SRH- 311

PRINCIPLES OF SOLUTION

OF MILITARY FIELD CODES USED BY

THE GERMAN ARMY IN 1917

[redacted]

RESTRICTED

[redacted]

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

PRINCIPLES OF SOLUTION OF MILITARY FIELD CODES USED BY THE GERMAN ARMY IN 1917

TECHNICAL PAPER

OF THE

SIGNAL INTELLIGENCE SECTION

WAR PLANS AND TRAINING DIVISION

UNITED STATES

GOVERNMENT PRINTING OFFICE

WASHINGTON: 1935

REVIEWER'S NOTE: This page (ii) blank and unnumbered in original copy

FOREWORD

This brochure was written by an officer of the Code Solving Section, General Headquarters, British Expeditionary Forces, in January 1918. No changes, additions, or deletions have been made therein.

WILLIAM F. FRIEDMAN, *Cryptanalyst,*
Chief of Signal Intelligence Section,
Office of the Chief Signal Officer.

JUNE 25, 1934.

REVIEWER's NOTE: This Page (iv) blank and unnumbered in original copy

CONTENTS

REVIEWER'S NOTE: This page (vi) blank and unnumbered in original copy

PRINCIPLES OF SOLUTION OF MILITARY FIELD CODES USED BY THE GERMAN ARMY IN 1917

INTRODUCTION

As the following brochure is primarily intended solely for the purpose of showing the methods adopted in solving the codes used by German field wireless stations, it is not proposed to enter into a long explanation of the nature and solution of codes in general. It is obviously impossible within the limits of a short treatise to treat exhaustively all the aspects of code solution; nevertheless, a few preliminary remarks on the subject may well fall within the particular scope.

DEFINITION OF A CODE

A code is, in essence, a conventional dictionary used for the purpose of translating, by means of combinations of letters or figures, a secret communication into such a form that it cannot be deciphered by anyone not in the possession of the code book.

In codes used by German field stations, certain groups of letters are allotted to the words and phrases most frequently used in conveying information of a military character as well as to numbers and to the most frequently used spelling groups.

A number of groups are also allotted to the various punctuation marks and grammatical signals such as

HAUPTWORT, MEHRZAHL, GEGENWART, MITTELWORT DER VERGANGENHEIT,

and several groups are definitely set aside as dummy groups to be inserted in frequently recurring phrases and in short messages of a more or less stereotyped character.

The advantages of such a system of secret correspondence are obvious. Encoding and decoding are easy and rapid; the encoded message is generally much shorter than the original text; the comparison of one message in code and in clear does not enable another message in the same code to be read; and the measure of security is high if not absolute, unless the code book falls into the enemy's hands, or has been in use for such a long time that a sufficiently large amount of material has been intercepted to enable the enemy to solve it.

QUALIFICATIONS FOR THE WORK

In order to undertake successfully the reduction of a code, certain preliminary qualifications are essential. Much time and much labor must be devoted to the work if any useful measure of success is to be obtained.

The would-be solver must possess a thorough knowledge of the language employed, not only from the point of view of vocabulary but also from that of a knowledge of all the peculiarities of its grammar, syntax, and idiom and of the peculiar phraseology—diplomatic, commercial, or military—in which the messages are likely to be couched.

He should possess a lively intelligence, the faculty of imagination tempered by a nighly developed critical faculty, the power of analysis, a high degree of a certain natural flair or instinct for the work, untiring patience and perseverance; in a word, the qualities of genius, defined as an infinite capacity for taking pains.

He will need a dogged obstinacy which, however, must not render him incapable of discarding a supposed clue once it has been discovered not to lead anywhere; a highly trained visual memory which will help him to remember the look of a code group, to recognize it on its reappearance, and to remember where he has seen it before, what its sequences were, and what theory, if any, he has formed about it each time it occurred.

He must possess the faculty of keeping anything from a dozen to 20 theories in his mind in order to build up a chain of coincidences and reasoning until each link fits into its place and forms a coherent whole.

IMPORTANCE OF METHOD

In addition to the above qualifications, however, a right method, and a clearly defined system of attack on a new code are necessary. It is the purpose of this brochure to try and lay down the main principles of a logical method, such as enabled the first code to be solved without the aid of previous analogies, and the more or less adventitious assistance of a knowledge of all the peculiarities of phraseology and procedure adopted by certain stations or groups of stations.

At the same time, however, as much reference as possible will be made to all analogies which may lead to a successful attack on a new code when its general outlines, scope, and procedure are known.

FIRST STEPS

At this stage a tabulated summary of the most essential steps to be taken will perhaps be most useful. Later on a more detailed elaboration of these steps will be brought in under the various sections as they occur.

1. The first step to be taken is to collect all the material that has been accumulated and have it typed out in such a way that the maximum amount of material can be brought under the eye at any one moment.

The material should be sorted as far as possible into sections showing the sender and receiver, and keeping as close together as possible all messages from the same station or group of stations.

Any indication in clear at the beginning or end of messages should be shown, such as sender, receiver, time group of transmission, CHI or ZIF numbers showing the numbers of groups, etc.

All pages should be numbered consecutively, and each separate message on a sheet should be given a serial letter. This will enable reference to be made to any particular code group or message by giving the number of the page and the letter of the message, i.e., 21B, 36K, etc. etc.

2. A book should now be prepared in which the letter or figure groups can be arranged in order, after which every group that occurs in the code should be indexed in the book by giving its reference as above.

As soon as the signification of any group is discovered, its indexing should cease, and the meaning should be inserted opposite to it on the line.

This book will then serve as a decoding or "Entzifferung" book as well as an index. It will be well at the same time to mark the initial and final groups of each message in some distinctive coloring in the index, so as to facilitate the study of these particular groups, and to aid hypotheses as to their function, when they should be frequent.

3. The index will soon begin to show the frequency of the recurrences of the various groups employed.

Attention should be concentrated on the initial and final groups which might indicate the address or signature respectively, or the word "an", "addressed to", or "intended for."

If the sequence of the first two groups should show any tendency to be at all constant it will be extremely probable that the first="an", and the second="unit" or person addressed.

Any outside knowledge as to the nature of the possible unit, or the rank, designation, or name of the possible person may well aid hypotheses at this stage.

Very soon it should be possible to identify the various groups for "Division", "Brigade", "Regiment", "Kampf-Truppen-Kommandeur", "Funken-Telegraphie-Station", etc. etc.

When the study of numbers, treated in detail elsewhere, has resulted in identifying the groups which must be numbers, although as yet their actual value is not known, we have now reached a very fruitful stage for hypothesis as to the numbers of the possible units mentioned.

INITIAL AND FINAL GROUPS

4. An analysis of the most frequent final groups in each message should now lead to the discovery of signature, of Punkt=Full stop, or of Fragezeichen=Note of interrogation. The last-mentioned is very frequent in short messages such as "Wo bleibt Abend Meldung?" or "Wie ist die Lage dort?", etc. etc.

A comparison of initial and final groups will now often show that the same group occurs at the beginning of some messages and at the end of others. This will point fairly conclusively to the fact that these groups represent the units or person sending or receiving the message.

Any outside indication as to the possible sender and receiver in each case will now be useful in forming an hypothesis as to the signification of these address and signature groups.

At this stage, as in fact at nearly every other, analogy with previous messages sent by the same station, in codes already known or solved, should be studied as far as possible.

A knowledge of the possible subject matter of messages sent at stated times, or under circumstances about which any outside or collateral information can be obtained, should always be sought for, and will invariably and inevitably assist in experiment and hypothesis.

INTERIOR GROUPS

5. We now approach the most difficult part of the solution, namely, that of the inside portion or text of the message. This it is proposed to undertake by a separate treatment of the several kinds of groups which normally occur in the text of messages.

These may be usefully treated under the general headings of phrases, words, spelling groups (used for spelling out words or names for which there is no equivalent group in the code), punctuation marks, and grammatical signs.

Of these, for reasons to be explained later, the numbers are, in the early stages of the code, the most important, and their study shall therefore be treated first.

It must be remembered, however, that it is almost impossible to separate one portion of the work of solution from others, and as stated earlier on, the efficient code solver must possess the faculty of keeping many possibilities and collateral theories in his mind, even while endeavoring to concentrate on some one particular aspect of the work.

The whole problem resolves itself into a coordination of hypotheses, separately obtained by analysis, theory, and imagination, but linked together by every possible means until the whole chain of reasoning is found to be complete.

NUMBERS

IMPORTANCE OF NUMBERS

In the days when cipher was employed to the exclusion of code, there was no necessity to concentrate on numbers apart from the context. The key once discovered, the whole message and all succeeding ones were immediately decipherable in their entirety.

Now, however, that code has taken the place of cipher, the verification of numbers assumes a much more important aspect.

As it is obviously impossible to solve the two-thousand-odd groups which exist in a code until they have been used in messages, or even then until some of them have occurred sufficiently often to enable one to analyze their sequences and positions, the code has to be built up little by little, in proportion as material comes to hand.

It becomes necessary, therefore, to concentrate on what will be most immediately useful, and one of the most important pieces of information that we can obtain from enemy wireless messages is the identification of units in the German lines on any particular portion of the front, for the purpose of ascertaining what is the strength of the enemy forces opposite to our own.

For this reason we will begin with the solution of numbers, and consider this problem from the double standpoint of solution by analogy and solution on first principles, combining the two methods whenever the necessary progress has been made.

An essential preliminary is a knowledge as complete and detailed as possible of the constitution of the Germany Army and of the German order of battle.

SOLUTION BY ANALOGY

In these codes numbers are used in the following ways:

(*a*) In mentioning units, divisions, brigades, regiments, etc.

(*b*) In mentioning dates and times of day.

(*c*) In giving map references after Karten, Punkt, and Planquadrat.

(*d*) In giving numbers of shots, casualties, Funken-Telegraphie Station accessories.

(*e*) Number of messages sent and received, e.g., "3 Funksprueche geschickt, 4 empfangen."

(*f*) In giving tabulated reports of the day's activity under various headings.

(*g*) Chi or Zif numbers and time of groups of messages answered or referred to, e.g., "Chi 17 an KS nicht verstanden", "Funkspruch 1306 erledigt", "Wer hat Funkspruch 1037 gegeben?" etc., etc.

A sample message, including most of the above uses, might run as follows:

"An Division 105. Abend Meldung 18–2–17. (1) Von 10 Uhr 25 Morgens bis 3 Uhr 30 Nachmittags 40 Schuesse schweren Kalibers auf Kartenpunkt M2 Planquadrat 5209. (2) Feindliche Flieger Taetigkeit gering, 5 Flieger ueber Abschnitt 7A. (3) Wetter gut, sicht klar. (4 bis 7) nichts. (8) 2 Unter-Offiziere und 7 Mann schwer verwundet, 10 Mann leicht verwundet. (9 bis 10) nichts. Gezeichnet Bataillon II/316."

The form of these report messages varies with each sector and group of stations, but the same station has the tendency to send the same form of stereotyped message at certain stated times each day, and a careful analysis of previous messages from the same station in an old code will often be of material assistance in solving a new code.

One of the most essential things therefore in starting to solve a new code is to study as carefully as possible all previous messages, with reference to matter, form, and station procedure with all its varying peculiarities, and to analyze and experiment on the new messages to find out any analogies which may exist.

It has often been possible to make a start on a very limited amount of material when the same stereotyped form of message is still being transmitted by the same station.

It frequently happens, however, that with a change of code or a change of unit, these messages are no longer sent in the same stereotyped form. Some messages rarely mention units, others rarely give a date, and some use letters instead of numbers in sending tabulated reports.

In one code certain stations regularly sent messages of this type:

"2 GESCHICKT, 6 EMPFANGEN",

but with a change of code such messages ceased altogether. In the same code one station regularly sent a message in the following form:

"REGIMENT B' ABEND MELDUNG B' (1) ETC."

"REGIMENT B' MORGEN MELDUNG B' (1) ETC."

with a tabulated report on stereotyped lines.

When the code changed, the form of these reports changed absolutely and no analogy could be observed. These changes were most possibly due to the transference of the particular Difua to another sector of the front.

When the form of procedure thus changes and analogy breaks down we are thrown back on solution by first principles, just as when the first code was solved without the help of previous knowledge of station procedure and phraseology.

SOLUTION BY FIRST PRINCIPLES

In solving a code without the aid of analogy there is a tremendous amount of preliminary spade work to be done

(*a*) By indexing,

(*b*) By analysis of frequent groups and their sequences,

(*c*) By a study of what may be called in a general way stationary groups, i.e., Punkt, Uhr, An, Von, Bis, Meldung, etc., and mobile groups, i.e. numbers, spelling groups, and words.

(*d*) By a search for groups which have a tendency to recur in pairs.

These are explained more fully elsewhere.

In earlier codes the problem was rendered much easier by the fact that there was only one group for Punkt, Komma, Uhr, etc., and by the fact that each number up to nine was represented by only one group.

This meant that to encode compound numbers such as 15, 23, or 105, the single numbers were used, and to encode 17th or 21st the single cardinals were written followed by "th" or "st", etc.

In the present codes, unfortunately, the tendency has been to increase the number of groups for each cardinal up to 10, to give groups for compound numbers from 11 to 20, and 20 to 100, and to allot groups to all cardinals up to the 12th, and to frequentatives from "einmal" to "zehnmal".

But in spite of these increased difficulties it is possible to lay down a certain number of first principles such as may help in elucidating numbers.

As numbers tend to be some of the most frequent groups apart from Satzzeichen, the preliminary spade work should have resulted in spotting certain frequent groups.

By marking these groups in distinctive colors it will be noticed that some of them have a tendency to attract each other, and to hunt in couples, threes, and occasionally fours.

Now groups which invariably appear in couples, *in the same order*, will most probably be nouns or verbs followed by "Mehrzahl" or "Mittelwort der Vergangenheit", etc., station calls, or stereotyped phrases such as "Morgen Meldung", "Abend Meldung", "KTK A" or "KTK 3", etc.

Groups which invariably run in threes or fours, or more, *in the same order*, will most probably be spelling groups, and might give P O ST, L AM P E, S A TZ B U CH, etc.

But when groups tend to appear generally in bunches of two, three, or four, *and not always in the same order*, most if not all of them will turn out to be numbers.

Thus if A, B, C, D, E, F should represent half a dozen of these frequent groups they might occur in the following orders: A B or B A; A C E, E A C, or F C A; B A D C or E A B D, etc. It will then be safe to presume that these groups represent numbers.

By tabulating the sequences before and after any one of these groups they will soon be seen to attract other, until anything from 12 to 20 of them can safely be presumed to be either numbers or some word or letters which frequently accompany numbers, such as Unit, Uhr, Komma, Planquadrat, von, bis, zwischen, und, etc., or one of the letters of a station such as K–3, 9–D, M–4, etc.

Bearing in mind at this stage what was said above about stationary and mobile groups, it should now be possible to discover that some one frequent group, not a number, frequently precedes two or three mobile groups and might be division, brigade, or regiment, or comes always second or third in the sequence, when it might be Uhr, or Komma used instead of Uhr.

If the presumption is in favor of the stationary group being Uhr, a tabulation should now be made of all the groups preceding and following it, going for instance four backwards and four forwards in each case, and keeping the stationary group always in the same perpendicular column.

If the presumption in favor of UHR should be correct, this group should practically invariably be preceded by and most frequently followed by one or two numbers, although as yet the latter may remain unidentified.

It should now be possible to discover von, bis, zwischen, and und, bearing in mind the usual formula as shown in the sample message above.

This is best done by concentrating on the most frequent group (not obviously a number) which almost invariably precedes the one or two mobile groups (numbers) followed by the stationary group (Uhr). If there is any such frequent group it should be "bis." The discovery of "von" follows logically.

As certain Satzzeichen such as Punkt, Komma, or Hindestrich, and certain frequent words such as "und" and "von" occur often in close proximity to numbers, it is well at this stage to try and separate these groups from those representing numbers. This is best done by the system of distinctive marks, as explained above.

When the groups colored in a distinctive way tend to occur in other parts of the messages away from numbers, and in certain more or less easily recognizable positions, they are probably not numbers themselves.

For instance "Punkt" will occur frequently at various parts of messages and often at the end; "und" will of course appear in many places where none of the presumable numbers are around it.

Punkt, Komma, and "und" moreover will not have appeared immediately *before* the Uhr which has been analyzed and its recurrences and sequences tabulated.

By proceeding on these lines it becomes possible to sort out many groups which, though they have a tendency to go with numbers, are not numbers themselves.

Having now arrived at the stage where we are practically certain of having discovered several groups which must be numbers, there are two or three ways in which it will soon be possible to allot values to them.

It is very useful at this stage to color or underline distinctively all presumable numbers, not necessarily in different ways, but by giving a uniform mark to distinguish it as a number.

It will then be possible to concentrate on any agglomeration of numbers which occurs at the beginning or at the end of messages.

This should result in identifying the groups representing units, especially if a careful analysis of all initial groups of messages has resulted in a presumable "an."

By studying the daily Intelligence E (c) summary to see what units are connected with the station concerned, it will be possible to conjecture numbers of divisions, brigades, and regiments.

By comparing one conjecture with another and noticing points of similarity, it will soon be easy to give definite values to the numbers of units. This is done in the following manner.

If one address or signature should be in the order X Y Z, and another in the order V Y W, and if there were regiments connected with those stations with the numbers 245 and 356, respectively; this would easily lead not only to the conjecture that the group Y=5, but also that X=2, Z=4, V=3, and W=6. It might then be possible to find an address, "an (Unit) X W" which might quite well fit as brigade 26 in the sector concerned.

By a system of check and cross-check on these lines many numbers will be identified.

Having got so far it will now be well to concentrate for a time on the numbers before and after "Uhr." Here certain definite assumptions may be made.

The numbers preceding Uhr must range from 1 to 12. If by good fortune there are two numbers in front of Uhr, the first must be 1 and the second 0, 1 or 2.

This was very easy to ascertain in the former series of codes, but unfortunately in the recent ones the compound numbers 10, 11, and 12 are practically invariably used.

If there is only one number after Uhr this will practically certainly be 5, 10, 15, 20, 30, 40, or 50. Of these, by far the most frequent is 30. When there are two numbers after Uhr the first will range from 0 to 5, and the second will almost invariably be 5.

These hypotheses may now help the checking and cross-checking of unit numbers, and may lead to more identifications.

At this stage much valuable assistance will result from an analysis of all messages containing "von — Bis —." Here the second number will obviously be higher than the first, except in such a case as "von 9 Uhr 15 bis 9 Uhr 45", when it will have the same value.

There are other frequent uses of "bis" besides those in connection with times of day, i.e.:

"20 bis 30 Schuesse"
"5 bis 8 Nichts" (in tabulated reports)
"von 4ten Abends bis 5ten Morgens"

which, however, are now almost invariably ordinal numerals, etc.

There are other clues which may lead to the comparative size of a number. A very frequent request is as follows:

"Sofort einen Mann nach KW schicken."

Here the number is nearly always "eins."

In asking for wireless apparatus and accessories one of the most frequent messages is

"Bitte ( ) Akkumulatoren",

where the number is always relatively low—1, 2, or 3.

In reporting the number of messages sent and received, in the form "— geschickt, — empfangen", the numbers are also relatively low, ranging generally between 1 and 8.

In the case of a message which mentions a Chi or Zif number, or the time-group which is always prefixed to each message, it is often possible to discover the message referred to.

For instance, in a message from KS to MD we might discover a group of four numbers, obviously referring to the time group.

Example: "Funkspruch ..... ohne Sinn."

By referring to previous messages on the same day, we find one from the same station timed 1309. The presumption is very strong that these are the four numbers referred to, and if we have already identified two or three of these numbers we can now determine the value of the remainder.

A still more satisfactory discovery is that of a serial report, such as the one quoted above, where the numbers will obviously be consecutive, and will sometimes give the whole series from 1 to 10.

Occasionally, numbers can be identified by their inclusion in spelling groups. Of such numbers "ein" is by far the most frequent, the group for this syllable frequently serving the double purpose of spelling groups and number "eins."

More rarely we have examples such as

"2 Mann RE — *VIER* krank"
"Erhoehte Funken-Telegraphie Bereitschaft, gut *acht* geben"
"Es besteht *zwei* — F E L darueber."

METEOROLOGICAL REPORTS

Meteorological reports are often extremely useful in assigning values to numbers previously unidentified. A characteristic code message would run:

"Wetter Meldung von 26–12–17. Boden wind hundert, null, sechs; zwei hundert, null, acht, fuenf; hundert, null, zwoelf; eins, fuenf, null, null; Barometer 03,6. Temperatur minus 3,6. Feuchtigkeit 92 prozent. Luft gewicht 171,30."

GERMAN WIRELESS PRESS

Another fairly frequent type of message is an extract from the wireless press dealing with number of prisoners and guns captured in some theatre of war. For instance, at the time of the Italian debacle we frequently had code messages of the following types:

(1) "A und B Kompagnie. Hundert achtzig tausend Gefangenen, hundert Geschuetze; an einem Tage sechzig tausend Mann und vier hundert Geschuetze. Gemona ist gefallen."

(2) "Gefangenen Zahl am Isonzo erhoehte sich auf sechzig tausend und 450 Geschuetze."

A study of our own meteorological reports for the same date and time, and a study of the day's German Wireless Press will be very useful. By comparing the code message with the clear it will be often possible to see exactly what the right translation should be.

REPORTS ON FLOODED AREAS

One of the most interesting and at the same time useful type of message is one which appears twice daily on the flooded sector of the Yser. By opening the dams at certain places the Germans are able to flood certain districts.

At the above-stated times each day a certain station sends a code message dealing with the height of the water above and below the dam in question.

As these messages are very stereotyped in form they are extraordinarily useful in identifying numbers far more quickly than would have been otherwise possible.

A typical example runs:

"1ste Reserve Pioniere 13. Wasserstand 6 Uhr
Abend ob–er–strom 4; unter-strom 3,65 Meter."

These things are of course only adventitious aids to the solutions of a code, and are of most use when the solution has already reached a certain stage, i.e., when some of the more frequent spelling groups and words have been identified.

By continual analysis, hypotheses, and experiment on all the above lines, employing analogy where available and first principles when that fails, leaving no stone unturned, and pursuing a perpetual system of check and cross-check, we at length reach the satisfactory stage of verifying all the numbers.

This is obviously a much more difficult task than in the previous series of codes, where it was only necessary to identify one group for each number, but even with the current series the problem is not incapable of solution.

71835—35—2

WORDS AND PHRASES

By the time that numbers have been identified, or at any rate a certain proportion of them, many odd words will have been discovered simultaneously. Of these the most probable discoveries will have been von, bis, zwischen, und, Uhr, times of day, and possibly more or less definitely fixed values of the various synonymous expressions for Schuss, Flieger, Akkumulator, etc.

Having arrived at this stage, further hypotheses becomes more easily possible, and we may be gratified by a leap forward in the solution, and a considerable number of obvious identifications for groups will occur to us.

It is at this stage however that it is necessary to make haste slowly, as there is always a tendency to assume that a certain group must have a certain meaning because of its context in one particular message.

It is here that the critical faculty should step in, and this should be aided by the use of the index which has been made. Before asserting that the meaning of a group is such as we presume it to be on the one example, it is absolutely essential to find all its references in the index, and to assure ourselves that the presumed meaning will fit in all the places in which the group occurs.

Having proved this by at least four or five occurrences we may then find that the group in question occurs in messages where none of the surrounding groups are as yet identified. When this is so it forms the basis of conjecture as to the probable meaning of the groups before and after it.

For this reason whenever the meaning has been proved without a shadow of a doubt it should be written over the group wherever it occurs, and all the surrounding groups should be exhaustively analyzed.

The best and safest method of doing this is to write the group in question on a separate sheet, and to write out its sequences, going backwards and forwards for at least four groups. When the meaning of any of the surrounding groups is determined, the translation of them should be given.

The same process should be gone through with any group that is being experimented on. It will then frequently become possible to form a chain of reasoning so secure that we can safely assume the meaning of the group to be correct on only one occurrence instead of having to wait for its repetition several times to assure ourselves of its correctness.

The basis of reasoning becomes almost Euclidean or algebraical, i.e.

If A=Z, then B should=Y; if B=Y, C should =X,

If C=X, we may by this time be fortunate to find a sentence in which the whole chain is found to be sound and the sentence will read coherently.

It is at this stage of solution that the faculty mentioned above of being able to keep a dozen or 20 groups in one's mind at a time, with their sequences and context whenever known, and any theories that may have been formed about them when first encountered, will be most invaluable.

It is obviously impossible to treat this process at all fully without taking a score or two pages in a code, and reconstructing all the mental processes, all the hypotheses, and all the clues, fruitful or otherwise, which have led to the complete reduction of the code.

A few examples may, however, serve to illustrate the meaning of what has been said above. When a sufficient number of spelling groups had been identified in one particular code to spell out V I Z E—W E B E L, very little additional evidence was necessary to supply the missing group "Feld."

In previous messages a certain group by its position and possible function in the sentence partly decipherable seemed to be a preposition.

By inserting the word "Feld" wherever its equivalent group occurred, it was found in one or two instances to follow the above preposition.

In another case this same preposition preceded a time of day. The assumption was very strong, therefore, that the preposition was "vor", giving "Vorfeld" in one case and "Vor acht Uhr Abends" in the other.

In another case it came followed by "und." This led to the assumption that the group after "und" was "hinter." The assumption, proving correct, led to the discovery "Vor-und Hinter-Gelaende", which fitted in excellently with a patrol report, and led on by successive steps to more and more identifications.

Returning once more to the group for "Feld", it was seen to occur after two unknown groups, where it might be part of a place or name or of the territorial designation of a unit.

The two unknown groups referred to (let us call them X and Y), were also discovered close together in a sequence of groups as follows: W L U E—X W IE Y, where W=another group previously unidentified.

By comparing the two messages we discovered, without undue difficulty, that the last mentioned sequence spelled out

SCH-LUE-SS-EL SCH–IE–BER,

i.e., a sliding alphabet ruler, and that the place name was EL-BER-FELD. By inserting, with the aid of the index, the identification SCH, SS, EL and BER wherever their groups occurred, many more spelling groups were discovered and these in their turn led to others, until most of the spelling groups were discovered.

SPELLING GROUPS

At this stage it is necessary to discuss the use of spelling groups and to know how their solution may be obtained.

In the initial stages of the solution of the codes used by German field wireless stations we were absolutely in the dark as to the nature and extent of the employment of spelling groups.

In many codes, when it is necessary to spell out a word for which there is no equivalent in the code, the custom is to employ spelling groups solely for individual letters.

This means that when the characteristic recurrences and sequences of simple substitution occur, the presumption is that spelling groups are being employed.

By applying the principle of the solution of simple substitution to the particular parts of the messages where these peculiarities are noted, it is a fairly simple matter to discover the groups used for individual letters.

This is especially the case when any outside knowledge of the probable subject matter of the message, or of the names of persons or places likely to be mentioned, is obtainable.

It would, for instance, be fairly simple to spot the translation of the sequence X Q V P Q V (where these letters stand for the code groups employed), as L O N D O N, of W B Z Z B D L B as C A R R A N Z A, of L J C F Q C F M as T H O U R O U T, of X Q S S Y A Y Z Y as Z O N N E-B E K E, of M D Q Q H Y A D Q Q M I Q Y Z as D R O O G E B R O O D H O E K, etc., etc., if these names were likely to be referred to in the text.

As in many codes it is customary to insert a "Buchstabier-Gruppe" i.e., "spelling begins", "spelling end", before and after a word spelled out, it is frequently possible to identify this group by the period of its recurrence, and when once discovered it leads in its turn to the knowledge that the groups within its two repetitions are spellings groups, even if it is impossible at an early stage to identify their exact meaning.

In the code under consideration there are certain frequent abbreviations spelled out. Among these the most frequent of the easily identifiable ones are the abbreviations K-T-K= Kampf Truppen Kommandeur, and R-I-R=Reserve Infanterie Regiment.

They sometimes occur with a Punkt or Bindestrich between them, and sometimes without any separating group.

In the early stages of experiment on these codes one of the things which led to the eventual solution of the code was the very frequent repetition of a sequence of groups which ran as follows: BS WK RJ WK BS. Variations of this procedure were noted, such as BS RJ BS alone; WK BS WK RJ WK BS WK, etc.

Before noticing these various peculiarities the tendency was, on the analogy to simple substitution, to imagine that the first form mentioned above was such a word as N E U E N, N E B E N, S T E T S, etc., but when, later on, the second and third variations were discovered, it eventually became evident that the WK=Punkt or Bindestrich, and that the BS RJ BS=either R I R or K T K.

This was apparently a very slender thread with which to unravel a whole code, but in codes it must be remembered that "c'est le premier pas qui coute", and upon this slender foundation the whole code was eventually reconstructed.

In the code under consideration there were groups for spelling far in excess of the 26 single letters of the alphabet. There were modified vowels, double consonants, frequent diphthongs such as AU, EI, EU, IE, etc., and frequent combinations of 2, 3, or even 4 letters such as BL, GR, SCH, HEIT, etc.

This made the problem of solving spelling groups more difficult, and it was not until this fact was realized that further progress was made. There still were however certain characteristics in the sequences of certain groups, which pointed to the fact that they must be spelling groups.

As was seen above there were sequences in the code, which might be spelling such words as "neuen", "neben", or "stets" which turned out to be K T K with Punkt or Bindestrich interspersed, but having thus obtained a very possible punkt it became possible to block out the messages into groups representing phrases or more or less self-contained sections of the text.

It was mentioned in the section above which dealt with the solution of numbers that when the code was analyzed with a view to marking in some distinctive way sequences of groups which occurred very frequently in the same order, but with different groups before and after them, the presumption was in favor of these sequences representing words or names spelled out in full.

It would be too great a stretch of the long arm of coincidence if on different dates, at different times of the day, and from different stations, there should be the same repetition of 4 or 5 groups which would stand for the same numbers before and after Uhr, or for exactly the same sequence of words in a stereotyped phrase such as for example

"25 Schuesse auf Abschnitt" or

"Waehrend der Abend Stunden Flieger Taetigkeit gering."

Therefore by collecting several of these frequently recurring sequences, analyzing and comparing them, and noticing certain clearly defined characteristics, and at the same time conjecturing what some of the most frequently spelled-out words or names would be, it became possible to determine the value of a good many spelling groups.

This process was materially aided by the fact that several of the frequently used spelling groups were also capable of being used as single words, e.g., in, an, ich, ist, es, da, ein, acht, und, etc.

As a fair proportion of these were capable of being discovered by other methods, such as their recurrence in certain definite places in a message such as "an", or by analysis having proved some of them to be numbers such as "ein" and "acht", we were already on the right road to find out some of the single letters and spelling groups.

Such words as ES T AM IN ET, L AM P E, W ACHT ME IST ER, FL AN DER N became gradually capable of solution. Having, as explained above, discovered the values of the groups for K and T from K T K, we were very soon able to identify such a word as T A K T I SCH or more easily still K O N T A K T.

This "premier pas" had started us off on the high road to success, after repeated failures, "culs de sac", and the inevitable preliminary groping in the dark which characterize the first attempts at code solution.

One of the most interesting words which helped in beginning to get out the spelling words in a new code was a sequence of groups in the order Q W X Q W X W. This turned out to be B A R B A R A, useful as the code name of a certain unit.

The fact that the same word was spelled out in a succeeding message as B AR B AR A gave us the group for "ar."

Having got a possible "S" in the word P O S T in another part of the code, we were soon able to identify another group as S A TZ B U CH. From this point all was plain sailing.

As the tendency in recent codes, however, has been to increase not only the number of groups for single letters, and short words such as "an", "in", "ist", etc., but also to add groups for less frequent spelling groups such as NG, CHT, RS, etc., the difficulty of solving groups on first principles has increased. The difficulty even then is not as great as it might otherwise seem to be, if the analysis is searching and thorough enough.

For instance it is possible to notice that the same sequence of groups sometimes occurs practically identically, but with one group varying in the different sequences.

When it is noticed that of these repetitions of an almost similar sequence two may be in the form

X K K X Q X T

and the third in the form

X K K W Q W T,

the presumption is very strong in favor of the groups represented by X and W being equivalent to the same spelling group or letter.

When a little thought had resulted in this sequence suggesting the word A P P A R A T, we not only have definite values for the P, R, and T but also the value of the two groups representing A.

At this stage it will be as well to repeat what cannot be too frequently insisted on, namely, that, when any value is discovered for a particular code group, this value should be immediately transferred to it every time it occurs in the code.

The mere fact that there are a few odd words, spelling groups, or letters hanging in the air in a message, will lead to new theories, which can be proved or disproved by reference to their context.

Spelling groups having been shown above to possess certain characteristic sequences when carefully analyzed, it is now possible to determine with more or less accuracy what groups are spelling groups, and apply certain principles of frequency to them.

The frequency tables used in solving substitution ciphers will obviously not apply when, as in the particular type of code we are studying, there are groups for compound letters, in addition to those for the single letters.

For example, the letter E, which is the most frequent letter in most languages, will in this code tend to become one of the less frequent groups, owing to its forming part of so many spelling groups.

For all single vowels excepting O in this code, there are two code groups, and as O only occurs in two words which can be used as syllables, namely, "WO" and "SO", and as moreover it is a fairly frequent letter, it should assume importance if analyzed among spelling groups.

It eventually becomes possible to discover a relative frequency of initial and final spelling groups, although this cannot be done with anything like the degree of certainty as in cipher. E, EN, ER, ST will be frequent final groups; GE, SCH, ST, ER, BE, VER will be frequent initial groups.

Of single letters at the beginning of words some of the least frequent in cipher, or in spelling in code when only equivalents for single letters are used, will tend to become much more frequent, owing to the fact that their relative infrequency in clearly defined spelling groups causes them to be employed alone.

Thus, D, F, K, M, P, W, and Z will rise to a much higher rate of frequency among letters than they reach in cipher.

STATION CALLS

In these codes many valuable identifications of single or modified letters may be obtained owing to their use in station calls. Each German field wireless station uses a particular call sign, and this consists generally of two single or modified letters with an occasional number.

Some stations are in the habit of putting these station calls into code, and when dealing with messages from such stations, bigroups between "Punkts" or at or near the end of messages should be looked for.

A list of call signs of the groups of stations concerned together with that of the adjoining ones should be referred to, and if one letter of a call sign is known the other will be readily found.

Compare the following message with list of calls:

"WO BLEIBEN GEGENWART STATION MELDUNG MEHRZAHL VON PUNKT SJ MO PUNKT RB SB PUNKT MO NE UND RT NE PUNKT."

List of calls: BD NT KS MO ER SG FG.

A glance at the above will show an important point, namely, that the final group of one bigroup is the same as the initial one of another, e.g.,

SJ MO MO NE

By consulting the list of calls it will be found that two of them have the same peculiarity.

K S S G

From the above SJ MO were assumed to be K S and MO NE to be SG. This again gave RT NE as F G which gave a further identification, viz, RT SB as F R.

Having now arrived at the stage where a great many spelling groups have been discovered, we are in a position to discover many short words, which are at the same time used as spelling groups, but which if inserted into their respective places wherever they occur as single words, fix a valuable basis for conjecture as to the meaning of their context. Some of these have been mentioned above, but there will be no harm in recapitulating a few of them.

The spelling M E IST ER gave "ist," which is a very valuable word in a sentence. GE WO R DEN gave WO and DEN, both extremely useful single words.

The spelling of P I RE ALLE R, a place not far from St. Quentin, constantly referred to in artillery reports, verified "alle", which led to the phrase "an alle Stationen."

KOMMA N D O definitely established "Komma" as distinct from Punkt or Bindestrich.

ACHT UNG proved the conjecture for the number "acht" to be the right one.

Leutnant NEU MANN and other proper names ending in "mann" eventually helped in the discovery of TOT, VERWUNDET, KRANK, etc.

BE T H MANN HOHL WEG established WEG as distinct from GRABEN or STRASSE and also gave us HOHL.

The average German operator is not very particular about correctness of spelling as shown in the above misspelling of the Chancellor's name; some of his misspelling, involuntary or jocular, have given us many valuable short words, and at the same time caused us a certain amount of amusement.

A place called "Itancourt", near Pirealler, frequently referred to in connection with artillery reports was spelled out by one sportsman as I T AN C UHR T. Uhr also appeared once in UHR L A UB.

B U K O WIE N A gave "wie", which with "ist" and "wo", quoted above, helped in the discovery of Fragezeichen, as we noticed that interrogative sentences nearly always had a characteristic final group which had previously puzzled us.

SCH MIT for Schmidt was valuable in proving "mit."

TEL E F O NIE SCH and even NIE CHT for "nicht" gave much help.

On the occasion of the promotion of one wireless operator to be a Funker, a comrade at another station sent the message

"ICH GRAD U L IE RE"

It seemed almost too good to be true that the group between ICH and ULIERE should be the word "GRAD", but this was confirmed by the use of the index, as we discovered that it came in a meteorological message referring to temperature, and also in GRAD AUS for "gerade aus."

FR OE H LICH E WEIN ACHT EN gave the group "Wein."

SCH ON EN DANK was also useful in verifying the possible identification for "Schon."

The gem of the whole collection however was "E SS EN"

"E SS EN (gegenwart) Abloesung schon da", which reminded one of the old Latin catch of one's school days "Mea mater est mala sus!"

It must be remembered, however, that such helps as these only come when a code has begun to reach a fairly advanced stage of solution.

None of these things which seem so simple and help such a lot at a later stage can take the place of a proper method of attacking a new code, and a firm grasp of the general principles of code solution, coupled with a long and exhaustive analysis on the lines laid down above.

Analogies with previous codes, and as much outside information as may be obtainable, must be worked to their utmost extent, but when the nature and structure of a code change, or when previous station procedure is no longer adhered to, it is necessary to start working on first principles.

As in the course of the preceding treatment of the solution of spelling groups frequent reference has been made to the principles of simple substitution ciphers, code solvers should make themselves familiar with the main principles of the solution of this form of cipher.

It would take up too much space in this pamphlet to discuss at the requisite length the methods adopted in this process, but information on this subject together with examples for practise, will be found in the "Manual of Cryptography."

A few dozen examples worked out, and a study of the tables of frequency of the language used in the code, and of its characteristic sequences, will prove very useful as a preparation for the study of the solution of codes.

HILFS-SIGNALE

In the particular code under consideration there is a recognized procedure in regard to "Hilfs-signale", and the discovery of these is often of great use towards the complete solution of a code.

Some of those have already been referred to, but at this stage a detailed consideration of their nature and use will be of value.

"Hilfs-signale" are grammatical groups placed after certain words to alter their meaning wherever necessary. The most frequent of them are indications of the tense or number in which a verb is intended to be translated, or of the number of a noun.

They will each be treated separately under their various headings, with an example of their respective uses, and the method of discovering them explained wherever necessary.

(1) *Hauptwort* (noun). This group is placed after a verb or an adjective when the corresponding noun does not exist in the code, e.g.:

"S.O.S. ist der drahtlose anrufen (Hauptwort) (i.e., Anruf) eines Schiffes das sich in groesster Gefahr befindet."

"Welche Wellen-lang (Hauptwort) (i.e., Laenge) gebraucht die Station?"

The context is often sufficient to determine the function of this group. Inserted at each recurrence by the aid of the index, it is often very useful in conjecturing the actual meaning of the preceding group, hitherto unidentified.

(2) *Einzahl* (singular). This is used to indicate the singular of a noun, of which only the plural form exists in the code, e.g., after "Kerzon" (inserted in the code in the plural because of its frequent use in speaking of candle power), or after "Kontroll scheusse", "gelbe Leuchtkugeln", "Granaten", etc., of which only the plural form is given.

It is also used after verbs to indicate the use of the singular number, e.g., "Wo bleiben (Mehrzahl) Abend Meldung," and even occassionally to convert a verb into a noun, i. e., "Reihen folgen (Einzahl)" "Reihenfolge."

(3) *Mehrzahl* (plural). This is one of the most frequently used grammatical groups. It indicates the plural number of a noun referred to, and is very frequent after Schuss, Kompagnie, Akkumulator, Funkspruch, Graben, Flieger, etc., etc.

Example, "30 Schuss (Mehrzahl) auf Graben (Mehrzahl) westlich von (Place name)."

Owing to the frequency of this symbol, it can often be very easily discovered. When beginning to analyze a code, all groups which have a tendency to occur in pairs should be specially marked, and the two groups bracketed together. It will then be found that one of them is invariably the second one of the bigroup.

When this second group occurs frequently as the second member of several bigroups it will frequently turn out to be "Mehrzahl." Conjecture as to this may be facilitated by a consideration of the position of these bigroups in the message.

This often helps to discriminate it from "Mittelwort der Vergangenheit" (past participle) which is also a very frequent "Hilfs-signale."

As it is exceedingly useful in guessing the meaning of a whole sentence to know that a certain group is either a noun or a verb, any group which has the newly discovered "Mehrzahl" after it, should be bracketed to it, and should be noted as a noun.

This noun, although as yet unidentified, should be noted as such, by the aid of the index, every time it occurs even when not accompanied by the plural sign.

(4) *Eigenschaftswort* (adjective). This is comparatively rarely used, but may serve to turn a word which only occurs as a noun in a code book into an adjective. When discovered, its occurrence should be similarly noted, as for "Mehrzahl."

(5) *1ste Steigerungs form* (comparative).

2te Steigerungs form (superlative).

These two symbols, as their name implies, give the degree of a comparison in which an adjective is to be translated, e.g.:

"Feindliche Artillerie Taetigkeit ruhig (1ste Steig. form) (i.e., ruhiger) als am Abend vorher."

"Gross (2te Steig. form) (i.e., groesste) Gas bereitschaft."

Any symbol followed by one of these degrees of comparison must be an adjective, and its occurrence, singly as well as accompanied by the degrees of comparison, should be noted, and its function inserted, even where it is as yet impossible to define its exact meaning.

(6) *Zeitwort* (verb). This group serves to indicate that a word which is only given as a noun in the code must be translated as a verb. Its use is, therefore, the converse of "Hauptwort" and it should be treated accordingly.

(7) *Gegenwart* (present tense), *Vergangenheit* (past tense), *Mittelwort der Vergangenheit* (past participle), *Zukunft* (future).

These serve to indicate the tense of a verb.

Example. "Regiment melden (Gegenwart) (i.e. meldet) dass Feind in unsere vorderen Graeben eindringen (Mittelwort der Vergangenheit) (i.e. eingedrungen hat).

Any occurrence of these tense symbols should be noted and treated in a similar manner to Mehrzahl or 1ste or 2te Steigerungs form as described above.

(8) *Buchstabier Gruppe* (spelling begins or ends). The use of this symbol has been described above when treating of spelling groups and their solution.

SATZ-ZEICHEN

For the very lucid and stimulating treatment of the various Satz-zeichen used in German field wireless code in the section which follows we are indebted to Lieut. D. Macgregor, whose collaboration has been of very great service to us in clearing up knotty points.

It would be very good practice for the beginner in code work to take the examples he gives, and endeavor to solve them before referring to the key which follows.

"A beginner in code solution is apt to fancy that punctuation marks are a very unimportant branch of his subject. This is quite wrong. They are of paramount importance; and any neglect of them, or any slipshod identification, not only bars the way to many valuable discoveries, to which their accurate identification would have led, but obstructs and obscures the whole work of solution. The mistake, if a fatal one, is still natural."

Given a complete, intelligible sentence, it often matters little if a colon be put for a dash or a stop, comma for brackets, or, say, an exclamation mark be left out.

But the code solver is not dealing with complete or intelligible sentences. At the start he is dealing with wholly unintelligible sentences, and even after a month's work he is hampered by unknown groups, by Morse errors, manuscript or typescript errors, and nearly every kind of doubt and difficulty which can be conceived. Here it is that the Satz-zeichen play their part.

At the start, thanks to the mechanical unintelligent pedantry of the German, they are themselves, some of them, readily discoverable, and they lead directly to solution of the preliminary difficulties; later, they act as guides to the sense, giving form and construction to the unintelligible, guiding and controlling the conjecture of the investigator.

In a word the study and discovery of these signs is not a mere scholarly refinement, a finishing touch to the work of solution; it is an integral and indispensable part of that work.

The following notes and examples are intended to illustrate this point, and to indicate a few of the technical uses which the solver can make of the Satz-zeichen. But it must not be forgotten that the rules given below are not the laws of nature or even grammatical canons. "Anforderung" is not always followed by "Doppelpunkt", most often it has no punctuation at all; sentences frequently follow each other without a "Punkt" between them; "8–30" is often written "830". Some codes scarcely punctuate at all. Nevertheless in any code where punctuation is regular it will be found to follow the lines indicated, and a full knowledge of these will be of incalculable value.

I. Punkt.—(*a*) Separating sentences; normal and frequent, not infrequently at the end of short, single-sentence messages.

(*b*) As the mark of abbreviation:

```
GE SCH AE F T S Z PUNKT
ST RE ICH H PUNKT
K PUNKT T PUNKT K PUNKT
R PUNKT I PUNKT R PUNKT.
```

Note especially GE XYZ PUNKT, where XYZ should always be tested for FR, giving GE FR. = Gefreiter.

(*c*) With figures; very frequent. Between a number and the unit to which it applies:

```
AN 8 PUNKT INFANTERIE BRIGADE.
1 PUNKT KOMPAGNIE.
```

Very frequent in tabulated messages, before and after (more commonly only after) figure or letter headings:

3 PUNKT ANSCHLUSS VORHANDEN 4 PUNKT SICHT DUNKEL
5 PUNKT NICHTS ETC.ETC.

Rarely=Uhr. "2 Punkt 30" (see under Komma).
Regular in dates: "12 Punkt 1 Punkt 18 Punkt."
(*d*) After the "address to" and before "address from":

BRIGADE PUNKT LAGE RUHIG PUNKT UNTERSCHRIFT K T K.

The following pair of actual messages affords an excellent example of various uses of the Punkt and of the incalculable value of the Punkt in the initial stages of solution. On the basis of these messages alone some 15 identifications can be made. The beginner should try his skill on these.

(A) TL v LQ 0245 GR 12 UFK RUR KNI ULT RWL RUR UF0 KQT
KHY RND RST UVG

(B) LQ v TL 0245 GR 48 UFK UVG KQT ROF KNI KNW UU0 RQW
RUR RWL ULT KNI RUR RWL UJQ RFP UIW KLD KNI RZT
UZM UJM RWL RTQ RXP KNI KWR KVT KNI KPG RZT RZI
KBD ULG KGD RWL RUR RTZ RYP ULT RBZ KNI RZT UZM
RUR ULT RUR

In passing a word or two on the "Punkt" (nicht das Satz-zeichen). This is used in the following ways:

(*a*) Topographical: "Zwischen Punkt L und K in Planquadrat" etc. Frequently preceded by "rot" or "blau."

(*b*) As a word or part of a word "Zeit-Punkt" "Punkt-lich."

(*c*) As the "Satz-zeichen." This is naturally very rare, but is commoner than might be supposed and has frequently been exceedingly useful.

In general, Punkt (nicht das Satz-zeichen) is a very valuable group and demands great attention. It must on no account be called "Kartenpunkt" or its other uses will be obscured, and the color identifications (a very difficult subject, the investigation of which is still in its infancy) to which it often gives the first clues, will be hampered and delayed. "Kartenpunkt" for which there is a separate group is probably very uncommon.

II. Komma.—Less frequent and, on the whole, markedly less useful to the solver than the punkt.

(*a*) Normal use—separating parts of a sentence.

(*b*) With figures=Uhr or decimal point—Very uncommon.

(*c*) *Very* rarely for Punkt after an abbreviation.

(*d*) KOMMA N D O used to be frequent, but seems never to be used now.

(*e*) In tabulated messages occasionally used as follows: "3 Punkt, vorhanden; 4 Punkt, dunkel; 5 Punkt Komma, 6 Punkt unveraendert" etc., where evidently Komma stands for "nichts" or the like (also Bindestrich & Trennungstrich) or means that 5 and 6 are "unveraendert."

III. Doppelpunkt.—Quite normal in use. The *locus classicus* is after "Anforderung" but it is frequently after the heading: Meldung Doppelpunkt, Eigene Taetigkeit Doppelpunkt, Verluste, etc., etc. Also found in map scales. (See example given under "klammer.") It naturally overlaps sometimes with Trennungestrich, e.g., "Losungswort : Deinz" and "Losungswort—Deinz" are equally correct.

IV. Bruchstrich.—Not frequent but easy to identify and enormously useful. But it must be identified exactly; under no other name does it smell so sweet. A vague rendering such as Strich or Komma hinders, not helps.

(*a*) "1/4 Stunde"—not common, but it must not be thought than an example of this use is necessary to prove the identification. The use and value of the Bruchstrich was discovered independently of this simple case; and the identification can now be made and used with absolute confidence in any code without a thought of fractions.

(*b*) Between battalion, company, or battery, and regimental number:

1/116=Bataillon 1 Regiment 116.

12/94=12th Kompagnie Regiment 94.

and so forth.

But the usage does not stop here. The following is a pretty "Bruchstrich identification": KGG/KIEL (Presuming that KGG is known not to be a number)=Bataillon I II or III Regiment Kiel.

Or take the following equation (signature of corresponding Meldungen on successive days): "RMC/RSJ"="2/RSJ—solve for the two unknowns RMC and RSJ; clearly RMC=Bataillon II", obtained from the order of battle maps.

NOTE.—The equation RMC XYZ RSJ=2 XYZ RSJ is, of course, easily soluble for the three unknowns in the same way, so that the previous knowledge of the Bruchstrich was unnecessary here. But this is an exceptionally simple and lucky case, and usually one is dependent entirely on the Bruchstrich for this kind of identification. Of course in the later stages of a code the group Battalion I II III are quite clearly recognizable on other grounds. The value of the Bruchstrich, as of the other Satz-zeichen, belongs mainly to the initial stages so far as *direct* identification is concerned.

(*c*) In Machinengewehr 08/15.

(*d*) In the various phrases "Empfang 2/2", "Hier 1/1", etc.

XYZ 2/2
FLIEGER TAETIGKEIT XYZ REGE

where of course XYZ=Beiderseits.

(*e*) Sometimes in map references.

V. Trennungsstrich.—This overlaps with Bindestrich in many uses and until recently was confused with the word "Unterschrift."

(*a*) Separating "address to" and "address from" from the text. In this use it is seldom (? never) preceded by Punkt. "Unterschrift", which is very common, naturally only separates "address from" from the text and may or may not be preceded by Punkt. In "Caesar" RIW was called Trennungstrich although this left UUD, a palpable Satz-zeichen, at a loose end. The former was, it is now clear, "Unterschrift."

(*b*) As a dash or "Gedankenstrich" in sentences, its use is quite normal. Sometimes preceded by Punkt. "Besatzungen, gesund Punkt Trennungsstrich, Satzbuecher erhalten."

(*c*) =bis. (cf. Bindestrich.)

(*d*) See Komma (*e*). Trennungsstrich and Bindestrich are much commoner in this connection than Komma.

VI. Bindestrich.—(*a*) Normal use as hyphen;
Artillerie-Schutz-Stellung
Funken-Telegraphie Bereitschaft
Infanterie-Schutz
Strasse Messines-Wervicq
(*b*) =bis. (cf. Trennungsstrich.)
(*c*) See Komma (*c*).
(*d*) With figures, in giving strengths of units, (note position of Punkt—see Punkt (*c*)).

1 PUNKT KOMPAGNIE 2 BINDESTRICH 5 4 2 PUNKT KOMPAGNIE 2 BINDESTRICH 13 BINDESTRICH 7 3 3 PUNKT KOMPAGNIE, ETC. ETC. I.E. NO. 1 COMPANY 2 OFFICERS 8 N.C.O'S AND 54 MEN, ETC.

A run of numbers in this form may easily yield identifications, such useful words as Kompagnie, M. G. Kompagnie, Minenwerfer, Bataillon, and others, which the following example illustrates:

UQV KSO KZA 12 KER BINDESTRICH 32 RUV BINDESTRICH 292 RZS KJV KZA 2 RZA RLC

identify KSO KZA KER RUV RZS, and, with the help of the following—UQV KJV RLC:

STREUFEUER AUF DEN HINTEREN UQV MEHRZAHL
SOFORT DRINGEND EIN WAGEN FUER EIN LEICHT UND 2 RLC.

VII. Fragezeichen.—Frequent and normal in use, but very often omitted where there is no ambiguity. Very occasionally followed by Punkt at the end of a short message. Its importance for the discovery of other groups—ist, sind, was, wie, warum, etc.—is plain. The following should be tackled. A reasonable conjecture can be, and was, made for the four underlined groups on these messages alone; it proved correct, and was of great use in solution when more material came to hand. (The Fragezeichen is omitted in these messages.)

DECEMBER 12—69 V ZB ZIF 3 RRR KZJ URE
DECEMBER 12—ZB V 69 ZIF 9 URE ETC. ETC.
DECEMBER 12—NQ V OY GR 2 URE RKM
DECEMBER 12—LQ V GU GR 9 UKT ETC. ETC. RKM.

VIII. Ausrufungszeichen.—Commoner than might be supposed. Comes after commands, urgent and reproachful questions (Wo bleibt Vorpflegung! etc.) and, of course, "verboten!" Not of great help to the solver, but sometimes gives a useful clue since it indicates the general nature of the preceding message. Negatively, its discovery is a great advantage; for it is a thorn in the side so long as it rests unidentified.

IX. Klammer.—Rare and elusive. Is usually given away by a foolish operator using the same group for the beginning and the end of parenthesis—after that the way is smooth. Generally useful when found; unidentified, it is a most treacherous and dangerous will-o'-the-wisp.
(*a*) Normal—for any parenthesis.
(*b*) Very rarely enclosing the heading numbers in tabulated messages.
Fill in the blanks in the following:

ZWISCHEN — — C UND D IM — 7D 36C — 1 DOPPELPUNKT 10 — —

Solutions to examples:

I. (*a*) AN K PUNKT T PUNKT K PUNKT MITTE BITTE MORGEN MELDUNG REGIMENT.

(*b*) AN REGIMENT MITTE EINE PUNKT MAESSIG{UUO / ----} feuer{RQW / ----} KALIBER K PUNKT T PUNKT K PUNKT BINDESTRICH RFP HAUS ZWEI PUNKT OHNE AENDERUNG DREI PUNKT VORHANDEN VIER PUNKT DUNKEL FUENF PUNKT ABLOESUNG OHNE NEU–IG–KEIT–SECHS PUNKT K A L T SIEBEN PUNKT OHNE AENDERUNG K T K.

It may be objected that U J P might be zwei—it follows a Punkt after K T K. This is quite fair; and the figure identifications should perhaps read R O F eins, Y J P ?2, K L D ?2 or 3, etc. The difficulty however would be cleared up very quickly.

VI. GRABEN STAERKE DOPPELPUNKT 12 OFFIZIER BINDESTRICH 32 N/OFFIZIER BINDESTRICH 292 MANN VERLUSTE DOPPELPUNKT 2 MANN SCHWER VERWUNDET.

VII. Wo bleibt Anforderung
Anforderung etc. etc.
Anforderung?
Ist etc. etc.?

} These of course are only "reasonable conjectures", not certain identifications.

IX. Zwischen Rot or Blau Punkt C und D im Planquadrat 7D 360 (1 : 10 tausend)

GENERAL HINTS AND SUGGESTIONS

It cannot be too frequently insisted upon, at this as at every other stage of code solution, that work on back messages should go on concurrently with that on the new material which continues to come to hand.

In fact it is often far more useful to concentrate on a dozen or more back messages, where there are frequently some which contain only a few untranslatable groups, or at any rate, some which have reached a sufficiently advanced stage of progress to enable the general meaning of the whole message to be conjectured.

It is necessary to dig deeply as well as widely in the process of code solution, and one message, if worried as a dog worries a bone, will sometimes yield more marrow than several pages discursively scanned.

It is well never to insert a conjectural translation into the code sheets, until it has been definitely proved. This is a dangerous proceeding and leads either to preventing the right meaning of the group being discovered, or to wrong conjectures being made about surrounding groups. All theories still in the air should be written on a separate sheet and kept until verified or disproved.

DISTRIBUTION OF WORK

When there are several people working on one code—and the more, not only the merrier, but also very much the faster—it is well to divide the work among them in the following manner.

One should sort all material as explained at the beginning according to place of origin, destination, etc., others should type all messages received in the manner laid down earlier on.

Several copies of each sheet should be made for distribution to those who have to work on them.

All sheets should be clipped together in such a manner that they can be easily handled, and should be kept in consecutive order, so that their subject matter may be chronologically arranged.

Others should be responsible for keeping an up-to-date index of all groups occurring in the code.

One person should be responsible for recording all identifications of code groups in a special index, correcting wrong or insufficiently specified meanings as the right meaning is discovered.

The rest of the available staff should be the actual solvers.

One person should be the controlling mind of the whole work of the code. He should check all theories, be personally responsible for the accuracy of every identification inserted in the index, suggest fruitful lines for experiment, and distribute any possible clues discovered among the remainder of his staff for separate experiment.

When one clue seems likely to be a fruitful one, everybody should work at it until it either proves to be the right one or is definitely discarded as leading nowhere.

All those engaged at work on the same code should work in harmony and conjunction one with the other.

No personal motives, and no jealous desire to keep possible clues from others, in order to have the credit of discovering or proving it, should be allowed to enter into the work.

Every mind should be bent towards the same end, namely the finding of the first identification to start building on, and the complete reduction of the whole code at the earliest possible moment.

Two heads are always better than one, and mutual discussion of possibilities will lead very far on the right road.

Nevertheless, after a certain stage has been reached it is often well to divide the work more or less roughly on the following lines. One person might concentrate on initial and final groups, another on an exhaustive study of numbers, another on spelling groups, another on common words and phrases, another on Hilfs-signale, and another on the discovering of the exact function of all the various marks of punctuation.

At the same time, as the code is an entity, it is obviously impossible to lock up these various things in water-tight compartments.

The discovery of a group for a particular unit will help in that of numbers, the discovery of a note of interrogation will assist in finding frequent interrogative words, and so on in every aspect of the work.

In conclusion, enough has been said to prove that no code ought to be insoluble, given a sufficient quantity of material, a proper method of work, the necessary qualities in the would-be solvers, and sufficient time between changes of the code book to admit of the reduction reaching such a stage as to yield information even if only fragmentary.

In code, as distinct from cipher, a certain length of time must elapse before complete or even partial reduction is possible. The time taken is directly proportionate to the amount of

material to work on, to the amount of outside information or of analogy with previous codes available, and to the number and experience of those engaged on it.

In a cipher, a fortunate shot may result in the finding of the system, periodicity, or keyword on the very first message, or at any rate on two or three, and the key once discovered, all material enciphered in the same system is immediately decipherable, whereas with a code, the translation of one message does not render the other messages decipherable.

Cipher deals, moreover, with the more or less mathematical arrangement of 26 letters, while code deals with anything from two to three thousand words.

It is obvious to the meanest intelligence that no meaning can be conjectured for a code group until it has been used in messages at least once, and frequently not until it has been used sufficiently often to enable its sequences to be experimented upon.

A code is not solved in a day, nor even in a week—not even by a miracle. Complete reduction of a code can only be attained when every group existing in it has been used in messages.

Nevertheless, it is often possible, as shown above, to obtain a certain amount of very valuable information, even when only about a hundred groups are solved, especially if several of these are the groups for numbers and units.

With the aid of the numbers, dates, times of day, and identifications of units are discoverable.

One final word. The fundamental principles of science and inductive logic hold good in code solution as in any other similar study. The material having come to hand, the phenomena are present.

Observation, experiment, hypothesis, verification are the links in the chain, and when the chain is complete in every link, a certain feeling of gratification may legitimately exist as the result of "something attempted, something done", which may help to shorten the war if only by 1 day.

○