warm during day, cool during night.
4 - Increasing.
5 - Decreasing.
6 - Normal
7 - Slight change.
8 - Near freezing-point.
9 - changing.

M.

0 - Dry
1 - For a short while, dry; later, precipitation.
2 - Diminishing precipitation.
3 - Sporadic rain storms.
4 - Extensive " "
5 - Rainfall.
6 - Snowfall.
7 - Only light precipitation.
8 - Precipitation in showers.
9 - Unable to state.

I.

0 - Increasing visibility.
1 - Normal visibility.
2 - Somewhat turbid.
3 - Turbid.
4 - Decreasing visibility.
5 - Ground mist.
6 - Invisibility, at some places misty.
7 - Misty.
8 - Unable to state.
9 - Changing visibility.

G.

0 - Quiet.
1 - Moderate.
2 - Turbulent.
3 - High.
4 - Choppy sea.
5 - Sea coming from N to E.
6 - Heavy sea coming from E to S.
7 - " " " " S " W.
8 - " " " " W " N.
9 - Unable to state.