~~SECRET~~ Register No. 59

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

ANALYSIS OF A MECHANICO-ELECTRICAL CRYPTOGRAPH

PART I

NO ACCOUNTING NECESSARY

REGISTRATION CANCELED
by
Authority Hqs. ASA ltr dated 27 Feb 46
2d Ind 11 Mar 46, signed:
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

~~SECRET~~

Register Nº 59

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

ANALYSIS
OF A
MECHANICO-ELECTRICAL CRYPTOGRAPH

PART I

TECHNICAL PAPER

BY

WILLIAM F. FRIEDMAN
Cryptanalyst, Chief of Signal Intelligence Section
War Plans and Training Division

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1934

CONTENTS

ANALYSIS OF A MECHANICO-ELECTRICAL CRYPTOGRAPH

PART I

SECTION I

INTRODUCTORY REMARKS[1]

1. **Nature of investigation.**—In the latter part of 1923, a crytographic machine called the "Hebern Electric Super-Code" was submitted to the Chief Signal Officer for examination and consideration relative to its suitability for use in the military service. The usual claims for indecipherability were made for this machine, which had also been submitted to another Government department interested in such devices, and had already been most favorably considered for adoption into their service.

This investigation was undertaken with a view to determining the merits of the device, more especially as to whether the degree of secrecy afforded by its use is sufficient to warrant further consideration as to its suitability for adoption in the military service.

2. **Preliminary statement of results.**—A cursory examination of the machine soon showed that it was worthy of the closest study. It is the smallest, most compact, and rugged device of its kind, considering the degree of secrecy which it is possible to achieve by its use. The latter factor seemed to be considerably higher than that afforded by any other machine heretofore examined, excepting the Printing Telegraph Cipher Machine, which, in its present form, is much bulkier and not at all suitable for use in the theater of war below Army Headquarters. As a device for use in the field, the machine herein described seemed more nearly to fulfill the necessary requirements than any other machine ever studied by the writer.

3. **Purpose of this paper.**—This paper was written for the purpose of setting forth in detail the results of the study of the cryptographic features of this machine. It is usually true that every really scientific system of cryptography presents a more or less unique case in cryptanalysis, for the solution of which new principles and special methods of attack must be devised. In this respect the system herein described does not lack novelty and interest for the cryptanalyst, and if only for scientific and theoretical considerations that are involved in such a study, it has been thought worthy of being made the subject of detailed investigation and presentation. A preliminary knowledge of the more important and fundamental principles of cryptanalysis is necessary for a proper understanding of the technical details of this analysis. Reference is therefore made to Signal Corps Training Pamphlet No. 3, "Elements of Cryptanalysis", wherein will be found elucidated the basic principles of the science.

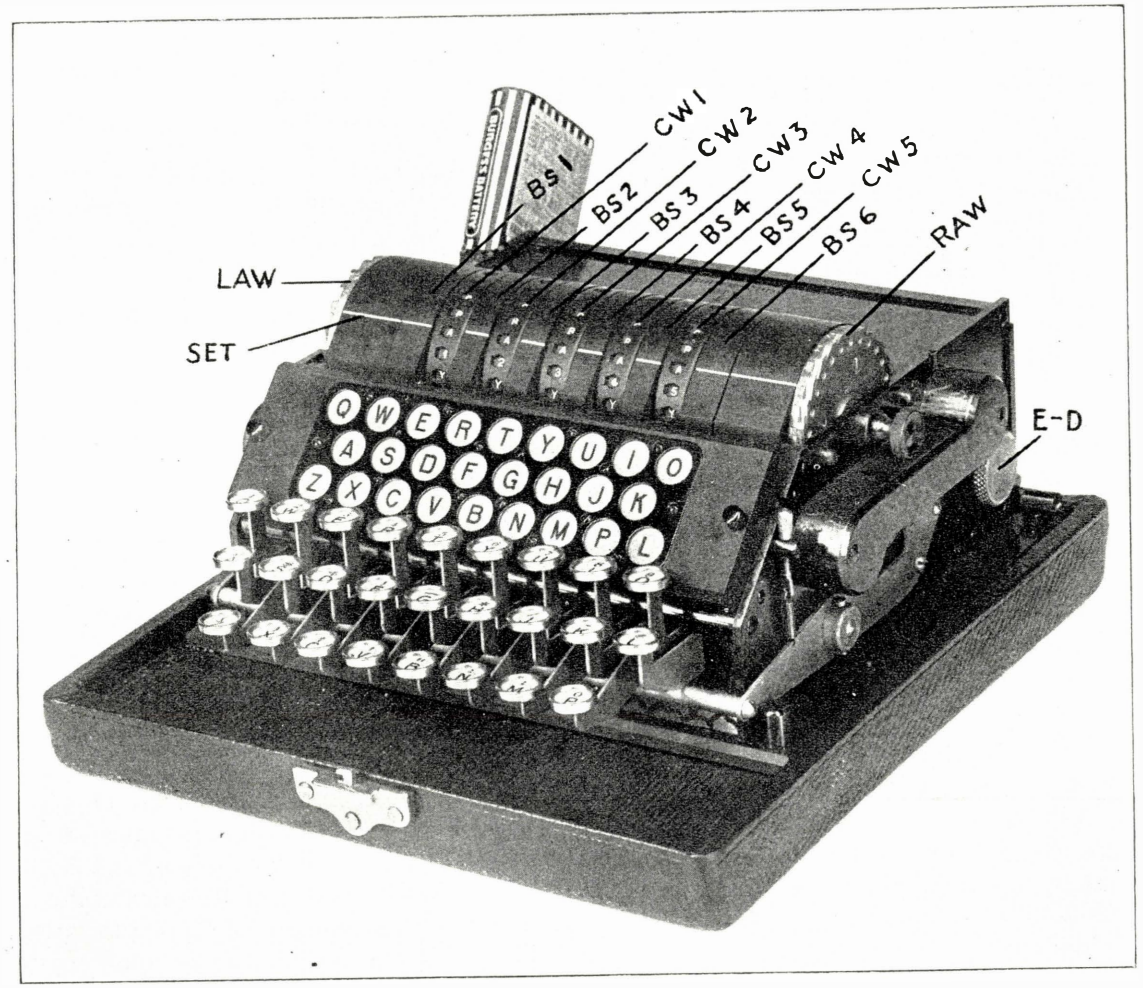
There is also a further purpose in recording the results of this investigation. The Hebern machine is but one of several recently patented cipher devices that are based upon very similar

[1] This paper was written early in 1924, soon after the successful conclusion of the tests described in the subsequent pages. Practically no changes, additions, or deletions have been made in the text as originally prepared.

cryptographic principles. The analysis herein presented is applicable to them, with minor modifications necessitated by slight differences in mechanical construction. With the ever increasing employment of radio telegraphy for military purposes, and the necessity for speedy, mechanical or electrical cryptographic apparatus, it is quite probable that machines of this nature will be used in future wars. They may, of course, be utilized by enemy military forces. A knowledge of the methods of analysis herein contained would be valuable and essential in the study of intercepted messages written by means of such devices. For this reason it has been deemed advisable to issue this paper as a secret document.

4. **Summary of conclusions.**—It is shown in this paper that the machine under investigation, as at present constituted, produces cryptograms which are by no means "absolutely indecipherable", or even "practically indecipherable." Nevertheless, the degree of secrecy is fairly high, and the machine offers possibilities for modification with a view to augmenting the degree of secrecy. One of its most serious disadvantages is that it makes no record of its operation, in the form of a printed copy of the dispatches enciphered or deciphered. It is understood that the manufacturers are now engaged in producing a model which will make a printed record. If their efforts are successful, the new machine may be worthy of serious consideration for use in the military service.

Plate 1a (To face p 3)



Section II

DESCRIPTION OF MACHINE AND ITS OPERATION

5. **Terminology.**—For convenience in discussion, those parts of the machine which are essential to an understanding of this paper will be referred to under the following designations, which apply to Plate 1a:

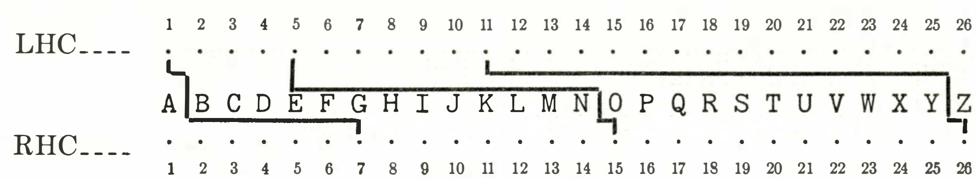
LAW—Left-hand aluminum wheel.
RAW—Right-hand aluminum wheel.
CW1—First cipher wheel.
CW2—Second cipher wheel.
CW3—Third cipher wheel.
CW4—Fourth cipher wheel.
CW5—Fifth cipher wheel.
E-D—Encipher-decipher set screw.
SET—Bench mark upon which the letters of LAW, the cipher wheels, and RAW are aligned in setting them according to the "key."
BS1—Bakelite separator between LAW and CW1.
BS2—Bakelite separator between CW1 and CW2.
BS3—Bakelite separator between CW2 and CW3.
BS4—Bakelite separator between CW3 and CW4.
BS5—Bakelite separator between CW4 and CW5.
BS6—Bakelite separator between CW5 and RAW

6. **Enciphering a dispatch.**—To encipher a dispatch, the large knurled screw (E-D, plate 1a) at the right and towards the rear of the machine, is revolved so as to bring the indicator (on the top rear plate) to the left, to the position marked DIRECT. LAW, CW1 to 5, and RAW are then revolved so as to align the letters of a KEY WORD upon the white bench mark or setting line, SET, at the front of the machine, the letters of the key word being set up in the usual direction of reading, viz., from left to right. The keys of the keyboard corresponding to the successive letters of the plain-text dispatch are depressed and the cipher letters that are indicated by being illuminated on the lightboard are written down. It will be noted that in the course of enciphering certain of the wheels become displaced from their original positions. These movements will be discussed subsequently in full detail.

7. **Deciphering a dispatch.**—To decipher a dispatch, the enciphering-deciphering set screw is revolved so as to bring the indicator to the position marked REVERSE. Then the letters of the key word, which must of course be known in advance, are aligned upon SET, and the keys of the keyboard corresponding to the successive cipher letters are depressed, whereupon

their equivalent plain-text letters will be illuminated on the lightboard. It is to be stated that while the normal method of encipherment and decipherment is with the indicator set at DIRECT and REVERSE, respectively, this is not absolutely essential. The machine will encipher and decipher just as well with the opposite arrangement, i.e., set to REVERSE for encipherment and to DIRECT for decipherment, but the correspondents must, of course, be in agreement in this respect.

8. **Construction of cipher wheels.**—Plate 1b shows one of the cipher wheels, which are all similar in construction. The rim of the wheel is divided up into 26 equal sections, hereafter designated as cipher-wheel segments, which are labeled by means of the normal alphabet, Z being replaced by a number for the purpose of identifying each wheel. The letters identifying the aforementioned segments are set in rectangular depressions or recesses into which a lever may fall and thus cause the wheel to be displaced one step at a time. Each peripherally lettered cipher-wheel segment has two electrical contact surfaces on the sides or faces of the wheel, one on the left, hereafter designated as the left-hand contact, abbreviated as LHC, and one on the right, similarly designated as the right-hand contact, abbreviated as RHC. Each LHC is provided with a binding post on the left face of the wheel, and each RHC with a binding post on the right face. An insulated conductor connected to the binding post of the LHC of every cipher-wheel segment goes through a hole in the center plate of the wheel, and is connected to the binding post of the RHC of some other segment on the same wheel. Thus, for example, on CW1 the LHC of A is connected to the RHC of G; the LHC of E is connected to the RHC of O; the LHC of K is connected to the RHC of Z, as may be shown diagrammatically thus:



The series of LHCs of all the segments are connected to the series of RHCs in an arbitrary mixed order. The set of connections established in this manner is different in each cipher wheel. These cipher wheels, therefore, act merely in the capacity of different mixed alphabets, which may be indicated diagrammatically in the alphabets below.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ } Alphabet 1.
BDFCWPAOMSHXVIEUQZYGJTNLRKBDFCWPAOMSHXVIEUQZYGJTNLRK }

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ } Alphabet 2.
WYDHKPUQAJFOTCMIVZSEGLNRXBWYDHKPUQAJFOTCMIVZSEGLNRXB }

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ } Alphabet 3.
HLSZVDJNXBTFMRPAWOUGIQECKYHLSZVDJNXBTFMRPAWOUGIQECKY }

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ } Alphabet 4.
DKHXWAFYORVBIMPTJEUQSCGLNZDKHXWAFYORVBIMPTJEUQSCGLNZ }

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ } Alphabet 5.
FRISYADPLJUXZGKOBTWCVMHEQNFRISYADPLJUXZGKOBTWCVMHEQN }
```

In the case of the alphabet applying to each cipher wheel, it is to be understood from what has preceded, that a wire not shown in the diagrammatic representation actually connects each letter in the upper sequence of letters to the same letter in the lower sequence. Thus, for example, Alphabet 1 shows that a current entering CW1 at the LHC of A leaves CW1 at the RHC of G; in other words, a current corresponding to the letter A becomes converted into one

Plate 1b (To face page 4)

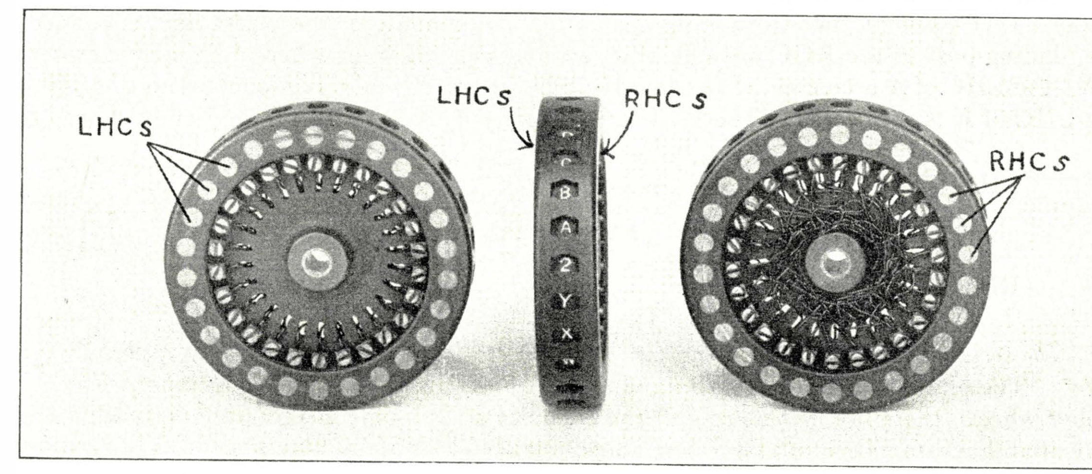
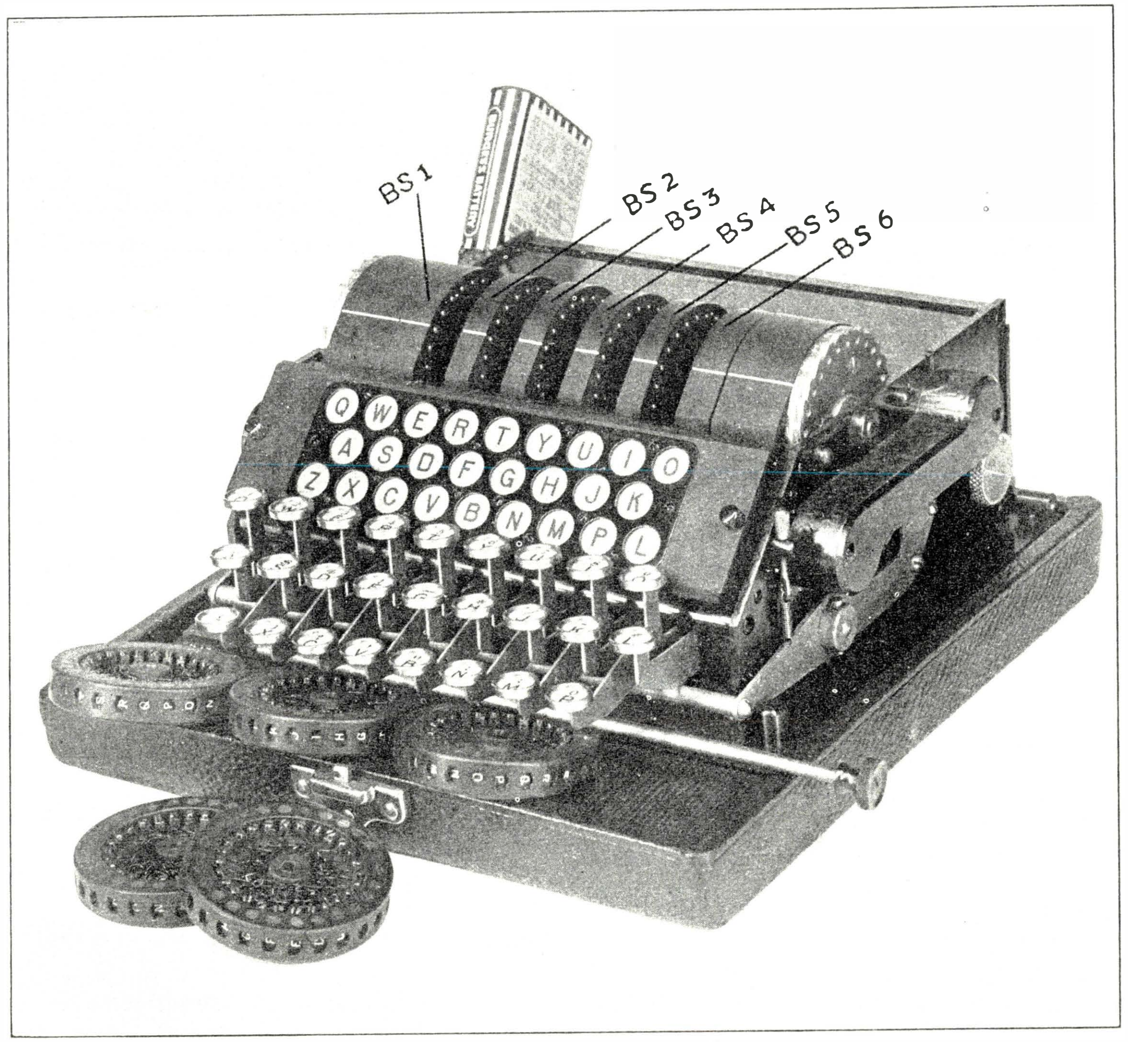


Plate 1c (To face p. 5.)



corresponding to the letter G. The upper sequence of letters in each cipher alphabet, because it coincides with the normal or standard alphabet, will be referred to hereafter as the *normal component;* the lower sequence in each alphabet, as the *mixed component.* The normal component, therefore, corresponds to and indicates the sequence of LHCs; the mixed component corresponds to the sequence of RHCs and indicates the point from which a current entering a LHC will emerge on the right hand side of the cipher wheel. For purposes of abbreviation, an alphabet will hereafter be designated by the letters AL followed by a number. Thus, AL1 refers to Alphabet 1. The normal component of AL1 will be designated by the abbreviation NAL1; the mixed component, by MAL1. Corresponding abbreviations will apply in the case of the other alphabets.

9. **Function of bakelite separators.**—Four circles of 26 fixed, spring-contacts, which are in the bakelite separators designated as BS2 to BS5 in Plate 1c, and which can only be seen by removing the cipher wheels, serve to form fixed paths for conducting the current from a cipher wheel into its adjacent one on the left or right. These contacts are not subject to change, the current merely being carried directly across the bakelite disk. For example, with CW1 and CW2 both set at A, a current which emerges from CW1 at the RHC of segment A will enter CW2 at the LHC of segment A; or in the reverse manner, a current which emerges from CW2 at the LHC of A will enter CW1 at the RHC of A.

10. **The left and right sequences.**—When the machine is set for DIRECT operation, the bakelite separators BS1 and BS6 contain the sets of contacts connected to the keyboard and lightboard contacts, respectively. *The connections are not made directly, but through the intermediacy of a bakelite switching plate in the rear of the machine.* The function of this plate and the nature of the connections there established will be described later (Section XIV). Suffice it to indicate at this point that the connections are established in such a manner as to produce the equivalents of two mixed alphabets corresponding to the sequences of the contacts in BS1 and BS6. For example, with the indicator set at DIRECT, starting with the first contact point of BS1 on a line with SET, this contact point is connected to the key "B" of the keyboard, and the homologous one in BS6 is connected to the lamp illuminating the letter "T". The next one, proceeding toward the rear of the machine is connected to the "S" of the keyboard, and "Y" of the lightboard, and so on, according to the following sequences, hereafter designated as the *left fixed sequence,* LFS, and the *right fixed sequence,* RFS, respectively:

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

With the indicator set for DIRECT operation the keyboard contacts lead to the contacts in BS1 (after passing through the rear plate mentioned above), and therefore LFS is applicable to them, the lightboard lamps are connected to BS6 (after passing through the rear plate), and there RFS is applicable. But with the indicator set for REVERSE operation, the sets of connections are reversed, the keyboard connections being through RFS, and the lightboard connections through LFS.

11. **Horizontal permutations of the cipher wheels.**—The cipher wheels being identical so far as their physical construction is concerned, they are all interchangeable, and any wheel can be inserted in any of the five positions on the shaft. There may be any number of cipher wheels from which a selection of five different ones can be made. Having selected a set of five cipher wheels to be used, since each one of them can occupy the first, second, third, fourth, or fifth position, the number of different arrangements or permutations of the cipher wheels themselves, as regards their relative order upon the shaft from left to right, hereafter termed the *horizontal permutations of the cipher wheels,* is $5 \times 4 \times 3 \times 2 \times 1$, or 120.

But the cipher wheels may also be mounted upon the shaft in an "upside down" position, that is, so that what were previously the RHCs now become the LHC's, and vice versa; this procedure, as will appear subsequently, yields an entirely new series of equivalents. Thus, each cipher wheel may be regarded as being the equivalent of two wheels. Therefore the five cipher wheels really amount to 5×2, or ten wheels. Now there are five positions in which wheels can be inserted either right side up or upside down. The first insertion can be made in any one of the five positions, 1, 2, 3, 4, or 5. There being ten wheels, for the first insertion there are ten possibilities. Having inserted one cipher wheel in position there are four positions left, and any one of eight wheels can be inserted, yielding eight possibilities. The third insertion yields six possibilities, the fourth, four, and the fifth, two possibilities. Therefore, the total number of possible horizontal permutations of the five cipher wheels themselves, as regards their relative order upon the shaft, is $10\times8\times6\times4\times2$, or 3,840. If there were more wheels available, from which a set of five were to be selected, the number of permutations on the shaft would be still greater, according to the formula

$$N=2n\times2(n-1)\times2(n-2)\times2(n-3)\times2(n-4),$$

where N is the total number of horizontal permutations, and n is the total number of cipher wheels from which a set of five can be selected.

Each one of these permutations or horizontal arrangements of the cipher wheels upon the shaft will yield different results in encipherment so that, for purposes of communication, it becomes absolutely essential to know exactly which horizontal permutation is in effect at any given moment.

12. **Rotatory permutations of the cipher wheels.**—When mounted upon the shaft, each cipher wheel is susceptible of being placed in any one of 26 different positions relative to the letter of its periphery which is aligned on the bench mark or setting line, SET. When two cipher wheels are inserted, they are susceptible of being placed in any one of 26×26, or 676 different positions relative to the pair of letters which are aligned on SET. When all five wheels are inserted, they are susceptible of being placed in any one of 26^5, or 11,881,376 different positions relative to the set of five letters which are aligned on SET. Each different alignment of the five cipher wheels from left to right on the shaft will hereafter be referred to as one of the *rotatory permutations of the cipher wheels*. It is obvious that for every one of the rotatory permutations the complete electrical path established for the passage of an electrical current from a given contact of BS1, through the cipher wheels and to a given contact of BS6 is different, *considered as a whole*. That is, the five cipher wheels provide a total of 11,881,376 different complete paths for the progress of the current from each contact of BS1 through the five cipher wheels into a contact of BS6. Since there are 26 contacts in BS1, one for each letter of the alphabet, it follows that for any given rotatory permutation of the cipher wheels there exists a different, or unique, secondary cipher alphabet; and since there are 11,881,376 different rotatory permutations, it follows that there are that many secondary cipher alphabets for each horizontal permutation of the cipher wheels. This will be discussed more in detail in the succeeding paragraphs of this section.

13. **Permutations of LAW and RAW.**—These two aluminum wheels, which are not concerned directly in the electrical relations, but are vitally concerned in the mechanical relations, can also assume different rotatory positions upon the shaft. Since there are but two wheels, and they are not interchangeable, there are only 26^2, or 676 different rotatory permutations of the pair of them, designated by the 676 permutations of the letters of the alphabet, taken in pairs. These designations form a part of the key word, the first and last letters of the word being used to determine the initial positions of LAW and RAW, respectively. Considered collectively, or as a unit, the particular horizontal and rotatory permutation of the cipher wheels, and the particular rotatory permutation of LAW and RAW in effect during the encipherment

of a letter of the plain text, or the decipherment of a letter of the cipher text, constitute the "*key*", in the cryptographic sense of the term.

14. **Functions of LAW and RAW; automatic displacement of the cipher wheels.**—These two wheels are the principal agents in controlling the automatic displacements or motions of two of the cipher wheels, viz., CW1, and CW3. RAW controls CW1, and LAW, CW3. The principal feature of this control, so far as this analysis is concerned is explained in connection with the accompanying sketch, fig. 1.

Depression of any key causes a universal bar, UB, to rotate a rocker shaft 1, attached to which are four levers or wheel-stepping "dogs." Dog 2, the lower end of which falls into one of the 26 small notches on the right hand side of RAW, serves to move RAW one step forward per

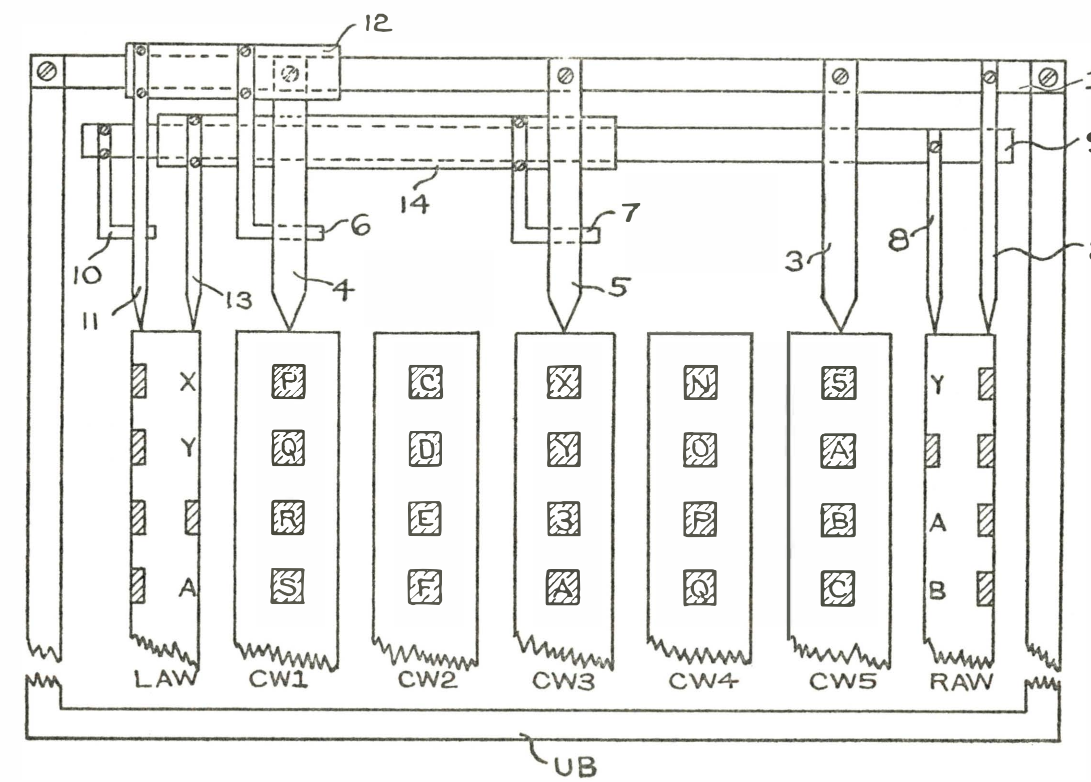


FIGURE 1.—Diagram of mechanical action on cipher wheels, LAW and RAW.

depression of any key; another dog, 3, does the same thing with respect to CW5. Since CW5 and RAW can be advanced only 26 times in making one complete revolution, their period, in terms of letters is 26. Dogs 4 and 5, also attached to shaft 1 cannot move CW1 and CW3 because the arms 6 and 7 are so placed as to prevent the ends of these two dogs from falling into the recesses of CW1 and CW3.

Now when trip dog 8 falls into the single large notch on the left hand side of RAW (at letter Z on this wheel, and when N is at SET) shaft 9 is caused to rock. At the other end of shaft 9 there is a release arm 10, which allows dog 11 to drop into one of the 26 small notches on the left hand side of LAW. Dog 11 is attached to a sleeve 12, which swings freely on shaft 1. At the other end of sleeve 12, release arm 6, mentioned above, moves when dog 11 drops into a notch on LAW. When arm 6 moves it allows dog 4 to drop into one of the recesses on CW1, and the next depression of a key causes both LAW and CW1 to advance one step. Since dog 8 falls into the

Z notch of RAW but once per revolution, i.e., once per 26 letters, and since release arm 10 thus allows dog 11 to fall into one of the notches of LAW but once per 26 letters, the period of LAW is 26×26 or 676 letters. Likewise, the period of CW1 is 676 letters.

Now dog 13 drops into the single large notch at Z on the right hand side of LAW only once per revolution of LAW. This dog 13, is attached to a sleeve 14 on shaft 9, and is free to swing on the shaft. At the other end of sleeve 14, arm 7, which normally prevents dog 5 from dropping into a recess on CW3, is withdrawn and allows dog 5 to drop whenever dog 13 drops. This happens but once in 676 letters, and thus CW3 is advanced one step per 676 depressions. The period of CW3 is therefore 676×26 or 17,576 letters.

In a previous model of the machine CW4 and CW5 were caused to advance by a similar arrangement of dogs and release arms. This, however, was thought unnecessary by the manufacturers, and in the model studied these two wheels could only be advanced manually.

It will be convenient to designate the letter N as the starting point of a revolution or complete period of LAW and RAW, and the letter O, as the finishing point, because the displacements of CW1 and CW3 occur when N is at SET and a key is just then being depressed.

The displacement relations of the wheels may be summarized as follows:

(1) CW5 and RAW are displaced one interval per depression of any key. Their period is 26 letters.

(2) CW1 and LAW are displaced one interval per one complete revolution or period of RAW. The periods of CW1 and LAW are therefore 676 letters.

(3) CW3 is displaced one interval per one complete revolution or period of LAW, and hence its period is 17,576 letters. CW2 and CW4 do not undergo automatic displacement and unless moved by hand remain fixed in their positions.

The length of the period produced by automatic displacement of the cipher wheels is 17,576 letters, but by displacing CW2 and CW4 by hand, the length of the period can be increased to 17,576×676, or 11,881,376 letters. That is, if each correspondent used a different permutation of CW2 and CW4, then there is possible a series of 676 different periods, each of 17,576 letters, and a total of 11,881,376 letters could be enciphered without repetition of cipher alphabets.

15. **Potentialities of the machine.**—It is absolutely essential for a full understanding of the subsequent analysis that a clear conception be had of the really staggering number of possible permutations and combinations afforded by the machine, and this can best be set forth in terms of the number of different paths that are available for an electric current to take in the process of encipherment of a single letter.

The exact path traversed is determined by a particular combination of the following six factors:

(1) The plain-text letter that is being enciphered.

(2) The position in the left fixed sequence, LFS, that is determined by the keyboard contact of the plain-text letter that is being enciphered.

(3) The position in the right fixed sequence, RFS, that is determined by the lightboard contact of the cipher letter that is to result from the encipherment.

(4) The setting of the machine with respect to the direct and reverse method of operation.

(5) The horizontal permutation of the cipher wheels that is in effect during the encipherment of the letter.

(6) The rotatory permutation of the cipher wheels that is in effect during the encipherment of the letter.

Consider now what happens when any key of the keyboard is depressed. A connection is established from the battery, through the contacts of the depressed key, through the rear plate (see paragraph 10), to some contact in the LFS, from which it emerges at some contact in BS1.

This current can enter CW1 through any one of its 26 LHC's, depending upon the rotatory position of CW1. Now having entered CW1 through a certain one of its 26 LHC's, the current will leave this cipher wheel through a certain one of its 26 RHC's, the particular one being determined only by the internal wiring of CW1 as explained in paragraph 8. But so far as any given letter of CW1 is concerned, the path followed by a current which has entered a given LHC is always the same on that cipher wheel, so long as the wiring is unchanged in the wheel. On leaving CW1 the current is carried directly across BS2 and enters one of the 26 LHC's of CW2, the particular one being determined by the rotatory position of CW2 as regards the SET line. Since CW2 is capable of 26 rotatory positions, a current entering a LHC of CW1 may traverse any one of 26×26 or 676 paths in finding its exit at a RHC of CW2. Continuing in a similar manner, when all five CW's are considered, a current entering a LHC of CW1 may traverse any one of 26^5, or 11,881,376 paths in finding its exit at a RHC of CW5, the particular complete path it actually takes being determined by a fixed set of conditions as governed by the rotatory permutation of the five wheels as they are mounted according to a given horizontal permutation upon the shaft. Now assuming that the five cipher wheels were caused to be displaced in such a manner as to present successively to the SET line every one of the possible 11,881,376 rotatory permutations, it will follow that, given an initial setting of the five wheels the particular permutation of the five separate paths composing the complete path traversed by a current caused by the first depression of a single key cannot be exactly the same for the succeeding 11,881,375 depressions of the same key, but will be the same for the 11,881,376th depression after the first.

Now it was shown above that there are 3,840 horizontal arrangements of five cipher wheels, and since each one of them can yield 11,881,376 rotatory permutations, the total number of paths which a single set of five cipher wheels can provide is 3,840×11,881,376, or 45,624,483,840. Furthermore, since the machine, when the indicator is set to REVERSE, will function just as efficiently for enciphering purposes as it will when it is set to DIRECT (see paragraph 7), and since in the former case the cipher equivalents are altogether different from what they are in the latter case, a second series of 45,624,483,840 paths is possible. That is, the cipher equivalent for a given letter may be the result of the traversing of a current of electricity over any one of over 91 billion different circuits from a key of the keyboard to a lamp of the lightboard, as provided by this small machine with but five cipher wheels.

The final cipher equivalent, however, in any case is expressible as, and can be but one of, 26 characters. Hence there will obviously be a myriad of repetitions of cipher letters brought about by this truly staggering number of different paths, but the order of repetition will be in an apparently absolutely random manner, though of course the exact order can be causatively determined by a very detailed study of the wiring of each wheel, and the permutations of the wheels. What has been said with respect to the results of depressing one key applies, of course, to all the keys, so that it may be said that the enormous total of over 91 billion secondary cipher alphabets are involved in this system. Another way of stating the case is this: By utilizing all the possibilities of one set of cipher wheels on one machine it would be possible to encipher a series of dispatches consisting of over 91 billion letters before encipherment by an identical sequence of alphabets would begin, and thus produce two or more messages in the same "key."

For reasons which will become apparent subsequently, this analysis will for the present be restricted to that method of using the machine in which the only variable factor concerned in the keys for a set of dispatches is that involving changes in the initial rotatory permutation for each dispatch. It will be assumed (1) that this initial permutation is to be given as the first word in the text of each dispatch; (2) that the machines are to be set at DIRECT for encipherment and at REVERSE for decipherment; and (3) that no change is made in the horizontal permutation of the cipher wheels during the course of the encipherment of the set of dispatches to be subjected to analysis.

SECTION III

BASIC CRYPTOGRAPHIC PRINCIPLES OF OPERATION

16. **Cipher relations.**—Having described the mechanics of the machine, and the manner in which the depression of a key of the keyboard causes a circuit to be established which results in the illumination of a lamp of the lightboard, the cryptographic principles of the system will now be examined more in detail.

The best way to do this is first to determine exactly how a letter is enciphered (from the cryptographic standpoint, not the mechanico-electrical); then determine what, if any, are the relations between successive encipherments of the same letter; and finally, determine what, if any, are the relations between encipherments of dissimilar letters. A set of sliding strips coinciding with the alphabets of the machine will be used for this purpose and it is recommended that the reader provide himself with a duplicate of the set of strips given below. These are arranged in the form of horizontal sliding alphabets, rather than vertical, merely for convenience in illustration.

```
SET
↓
BSXRZTKDNGCHMVOLYQEUPWJAIF.............................. { Left fixed sequence.

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
BDFCWPAOMSHXVIEUQZYGJTNLRKBDFCWPAOMSHXVIEUQZYGJTNLRK } Alphabet 1.

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
WYDHKPUQAJFOTCMIVZSEGLNRXBWYDHKPUQAJFOTCMIVZSEGLNRXB } Alphabet 2.

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
HLSZVDJNXBTFMRPAWOUGIQECKYHLSZVDJNXBTFMRPAWOUGIQECKY } Alphabet 3.

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
DKHXWAFYORVBIMPTJEUQSCGLNZDKHXWAFYORVBIMPTJEUQSCGLNZ } Alphabet 4.

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
FRISYADPLJUXZGKOBTWCVMHEQNFRISYADPLJUXZGKOBTWCVMHEQN } Alphabet 5.

TYOEUMXDFJQVKWBNSHCILRZAGP.............................. { Right fixed sequence.
↑
SET
```

These strips are to be arranged so that the left and right fixed sequences are held in place by thumb tacks on a drawing board, and between these two strips the cipher alphabets should slide freely. The arrow coincides with the setting line SET, and it will be noted that the first letter of the left fixed sequence is directly over the first letter of the right fixed sequence. By using

these strips it is possible to duplicate the results of the machine in every detail. Instead of the mere depression of a key that closes a circuit from the positive pole of battery, through a keyboard contact, a contact in BS1, a path established by the cipher wheels, a contact in BS6, a lamp, and thence to the negative pole of the battery, the mind of the cryptanalyst must perform an equivalent function through the agency of the strips of alphabets; and whereas the electric current traverses the path through the machine with unerring accuracy at the rate of 186,000 miles per second, the mind can do so only at an almost infinitely slower rate of speed, and at the ever present risk of inaccuracy.

Set the machine [1] to the following keyword:

Wheels	LAW	CW1	CW2	CW3	CW4	CW5	RAW
Setting	S	I	G	N	A	L	S

and depress A on the keyboard. The cipher resultant, as illuminated on the lightboard, is P, or $A_p = P_c$. It will be noted that the circuit is not established until *after* the wheels CW5 and RAW have been advanced by the depression of the key to their next positions. In other words, the setting by means of which a letter is enciphered is shown only *after* the encipherment has been effected. This is very important to keep in mind. In the case just noted, with the setting SIGNALS, the actual setting at which encipherment was effected is SIGNAMT, in which it will be noted that CW5 and RAW have advanced one step. Hence, hereafter, that setting of the wheels which governs the actual path taken by the current during the encipherment of a letter will be termed the *effective setting*, and will be the one immediately following the *apparent* or *keyword setting*.

In setting up the wheels to a keyword, it is obvious that the setting letters on the cipher wheels correspond only to the LHC designations, and not to the RHC designations of the wheels, because the sequence of letters on the periphery of each cipher wheel is the normal alphabet sequence. The RHC designations are all in a random or mixed order. This point is to be remembered in setting the sliding strips to a keyword, as explained in the next paragraph.

17. **Use of sliding alphabets in tracing electrical paths traversed in encipherment.**—The identical result will now be found by means of the sliding strips. First, it is necessary to set the strips in relative positions corresponding to the relative positions of the cipher wheels, viz., in the order LFS–AL1–AL2–AL3–AL4–AL5–RFS, and these must be juxtaposed relative to their points of coincidence so as to correspond to the keyword, read upon their normal components. Although the wheels LAW and RAW do not enter into the electrical relations, and may be disregarded in tracing actual paths through the sliding strips, they must, nevertheless, be kept in mind constantly, as will be discussed later in connection with the displacement of AL1 and AL3. Now since the second letter of the keyword is the one that governs the position of CW1, and since this letter in the case of the keyword SIGNALS is I, therefore AL1 is set so that I of its normal component is under the setting arrow; similarly AL2 is set so that G of its normal component is under the setting arrow; AL3 is set so that N of its normal component is under the setting arrow; AL4 is set so that A of its normal component is under the setting arrow; and

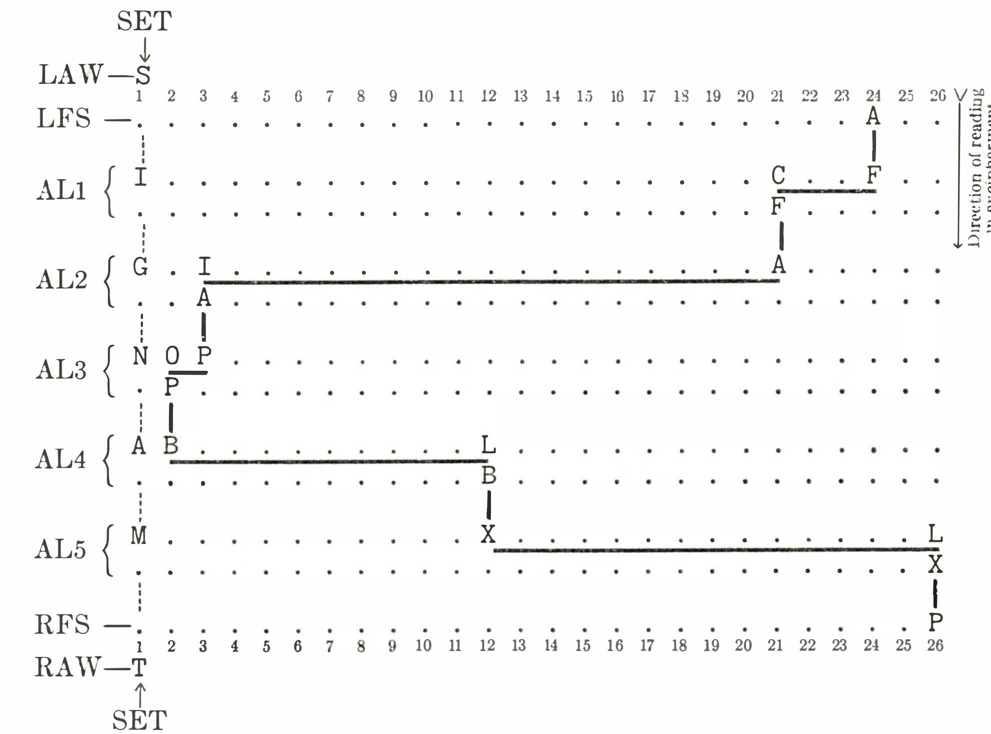
[1] It will be assumed that the reader is provided with one of the machines, and that the wiring corresponds to that indicated in the preceding pages. As stated above, actual possession of a machine is not absolutely essential, inasmuch as every function of the machine can be duplicated by employing a set of sliding alphabets.

AL5 is set so that M of its normal component (to correspond with the effective setting SIGNAMT) is under the setting arrow. All of these settings are as indicated in the following diagram:

```
               SET
                ↓
                STUVWXYZABCDEFGHIJKLMNOPQR       LAW
                BSXRZTKDNGCHMVOLYQEUPWJAIF       LFS

        ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGH... } AL1
        BDFCWPAOMSHXVIEUQZYGJTNLRKBDFCWPAO... }

          ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF... } AL2
          WYDHKPUQAJFOTCMIVZSEGLNRXBWYDHKP... }

   ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLM... } AL3
   HLSZVDJNXBTFMRPAWOUGIQECKYHLSZVDJNXBTFM... }

                ABCDEFGHIJKLMNOPQRSTUVWXYZ... } AL4
                DKHXWAFYORVBIMPTJEUQSCGLNZ... }

    ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKL... } AL5
    FRISYADPLJUXZGKOBTWCVMHEQNFRISYADPLJUX... }

                TYOEUMXDFJQVKWBNSHCILRZAGP       RFS
                TUVWXYZABCDEFGHIJKLMNOPQRS       RAW
                ↑
               SET
```

The strips are now ready to serve as guides in encipherment. In employing the machine itself, it was found that with the keyword given, A_p was enciphered as P_c. Refer now to the sliding strips. Find A in LFS; it is the 24th letter of the sequence and is directly over F of NAL1. Imagine a wire connecting the F of NAL1 (which, it will be recalled, represents the set of LHC's of CW1) to the F of MAL1. It will be found that F of MAL1 is directly under C of NAL1; that is, the current originating at A of LFS, entering CW1 at the LHC of F, emerges from CW1 at the RHC of C. As shown in the diagram of alphabets above, C of NAL1 is now opposite A of NAL2. Imagine a wire connecting A of NAL2 to A of MAL2. The latter will be found under I of NAL2 (that is, the RHC of I of CW2), and I is now opposite P of NAL3. Continuing in a similar manner to trace the path taken by the current through CW3, 4, and 5, by means of the corresponding alphabets AL3, 4, and 5, it will be found that the current emerges from CW5 at the RHC of L, which is opposite P of RFS. Hence, with the

effective setting given, $A_p = P_c$. The entire sequence of sub-paths taken by the current may be represented graphically, as shown below:



Upon depressing the next key, CW5 advances one step to the next effective setting before completion of the enciphering circuit, and therefore, AL5 must be correspondingly advanced. But in which direction, to the left, or to the right? It will be seen that in the machine itself the movement of the wheel is opposite in direction to that followed by the letters on the periphery of the wheel.[1] Hence, since NAL5 is the normal or straight alphabet, proceeding from left to

[1] It will constantly be kept in mind that the assumption made regarding the cipher wheels is that they are in the "right-side-up" position. Only a slight modification in analysis is necessary in the case where they are in an "upside-down" position.

right, to make the change in position of the sliding strip correspond with the change in position of the wheel, the strip must be advanced one space *to the left*, to the position indicated below:

```
                    SET
                     ↓
                     BSXRZTKDNGCHMVOLYQEUPWJAIF          LFS
                     :
           ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGH...}  AL1
           BDFCWPAOMSHXVIEUQZYGJTNLRKBDFCWPAO...}
                     :
             ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF...}  AL2
             WYDHKPUQAJFOTCMIVZSEGLNRXBWYDHKP...}
                     :
       ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLM...}  AL3
       HLSZVDJNXBTFMRPAWOUGIQECKYHLSZVDJNXBTFM...}
                     :
                     ABCDEFGHIJKLMNOPQRSTUVWXYZ...}  AL4
                     DKHXWAFYORVBIMPTJEUQSCGLNZ...}
                     :
       ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLM...}  AL5
       FRISYADPLJUXZGKOBTWCVMHEQNFRISYADPLJUXZ...}
       ←Direction    :
        of motion    :
                     TYOEUMXDFJQVKWBNSHCILRZAGP          RFS
                     ↑
                    SET
```

Suppose the second letter to be enciphered is R. A condensed graphic representation of its encipherment is as follows:

$$\underset{LFS}{R_p} \Rightarrow \overbrace{L_1 \rightarrow L_2}^{AL1} \Rightarrow \overbrace{V_1 \rightarrow V_2}^{AL2} \Rightarrow \overbrace{X_1 \rightarrow X_2}^{AL3} \Rightarrow \overbrace{V_1 \rightarrow V_2}^{AL4} \Rightarrow \overbrace{X_1 \rightarrow X_2}^{AL5} \Rightarrow \underset{RFS}{G_c}$$

In the foregoing graphic representation L_1 stands for the letter L in the upper or normal component, and L_2 for the same letter in the lower or mixed component of Alphabet 1. The same designating characters also apply to the other letters in the diagram.

If the next letter to be enciphered were E_p, the graphic representation would be as follows:

$$\underset{LFS}{E_p} \Rightarrow \overbrace{A_1 \rightarrow A_2}^{AL1} \Rightarrow \overbrace{E_1 \rightarrow E_2}^{AL2} \Rightarrow \overbrace{A_1 \rightarrow A_2}^{AL3} \Rightarrow \overbrace{C_1 \rightarrow C_2}^{AL4} \Rightarrow \overbrace{J_1 \rightarrow J_2}^{AL5} \Rightarrow \underset{RFS}{R_c}$$

This process is continued for the succeeding letters in a similar manner, AL5 being slid to the left one space for each letter. No shifting of CW1, 2, 3, or 4 will occur until N of RAW reaches the SET line, whereupon, as explained in paragraph 14, section II, with the next depression, CW1 as well as CW5 (also LAW and RAW) will be advanced one space. In this case since the first letter of the dispatch is enciphered with T of RAW at SET (Key: SIGNALS, effective setting = SIGNAMT), then N will be reached with the encipherment of the 21st letter (T to N, inclusive, in the normal alphabet equals 21 intervals). With the encipherment of the 22d letter, therefore, CW1 and CW5 will both be advanced one space each, and therefore AL1 and AL5 in the equivalent sliding strips must be advanced one space to the left to correspond with the displacement of CW1 and CW5.

The process of finding cipher equivalents is now the same as before. No second shifting of CW1 must be accounted for on the strips until the 22 + 26 = 48th letter of the dispatch

is to be enciphered, for once more (with the encipherment of the 47th letter) N of RAW will have reached SET and CW1 will be advanced one space. This process of shifting AL1 to make it correspond with the successive displacements of CW1 is continued in like manner until the letter N of LAW reaches SET, which will be the 22 + (26×20) = 542d letter (T to N, including T but not N, on LAW = 20 intervals). The 542d letter will bring LAW to N and CW1 to D. The 543d letter will cause CW3 to advance one space, whereupon sliding AL3 must be shifted one space to the left correspondingly.

It may be advisable to make an actual outline of the positions into which the successive letters fall, and the successive displacements to which the various wheels are subject during the course of the encipherment of a dispatch of say 600 letters, with the keyword SIGNALS. It is recommended that the reader examine the following diagram very carefully. The numbers refer to the successive letters of the dispatch. At the top, the effective enciphering positions of CW5 and RAW are given; at the left, those of LAW, CW1, and CW3 are given.

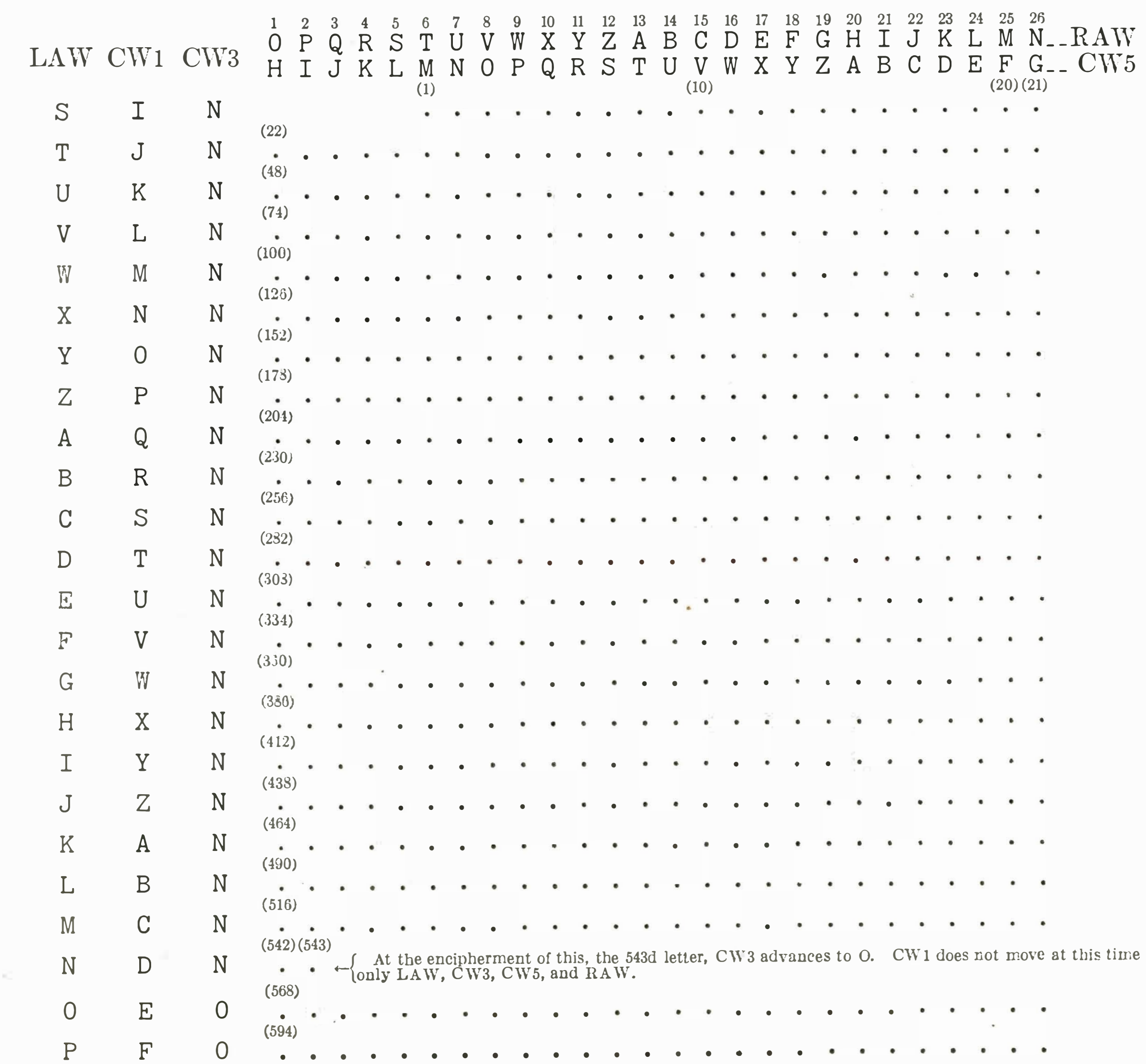
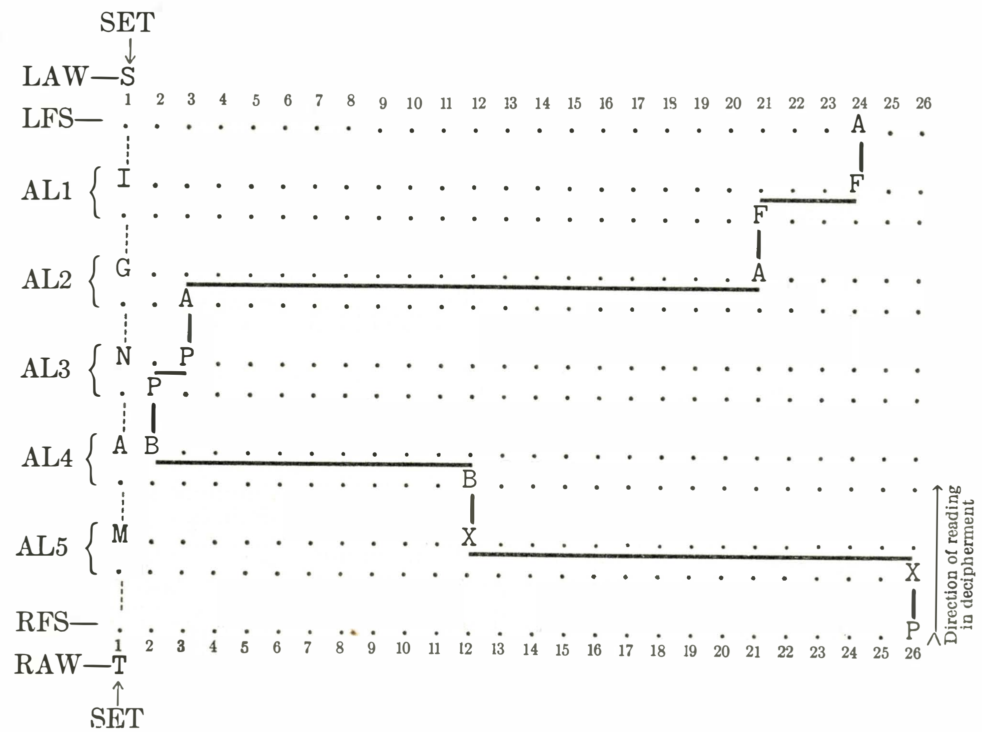


FIGURE 2.

18. **Enciphering an example.**—It is necessary that this chain of reasoning be noted very carefully, for in the subsequent analysis these factors must be considered in great detail. As practice in the procedure let the reader first encipher the following message, by means of the sliding strips and the keyword MEANING, and then check it back by deciphering it:

AMMUNITION EXHAUSTED [1]

19. **Deciphering by means of sliding alphabets.**—In decipherment by means of the sliding alphabets, the only difference in method is that now the analyst must proceed in the reverse direction in tracing paths, beginning with the cipher letter in RFS, progressing upward through the five alphabets, and emerging at LFS. Each letter must first be located in the lower half or mixed component of each alphabet, carried to the upper halves or normal components, and so on. Thus, to trace back the equivalents $A_p = P_c$ found with the initial setting SIGNALS, the steps are graphically illustrated as follows:



[1] The correct encipherment is: ONZOV HLDGN XBVPW YMRN.

SECTION IV

ANALYSIS BASED ONLY UPON A KNOWLEDGE OF THE MECHANICS OF THE MACHINE

20. **Introductory remarks.**—First, the method of analysis when only a knowledge of the mechanics of the machine is available will be presented. Then, the method of analysis when LFS and RFS are known will be presented. The reason for the treatment in this manner will appear subsequently.

21. **Alphabets employed in demonstration.**—In demonstrating the principles of analysis, use will be made of the alphabets given in paragraph 16, section III. From the workings of known alphabets, certain principles will be deduced. From these deductions, inductive reasoning will lead to the establishment of other principles, by means of which unknown alphabets may be reconstructed. This, in general, is always the method of the cryptanalyst engaged in studying a complex system of cryptography.

22. **Fundamental principle.**—Consider the simplest case of all, viz, the successive encipherment of one letter 26 times, beginning with Z of CW5 at SET (so that A will be the effective setting on CW5) and with no displacement of the other cipher wheels occurring during the 26 successive encipherments. It follows from what has gone before that the electrical impulses originating in LFS will trace exactly the same path through CW1, 2, 3, and 4 every one of the 26 times, and will emerge from CW4 at one and only one of its RHCs every time, thus always entering CW5 from a fixed or constant point in BS5. *The different cipher equivalents which will be produced for the 26 successive encipherments will therefore all be due solely to the successive displacements of CW5.* For example, consider the successive encipherments of A_p with the initial effective setting of the wheels given as OAAAAAO. Tracing the encipherments, or operating the keyboard of the machine, the first equivalent of A_p will be Y_c; the second one, O_c; the third one N_c, and so on, yielding the following sequence:

```
1       5         10        15        20        25
Y O N D S W M A U Z X F L Q K G X V H R B T E C J P
```

If the encipherment has been accomplished by means of the sliding strips, it will be observed that in every one of the foregoing 26 encipherments the current emerges from E of MAL4, and enters the successive letters of NAL5 from a point which may best be referred to as the eighteenth contact of BS5. Now note the following very carefully, for it involves the essence of this whole analysis:

(1) No matter what the rotatory permutation of CW1, 2, 3, and 4 may be;

(2) No matter what plain-text letter is being enciphered 26 consecutive times, designate it by the symbol θ_p;

(3) Providing no displacement of CW1, 2, 3, or 4 occurs during the 26 successive encipherments;

(4) If the current enters CW5 from the eighteenth contact of BS5 and
(5) If A of NAL5 is at the SET line, the series of cipher equivalents for the 26 consecutive encipherments of θ_p will be the sequence

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

To repeat, it makes absolutely no difference what the rotatory permutation of the first four cipher wheels may be, if the other conditions set forth above hold true, the 26 successive cipher equivalents of θ_p will coincide with the sequence YOND. . . . The latter may be regarded as absolutely fixed for the given CW5. For example, set up the following permutation of the wheels: KTHWKZN, which may be regarded as being a random one; depress the universal bar so as to advance CW5 to A, and CW1 to the next position so as to provide for a complete sequence of 26 encipherments; hold the universal bar down with the left hand; and then with a finger of the right hand find that key which will cause Y to be illuminated on the lightboard. It will be found that F_p will produce Y. Now release the universal bar and depress F successively 25 more times. The sequence of equivalents will be YOND. . . . Both of the procedures in establishing the preceding sequence started with CW5 at an initial point, which for convenience was selected as A. But if the sequence is started with some setting other than A, the only difference is that the initial letter of the sequence is no longer Y, but some other letter of the *same sequence:* invariably, there will be produced this same YOND. . . sequence. For example, with the setting QWKANFN, depressing K_p successively yields the following sequence:

```
      10        15          20                  1       5
M A U Z X F L Q K G X V H R B T E C J P Y O N D S W
```

which, it will be noted, is exactly the same as the YOND. . . sequence given above, but with a different initial point. In other words, the YOND. . . sequence may be regarded as being in the nature of a *cycle,* which can be initiated at any point. For convenience, therefore, this cycle of letters, no matter what its initial point is, will be called the YOND. . . sequence.

There are 26^4 or 456,976 rotatory permutations of CW1, 2, 3, and 4. For every single one of them there will be a certain key of the keyboard, depression of which will produce the YOND. . . sequence because the current which results from depressing that particular key will enter the LHC's of CW5 from the eighteenth fixed contact of BS5. *What that key will be for each one of those 456,976 permutations of CW1, 2, 3, and 4 is of no importance at this point of the analysis.*

Now it is obvious that BS5 has 26 and only 26 fixed contacts through which current can emerge from a RHC of CW4 and enter into the LHC's of CW5. *It follows, therefore, that there can be 26 and only 26 such final cipher sequences for any setting of CW1, 2, 3, and 4; and thus, for any one of the 26 letters of the alphabet, no matter what the initial positions of the first four cipher wheels may be, the consecutive depression of any one key, for 26 times, with no intervening displacement of CW1, 2, 3, or 4, will yield a sequence of cipher equivalents that is absolutely fixed.* The complete set of sequences, designated hereafter as the BASIC CIPHER-TEXT SEQUENCES,[1] is given in the accompanying table 1.

[1] The table of basic cipher-text sequences will be entirely different when the machine is set with the indicator at REVERSE.

TABLE 1.—TABLE OF BASIC CIPHER-TEXT SEQUENCES

	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	Repeated	Omitted
1	Y	O	N	D	S	W	M	A	U	Z	X	F	L	Q	K	G	X	V	H	R	B	T	E	C	J	P	X	I
2	Q	I	S	F	T	D	P	J	V	A	W	N	Y	J	B	L	G	H	E	X	R	K	O	U	M	C	J	Z
3	U	V	E	W	N	Y	H	I	M	W	C	G	O	R	D	Q	P	S	X	F	J	Z	B	A	L	K	W	T
4	A	P	V	I	G	U	F	Y	W	S	M	Z	K	B	N	O	L	E	T	C	Q	H	J	I	R	D	I	X
5	C	Q	O	J	Y	V	W	P	N	H	E	V	S	Z	T	I	M	F	A	B	U	X	D	L	K	R	V	G
6	R	G	W	U	L	Z	A	Q	O	V	F	T	C	P	H	Y	E	N	M	D	I	Y	X	K	S	J	Y	B
7	D	A	P	T	W	M	B	V	E	R	O	L	U	X	C	F	Q	Z	U	J	N	I	K	G	Y	S	U	H
8	K	U	B	S	O	C	L	X	B	I	P	E	Z	F	V	T	H	D	J	Q	A	N	G	R	W	M	B	Y
9	L	H	J	Y	F	T	Q	K	G	B	S	O	Q	N	R	P	C	U	D	Z	W	E	M	X	I	V	Q	A
10	S	C	U	L	Z	F	S	R	Y	M	G	Q	W	O	I	J	V	K	P	H	T	A	N	D	B	X	S	E
11	P	B	M	R	A	G	V	E	K	J	Y	I	T	C	O	U	S	X	F	L	O	D	W	H	Q	Z	O	N
12	Z	Y	D	V	U	S	I	F	P	N	H	C	M	A	X	E	R	W	L	K	Z	G	Q	T	O	B	Z	J
13	O	F	K	M	H	L	J	T	S	C	I	X	G	D	U	Z	B	R	W	A	P	V	Y	E	N	A	A	Q
14	H	J	C	N	D	P	X	G	F	Q	Z	K	B	T	F	W	I	A	S	O	M	L	V	Y	E	U	F	R
15	W	R	T	X	Q	E	N	C	D	G	B	S	H	U	Z	M	O	L	K	I	V	R	A	J	P	Y	R	F
16	V	E	Q	O	K	B	T	S	C	U	K	H	A	Y	L	X	J	G	N	M	D	F	R	W	Z	I	K	P
17	G	T	Y	B	X	N	K	U	Z	E	R	M	D	I	J	V	A	M	Q	S	L	W	P	O	H	F	M	C
18	M	N	H	E	I	R	D	N	L	T	U	A	J	K	Y	C	F	Q	V	G	S	P	Z	B	X	W	N	O
19	E	S	F	H	B	X	G	M	A	D	J	R	V	W	P	D	K	C	Z	N	Y	U	I	Q	T	O	D	L
20	I	M	R	A	J	H	Z	O	X	P	V	B	E	L	Q	K	W	T	C	Y	G	S	F	N	D	H	H	U
21	B	D	I	Z	V	O	C	L	R	F	T	J	X	G	S	A	N	P	Y	W	E	M	H	P	U	Q	P	K
22	N	X	Z	G	P	K	U	W	Q	O	L	Y	I	E	M	H	D	J	R	E	F	B	C	V	A	T	E	S
23	J	W	X	C	R	Q	Y	H	I	L	D	P	F	M	A	N	Z	B	G	T	K	O	U	S	G	E	G	V
24	X	Z	G	Q	C	A	E	D	T	K	N	U	R	V	W	B	Y	I	O	P	H	J	S	F	C	L	C	M
25	T	K	L	P	M	J	O	B	H	X	A	W	N	S	E	R	U	Y	I	V	C	Q	L	Z	F	G	L	D
26	F	L	A	K	E	I	R	Z	J	Y	Q	D	P	H	G	S	T	O	B	U	X	C	T	M	V	N	T	W

23. **Nature of table of basic cipher-text sequences.**—It will now be shown that the table of basic cipher-text sequences given in the accompanying table 1 may be regarded as being merely a set of 26 secondary alphabets resulting from the sliding of two primary alphabets against each other. One of the primary alphabets (only when indicator is at DIRECT) is the right fixed sequence, RFS, the other is MAL5 (which merely represents the series of RHC's of CW5). There is, however, a slight difference between the mechanics of the system of producing the secondary alphabets in this case, and the mechanics of the usual or ordinary systems of producing secondary alphabets. In the usual systems each secondary alphabet is produced by finding the whole set of cipher equivalents for each different setting (or juxtaposition) of the two primary alphabets. In this system, not only are the initial settings of the two primary alphabets different for each secondary alphabet, but in addition to this, one of the primary alphabets is regularly displaced one interval in deriving each successive letter of each secondary alphabet. To demonstrate, set MAL5 against RFS so that their initial letters are opposite each other, thus:

```
MAL5----  F R I S Y A D P L J U X Z G K O B T W C V M H E Q N F R I S Y A D P L...
RFS------ T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Now construct an enciphering alphabet by successively displacing the upper component, MAL5, one interval to the left and writing down the equivalents found on RFS for the letters A, B, C, . . . of MAL5. For this initial setting the sequence is the following:

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

Comparing this with the eighteenth sequence in table 1, it is seen to coincide with it.

If the two primary sequences are set at the following initial positions, and the same process of finding cipher equivalents is followed, the sequence obtained coincides with the eighth sequence of table 1.

```
MAL5----  F R I S Y A D P L J U X Z G K O B T W C V M H E Q N F R I S Y A D P L...
RFS------   T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

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

The reason why this secondary alphabet begins with the second letter of the corresponding basic cipher-text sequence of table 1 is, of course, that the upper primary alphabet, MAL5, was at a setting equivalent to the second position of CW5, the setting when A of its normal alphabet component is at SET being considered the first position.

It is therefore apparent that (1) the table of basic cipher-text sequences is only a table of secondary alphabets produced by the sliding of two mixed alphabets against each other, and (2) this being the case, the secondary alphabets are all interrelated in some manner which ought to permit of the reconstruction of all of them having given only two of them.[1]

24. **The table of basic cipher-text sequences and the right fixed sequence.**—As a matter of fact, a clear way of looking at the cipher mechanics of the machine in encipherment (DIRECT) is to consider that all that the machine does is to apply a sort of an arbitrary "yardstick", or measuring rule to the right fixed sequence. This measuring rule simply marks off the letters of the right fixed sequence according to an absolutely definite interval-length (when the wiring is unchanged). To demonstrate exactly what is meant, take the first sequence of table 1, YOND. . . , refer to RFS and count the number of intervals between the successive letters of the YOND. . . sequence as they are located on the RFS, always counting from left to right. Thus, from Y to O on the RFS there is one interval; from O to N there are 13 intervals; from N to D, 18 intervals, and so on. The following sequence of intervals results:

```
RFS----  T  Y  O  E  U  M  X  D  F  J  Q  V  K  W  B  N  S  H  C  I  L  R  Z  A  G  P  T
         Y  O  N  D  S  W  M  A  U  Z  X  F  L  Q  K  G  X  V  H  R  B  T  E  C  J  P  Y
          1 13 18  9 23 18 18  7 18 10  2 12 16  2 12  8  5  6  4 19 12  3 15 17 16  2
```

This sequence of interval-numerals is the measuring rule. Apply it to RFS at any point and see the distribution of letters it yields. For example, start with A of RFS. The first interval length is 1; hence the letter which occupies the first position to the right of A, viz, G, is the second letter. The next interval length is 13; hence the letter which occupies the thirteenth position to the right of G in RFS is the third letter, and so on. The following sequence results:

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

Compare this with the eleventh sequence of table 1 and it will be seen to coincide with it, the initial point merely being different.

[1] See sec. XI of Tr. Pamphlet No. 3, and Riverbank Publications Nos. 15 and 21, listed in the bibliography to Tr. Pamphlet No. 3.

It is seen, therefore, that the measuring rule merely lays off a sequence of specific distances on RFS, and this sequence of distances is always constant. Now then, what is the measuring rule after all? It is merely the equivalent of CW5. To show that it is, consider the basic sequence YOND . . . The first letter Y is given by the setting as follows:

```
                                                     ↓
NAL5----  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
            ┌──────────────────────────────────┘
MAL5----  F R I S Y A D P L J U X Z G K O B T W C V M H E Q N
RFS ----  T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
            ↓
```

The letter R of MAL5 is the one involved. Now slide AL5 one space to the left; O is the second letter of the basic sequence, and the letter of MAL5 that is involved is S. Slide AL5 once more to the left; N is the third letter of the basic sequence, and the letter of MAL5 that is involved is T. Those letters of MAL5 which are successively involved are seen to follow the sequence of the normal alphabet, A, B, C, . . . Z. Now count the number of intervals between A, B, C, . . . as they appear on MAL5, always counting to the right. The intervals are as follows:

```
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
 11  3 13 17  3 13  9  6  7  5 20 13  4 16 18 17  3  2 14 19 10 24 19 19  8 19
```

But since CW5 moves one space to the left each time a letter is enciphered, and since the determination of the intervals was made by counting always to the right, a deduction of one interval should be made from each of the intervals above. This yields the following:

11-3-13-17-3-13-9-6-7-5-20-13-4-16-18-17-3-2-14-19-10-24-19-19-8-19
10-2-12-16-2-12-8-5-6-4-19-12-3-15-17-16-2-1-13-18- 9-23-18-18-7-18

Compare this with the original sequence of interval-lengths given above (p. 20), and it will be seen to be the same, merely displaced nine spaces to the left.

The question is asked, why is it that those letters of MAL5 which are successively involved in yielding a basic sequence follow one another according to the normal alphabetic sequence? The answer is quite clear: since the current always enters CW5 from the same fixed contact in BS5, and since CW5 advances regularly one step per depression, the LHC's of CW5 which are presented successively to that fixed contact are in normal alphabetic order, ABC . . . XYZABC . . .

It is apparent therefore that a very clear way of looking at the whole problem is this: RFS is an endless or cyclic series of letters, and CW5 is likewise an endless or cyclic measuring rule with a definite set of graduations marked upon it. Applying the two circles to each other, a set of 26 interval expressions of the letters of RFS are yielded by the measuring circle, CW5. *The only part played by CW1, 2, 3, and 4 is that concerned with the initial point at which the measuring rule is applied to RFS; the resultant of the interaction of CW1, 2, 3, and 4 determines merely the initial point of application of CW5 to RFS.*

It also follows that if CW5 is replaced by another wheel, the "graduations" on the new measuring rule are no longer the same as before, and different interval expressions of the same RFS will be obtained. Therefore the sequences of cipher resultants will be altogether different from those of before, and a new table of basic cipher-text sequences will result. Now in a given machine there are five cipher wheels, and the wheels are interchangeable. With five wheels, as stated before, 120 different horizontal permutation arrangements on the shaft are possible (the wheels all right-side up), but the fifth wheel in any of these 120 arrangements can be only one of five wheels. Now it was demonstrated in paragraph 22 that the point at which the electric current enters the LHC's of CW5 from BS5 is the only determining factor in establishing the particular sequence of cipher equivalents resulting from the successive depressions of any key. No matter, therefore, what the rotatory permutation of CW1, 2, 3, and 4 is, providing no displacement of any one of them occurs during the successive 26 encipherments of a single letter, the current will enter the successive LHC's of CW5 from the same contact of BS5. It follows, therefore, that it makes no difference whatever, as far as this particular factor is concerned, what the horizontal permutation of the first four cipher wheels is, whether they are in the order 1–2–3–4, or 4–2–1–3, or any other permutation, the electric current will always enter the LHC's of CW5 from one and only one contact of BS5, providing no displacement of the first four wheels occurs during the successive 26 encipherments of a particular letter.

This question raises itself: if the final cipher resultants are determined merely by the interaction of CW5 and RFS, what then is the function of the other cipher wheels?

The answer is that the particular sequence or succession in which the basic sequences follow each other in the table is determined by the particular combination of rotatory and horizontal permutations of CW1, 2, 3, and 4 upon the shaft. For the arrangement studied, viz, where CW1 occupies the first position on the left, CW2, the second, and so on, and where the cipher wheels are set to A all the way across, the first basic sequence corresponding to the encipherment of A_p, is YOND. . . ; the second basic sequence, corresponding to the encipherment of B_p is QISF. . . , and so on. For a different rotatory permutation of CW1, 2, 3, and 4 upon the shaft, or for the same rotatory permutation but with a different horizontal permutation of CW1, 2, 3, and 4, the order in which the 26 basic cipher-text sequences corresponding to the encipherments of A, B, C. . . Z will fall will be entirely different, *but the sequences themselves will be exactly the same as before.* In short, the only function of CW1, 2, 3, and 4 is that concerned with determining the particular order in which the individual sequences of the whole table of basic cipher-text sequences are produced.

It has been stated above that each different cipher wheel, when employed in the fifth position, will yield a different table of basic cipher-text sequences, even though RFS remains the same. If there are *n* cipher wheels available, then there can be *n*, and only *n* different tables, since the horizontal and rotatory permutations of the other four cipher wheels act as CW 1, 2, 3, and 4 and have nothing to do with the sequences of the tables.[1]

Assuming, however, the encipherment of a series of dispatches all prepared by means of the same horizontal permutations of the cipher wheels, it follows that one and only one table of basic cipher-text sequences is in effect. It will be shown herein that the entire table can be reconstructed if two and only two of its sequences are known, or if only one sequence and the RFS are known, and that the entire table is in reality composed of but one sequence of 26 letters, which when reconstructed destroys the entire secrecy of a system involving almost twelve million secondary cipher alphabets. One might even go further and say that under certain circumstances the entire secrecy of a system embracing over 91 billion secondary alphabets is dependent upon maintaining secrecy with respect to a single sequence of but 26 letters.

[1] If it is taken into consideration that each wheel may be inserted in an "upside-down" position when acting as CW5 then there are $2n$ different tables possible.

Section V

THE TABLE OF BASIC CIPHER-TEXT SEQUENCES

25. **Effects of repetition of plain-text letters.**—Assume for the moment a dispatch of 26 letters consisting exclusively of the letter A_p, enciphered by the effective setting OAAAAAO of the cipher wheels. The cipher text will be YOND. . . , one of the basic cipher-text sequences. Now assume a dispatch of 26 letters consisting exclusively of the letter B_p, also enciphered by the same effective setting. The cipher text will be QISF. . . , another one of the basic sequences. Now assume a dispatch of 26 letters consisting exclusively of the letters A and B, alternately, also enciphered by the effective setting OAAAAAO. The cipher text will be as follows:

```
Plain----  A B A B A B A B A B A B A B A B A B A B A B A B A B
Cipher---  Y I N F S D M J U A X N L J K L X H H X B K E U J C
```

This consists merely of alternate letters of the two basic sequences YOND. . . and QISF. . . , as is shown herewith:

```
Plain----    A B A B A B A B A B A B A B A B A B A B A B A B A B
Cipher---    Y I N F S D M J U A X N L J K L X H H X B K E U J C

Sequence 1_  Y . N . S . M . U . X . L . K . X . H . B . E . J .
Sequence 2_  . I . F . D . J . A . N . J . L . H . X . K . U . C
```

Now assume a dispatch of 26 letters, consisting exclusively of the letters T and D alternately, enciphered by the initial effective setting OVGMBAO. It is as follows:

```
Plain----  T D T D T D T D T D T D T D T D T D T D T D T D T D
Cipher---  Y I N F S D M J U A X N L J K L X H H X B K E U J C
```

The cipher text is exactly the same as for the alternate $A_p - B_p$ dispatch, with an entirely different setting or key. The plain-text letters are different in the two dispatches but the cipher letters are identical. In fact, an identical cipher sequence can be obtained for any pair of different letters whatsoever when the proper initial setting is chosen. Why is this? Is it not due to the effects that *mere repetition* of plain-text letters produces in this machine, regardless of what letters are involved? What has gone before should make this clear. In other words, what concerns the cryptanalyst in this case so far, is not the question as to *what* letter is repeated in the plain text but *whether or not a letter, any letter, is or is not repeated.* The results of repetition of any letter are predetermined, and the cipher equivalents occupy definite positions in one of the basic cipher-text sequences. The *identity* of the repetition is of no immediate concern, but the *existence* or *nonexistence* of the repetition is of the highest importance.

Now consider what happens in the encipherment of intelligible text. Let the dispatch be THE ELEMENTS OF THE SCIENCE OF CRYPTANALYSIS..., enciphered with the initial effective setting OAAAAAO. The results are as follows for the first 26 letters:

Plain	T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
Cipher	I	U	O	J	U	V	J	P	F	P	J	S	C	L	V	I	K	S	D	B	M	Z	D	J	S	K

From what has gone before, it is to be expected that—

(1) The cipher equivalents of identical letters will all belong to the same basic cipher-text sequence, and will fall into definite positions in that sequence;

(2) There will be present elements of as many basic cipher-text sequences as there are different plain-text letters; and

(3) As a corollary of the foregoing, the cipher equivalents of dissimilar letters will never exhibit coincidences with the same individual basic sequence.

With these three principles in mind, examine the foregoing encipherment.

Take the basic sequence which begins with I (the 20th in table 1) and apply it to the cipher text. Coincidence of the 1st, 10th, and 14th cipher letters with the 1st, 10th, and 14th letters of the basic sequence is noted as stated in (1) above, and noncoincidence with all the other letters also is noted, as stated in (3) above.

Plain	T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
Cipher	$\underline{I}$	U	O	J	U	V	J	P	F	$\underline{P}$	J	S	C	$\underline{L}$	V	I	K	S	D	B	M	Z	D	J	S	K
Sequence 20	$\underline{I}$	M	R	A	J	H	Z	O	X	$\underline{P}$	V	B	E	$\underline{L}$	Q	K	W	T	C	Y	G	S	F	N	D	H

Here the coincidences are due to repetitions of one letter, T_p; the noncoincidences represent letters which can *not* be T_p. If one did not know the plain text, but had merely the two bottom lines, one could nevertheless state definitely that the 1st, 10th, and 14th letters of the plain text are identical, and that whatever this plain-text letter is, it does not appear elsewhere in that line. The frequency of that plain-text letter is thus directly indicated by the number of coincidences with the basic sequence.

Now take the basic sequence which has U for its *second* letter (it is the 8th of table 1), and apply it to the cipher text. The coincidences are underlined below:

Plain	T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
Cipher	I	$\underline{U}$	O	J	U	V	J	P	F	P	J	S	C	L	$\underline{V}$	I	K	S	D	B	M	Z	D	J	S	K
Sequence 8	K	$\underline{U}$	B	S	O	C	L	X	B	I	P	E	Z	F	$\underline{V}$	T	H	D	J	Q	A	N	G	R	W	M

Now take the basic sequence which has O as its *third* letter (the fifth of table 1), and apply it to the cipher text. The coincidences are underlined below:

Plain	T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
Cipher	I	U	$\underline{O}$	$\underline{J}$	U	$\underline{V}$	J	$\underline{P}$	F	P	J	S	C	L	V	$\underline{I}$	K	S	D	$\underline{B}$	M	Z	$\underline{D}$	J	S	K
Sequence 5	C	Q	$\underline{O}$	$\underline{J}$	Y	$\underline{V}$	W	$\underline{P}$	N	H	E	V	S	Z	T	$\underline{I}$	M	F	A	$\underline{B}$	U	X	$\underline{D}$	L	K	R

This process can be continued until all coincidences have been noted. For the purpose of graphic representation, all the coincidences have been reassembled into the one diagram below, those belonging to the same basic sequence being indicated by identical numbers.

Plain	T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
Cipher	I	U	O	J	U	V	J	P	F	P	J	S	C	L	V	I	K	S	D	B	M	Z	D	J	S	K
	1	2	3	3		3		3	4	1	5	6	7	1	2	3	5	8		3	4	8	3	6	7	8

This procedure shows, therefore, that intelligible text when enciphered by the machine produces cipher text whose letters when arranged in lines of 26 can be distributed into definite positions in as many basic cipher-text sequences as there are *different* plain-text letters enciphered in each line; that those letters of the cryptogram which coincide with the letters of the same basic cipher-text sequence represent encipherments of identical plain-text letters; and that the frequency of occurrence of all plain-text letters in each line of text can be definitely ascertained by the process. What the plain-text letter in each case really is does not concern us at present.

26. **Use of the table of basic cipher-text sequences.**—Let us assume for the moment that the table of basic cipher-text sequences applying to a series of dispatches has been obtained in some illegitimate manner by capture, or otherwise. It is obvious that one could immediately determine those letters in each line which represent repeated letters of the plain text. For example, in the case of the enciphered message on page 24, one would be able to underline the repetitions in exactly the same manner as was done there. One would know then that the 1st, 10th, and 14th plain-text letters were the same; the 2d and 15th, and so on. The analyst could do this for all the lines of cipher text. *The result would be that the cipher text would have been decomposed into a series of single-alphabet substitution ciphers, the solution of which would not be very difficult*, as will subsequently be fully illustrated. Thus, it is apparent that the entire secrecy of the machine can be almost entirely destroyed if the table of basic cipher-text sequences is known to, or can be reconstructed by the enemy.

27. **Summary of preceding analysis.**—The most important facts and conclusions that were developed in the foregoing analysis may be conveniently summarized as follows:

(1) Cipher text produced by the machine is composed of the elements of 26 and only 26 basic cipher-text sequences.

(2) Every line of 26 letters of cipher text is composed of the spatial elements of as many different basic cipher-text sequences as there are different letters in the line.

(3) All that the machine does is to determine (in what *appears* to be a random, haphazard manner) the particular basic sequences that will be represented in each line of cipher text.

(4) The fifth cipher wheel in interaction with RFS produces the 26 basic sequences; the other four cipher wheels merely determine the permutations of the horizontal lines of the table of basic cipher-text sequences, or in other words, the order in which the basic cipher-text sequences follow each other in the encipherment of a dispatch.

(5) Possession or reconstruction of the table of basic cipher-text sequences will enable the cryptanalyst to distribute the letters of the text of cryptograms into a series of single-mixed substitution alphabets, which can be solved rather readily.

SECTION VI

MATHEMATICAL THEORY OF ANALYSIS

28. **Application of the general principles of frequency to the problem.**—In an actual tabulation of 100,000 letters occurring in telegrams of an administrative nature handled by the War Department Message Center on one day, the following distribution was found:

TABLE 2

E	12, 604	O	7, 408	C	3, 345	M	2, 534	B	1, 146
T	9, 042	A	7, 189	H	3, 287	Y	2, 099	X	469
R	8, 256	S	5, 759	F	2, 994	G	1, 795	K	353
I	7, 572	D	4, 029	U	2, 993	W	1, 401	Q	318
N	7, 558	L	3, 549	P	2, 661	V	1, 340	J	198
								Z	101

This frequency table, based as it is upon a fairly large number of letters, may be considered as representative of the normal or typical constitution of telegraphic English text.

What this normal frequency table means, of course, is this: If a volume of telegraphic English text totalling 100,000 letters is examined, there will be found approximately 12,600 E's, 9,000 T's, 8,300 R's, and so on. In other words, the data based upon 100,000 cases may be considered as giving a true picture of the constitution of any large volume of such text, and in any equivalent volume of text similar in nature, practically the same relative proportions of occurrences will be found to exist as were found in the 100,000 cases examined. Now if the 100,000 letters of which the text is composed were placed in a hat, and thoroughly mixed, the chances of drawing an E by a random selection are $\frac{12,604}{100,000}$ or approximately 0.126; that is, according to the laws of probability, in 1,000 successive drawings, a total of 126 E's would be chosen. Mathematically stated, P (the probability) for selecting an E is 0.126. Likewise, P for T_p is 0.090, P for R_p is 0.083, and so on. Now, if instead of placing the letters in a hat, one should have at hand all the text upon a large sheet of paper, and one should close one's eyes and at random point a pencil at one letter in the text just as it stands, it is obvious that P for E would still be somewhere in the neighborhood of 0.126; for T_p it would still be approximately 0.090; and so on, because, considered in its broadest aspects, the text is composed of a great variety of words, and so far as words are concerned, they are made up of such a diversity of permutations and combinations of letters that plain text can almost be regarded as being a random assortment of letters in the relative proportions given above.[1]

Now proceed one step further. Suppose two pencil points be directed, at random, with one's eyes closed, at intelligible text; what are the chances for designating two E's simultaneously, or two T's, or two of any other letter? According to the mathematical theory of probability, the probability that both of two independent events will occur together is the product of their

[1] This, of course, is not strictly true, and is discussed in section IX, p. 51.

separate probabilities. Hence, the chances for simultaneously designating two E's are 0.126 × 0.126, or 0.016; the chances in the case of two T's are 0.090 × 0.090, or 0.008, and so on.

Again, according to the theory of probability, the probability of the occurrence of several events which cannot occur together is the sum of the probabilities of their separate or individual occurrences. Thus, if $p, q, \ldots$ denote the separate probabilities of different events, the probability, P, that one of the events will happen is $P = p + q + \ldots$ Since the probability for random selection of two E's is 0.016, that for two T's is 0.008, and so on, the probability for the random selection of *any two similar letters, regardless of their identity*, is the sum of the respective probabilities for the random selection of two A's, two B's, two C's, and so on, up to and including two Z's. That is to say, the probability of directing two pencil points simultaneously at *any repetition* (two identical letters) is the sum of the separate probabilities for repetition of each letter of the alphabet. In table 3 the separate probabilities and their total are shown. The total of the separate probabilities for repetition, 0.066, means that in 1,000 cases where a pair of letters is selected or designated at random there will be 66 cases in which both members of the pair so selected will be the same letter; in other words, P for the simple occurrence of repetition, (hereafter denoted by the symbol $_rP$) *regardless of what the repetition may be*, is 0.066. As a matter of fact, the 66 cases will be composed of 16 cases where the repetition is the letter E, 8 cases where the repetition is T, 7 where it is R, and so on, in accordance with the last column of table 3. This, however, does not concern us at present.

TABLE 3

Letter	Frequency	P for separate occurrence	P for repetition (P^2)
E	12, 604	0. 126	0. 016
T	9, 042	. 090	. 008
R	8, 256	. 083	. 007
I	7, 572	. 076	. 006
N	7, 558	. 076	. 006
O	7, 408	. 074	. 006
A	7, 189	. 072	. 005
S	5, 759	. 058	. 003
D	4, 029	. 040	. 002
L	3, 549	. 035	. 001
C	3, 345	. 033	. 001
H	3, 287	. 033	. 001
F	2, 994	. 030	. 001
U	2, 993	. 030	. 001
P	2, 661	. 027	. 001
M	2, 534	. 025	. 001
Y	2, 099	. 021	. 000
G	1, 795	. 018	. 000
W	1, 401	. 014	. 000
V	1, 340	. 013	. 000
B	1, 146	. 011	. 000
X	469	. 005	. 000
K	353	. 004	. 000
Q	318	. 003	. 000
J	198	. 002	. 000
Z	101	. 001	. 000
Total	100, 000	1. 000	$_rP$ = . 066

On the other hand, since the probability that an event will not happen is the difference between unity and the probability that it will happen, or $(1-P)$, the probability, P, for *non-repetition* (hereafter denoted by the symbol ${}_{nr}P$) is $1-0.066$, or 0.934. That is, in 934 of the 1,000 cases, the two letters selected at random will be different.

29. **Development of mathematical theory applicable to the problem.**—The relation of this mathematical theory to the problem in hand will now be studied.

The normal frequency table shown in table 2 may be considered as being heterogeneous in this sense: It is composed of letters of widely different but rather definite or constant frequencies which gives the table a characteristically irregular "crest and trough" appearance. It is this very heterogeneity or irregularity of the table which leads directly to the solution of the simplest type of substitution cipher, that known as the single, mixed alphabet type. Any really scientific cryptographic method has for its aim the suppression of the frequency characteristics of the normal table, whereby the elements composing the cryptographic text may be identified, and the better the cryptographic method, the more complete is the suppression. In a perfect cipher system, the frequency table for the cryptographic text should be completely homogeneous or regular in this sense: (1) That all the letters of the alphabet should be represented, (2) they should occur with practically equal frequencies, thus suppressing the appearance of any "crests and troughs", and (3) *there should be no easy way of decomposing the homogeneous or regular table for the cryptographic text into one or more heterogeneous or irregular tables such as apply to single-alphabet substitution ciphers.* The cipher machine under consideration has been designed to produce such a result as nearly as possible, and it really does so to a very high degree. The following very homogeneous single-frequency table is based upon ten cryptograms produced by the machine, no two messages being in the same rotatory key.

A	B	C	D	E	F	G	H	I	J	K	L	M
117	128	130	122	105	100	133	136	118	113	125	128	115
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
115	128	117	116	114	144	120	130	132	129	122	· 130	144

Bearing in mind the three characteristics stated above, with respect to the frequency table for the text of a cryptogram produced by a theoretically perfect cipher system, examine the foregoing table. It will be noted (1) that all the letters of the alphabet are represented, and (2) that they occur with practically equal frequencies. There remains to be considered, therefore, only the third factor above-mentioned. Can this frequency table be decomposed into a multiplicity of tables exhibiting the heterogeneity and irregularity of normal single-alphabet distributions? That is the problem before the analyst in this case.

Now in any letter-for-letter substitution in a cryptographic system resulting in the production of homogeneous text in the sense stated above, the values ${}_rP=0.066$ (as explained in par. 28) and ${}_{nr}P=0.934$, must still hold true. This must be so because each cipher letter represents but one plain-text letter at a time, even though the plain-text letter may in each separate case be any one of the 26 letters of the alphabet. Taking the cipher text as it stands, according to the theory of probability as applied above, *in 66 cases out of every thousand, any two cipher letters selected at random will represent the same plain-text letter, and in 934 cases out of every thousand, any two letters selected at random will not represent the same plain-text letter.*

Now in each case of repetition it is of absolutely no consequence in the thus-far developed analysis what the repeated plain-text letter is, because it was demonstrated in sections IV and V, that the mere occurrence of repetition is the important phenomenon. For example, considering the YOND. . . sequence alone, if a plain-text letter is enciphered by Y_c at the initial point of this basic sequence, no matter what the plain-text letter be, its repetition in the next succeeding

position will produce O_c; in the next, N_c; in the next D_c, and so on. The mathematical theory developed above states that 66 cases out of 1,000 will be repetitions of letters, and these may be repetitions of 2 A's 2 B's 2 C's etc.[1] Now it is perfectly permissible to assume 1,000 cases where the first letter of the two members of a repetition is enciphered by Y_c at the initial point of a basic sequence, for this can be granted in view of the assumption of homogeneity of cryptographic text produced by the machine, so that of 26,000 lines of cipher text produced by this machine, and properly arranged, about 1,000 of these lines will have A_c as their initial letter, about 1,000 of them will have B_c as their initial letter, and so on. There will also be about 1,000 lines beginning with Y_c. Since the mathematical theory postulates that 66 out of 1,000 cases of a pair of letters selected at random will be repetitions, it follows that if a tabulation is made of only those letters which immediately follow Y_c in the 1,000 lines beginning with that letter, then in 66 cases the letter O_c should appear, and in 934 cases the letter should be some letter other than O_c. The reason that O_c will be the letter representing a repetition of the first plain-text letter in the line is, of course, that in this particular basic sequence O immediately succeeds Y in the YOND. . . sequence. Likewise, if a tabulation is made of only those letters which are in the second position after Y_c in those 1,000 lines, then in 66 cases the letter N_c should appear, and in 934 cases the letter should not be N_c. The same reasoning applies to tabulations made for any position after Y_c, and the letter which should appear 66 times out of 1,000 should be the letter which actually occupies that position in that particular basic sequence. The production of each letter in each of these cases is absolutely determined by the mechanico-electrical features (including the wiring, of course) of the machine, and by the mechanics of the English language: for the first position after Y the letter representing a repetition must be O; for the second, N; for the third, D; for the fourth, S; and so on, yielding sequences

$$\overset{1}{Y}\ \overset{2}{O};\quad \overset{1}{Y}\ \overset{2}{.}\ \overset{3}{N};\quad \overset{1}{Y}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{D};\quad \overset{1}{Y}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{.}\ \overset{5}{S},\ \text{etc.}$$

As before, for convenience, the symbol θ_c will again be used as a symbol to designate any unspecified letter of the cipher text. The symbol ${}_r\theta_c$ will be used to designate the cipher equivalent of a repetition; for example, in the case of the YOND. . . sequence ${}_r\theta_c$ for the first position after Y_c is O; or briefly stated θ_c in $\overset{1}{Y_c}\,\overset{2}{{}_r\theta_c}$ is O; θ_c in $\overset{1}{Y_c}\,\overset{2}{.}\,\overset{3}{{}_r\theta_c}$ is N; θ_c in $\overset{1}{Y_c}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{{}_r\theta_c}$ is D; and so on. The symbol ${}_{nr}\theta_c$ will be used to designate the cipher equivalent of a nonrepetition.

Now let attention be concentrated upon θ_c for a given position in the YOND. . . sequence, for example, θ_c in $\overset{1}{Y_c}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{{}_r\theta_c}$. In 66 cases out of 1,000 (the ${}_r\theta_c$ cases) $\overset{4}{\theta_c}$ will be D; in 934 cases (the $\overset{4}{{}_{nr}\theta_c}$ cases) it will not be D. Of the 66 $\overset{1}{Y_c}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{{}_r\theta_c}$ cases, a certain portion of them will represent the occurrence of $\overset{1}{E_p}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{E_p}$, another portion will represent the occurrence of $\overset{1}{T_p}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{T_p}$, another of $\overset{1}{R_p}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{R_p}$, and so on, each in proportion to its specific probability of repetition. But of the 934 $\overset{1}{Y_c}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{{}_{nr}\theta_c}$ cases, in each case the occurrence of two *different* letters is involved. A certain portion of them will represent the occurrence of $\overset{1}{E_p}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{T_p}$; another will represent the occurrence of $\overset{1}{T_p}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{E_p}$;

[1] The fact that each of these repetitions occurs with a characteristic frequency is immaterial in this connection. The 66 cases of repetition are here considered as a unit, without reference to the diversity of its constituent elements.

56973—34——3

another of $\overset{1\,2\,3\,4}{E_p..R_p}$; another of $\overset{1\,2\,3\,4}{R_p..E_p}$; and so on, each in proportion to its separate and specific probability of occurrence. Now in each of these 934 $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$, or nonrepetition cases, $\overset{4}{\theta_c}$ may be any letter except Y and D; what $\overset{4}{\theta_c}$ will be in each case is determined solely by the particular setting of the cipher wheels and by the plain-text letter which $\overset{4}{\theta_c}$ represents. For example, consider only the plain-text nonrepetition case $\overset{1\,2\,3\,4}{E_p..T_p}$, whose probability of occurrence is 0.126 × 0.09, or 0.011. Among the 934 $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$ cases there will be eleven cases in which $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$ represents $\overset{1\,2\,3\,4}{E_p..T_p}$. Here, $\overset{4}{\theta_c}$ can be any one of the 26 letters except Y and D, and in these 11 cases exactly what $\overset{4}{\theta_c}$ will be is determined solely by the particular rotatory permutation of the cipher wheels. In one case $\overset{1\,2\,3\,4}{E_p..T_p}$ may yield $\overset{1\,2\,3\,4}{Y_c..A_c}$, in another it may yield $\overset{1\,2\,3\,4}{Y_c..B_c}$, in another $\overset{1\,2\,3\,4}{Y_c..C_c}$, and so on. The same will be true with respect to any other $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$ case such as $\overset{1\,2\,3\,4}{E_p..R_p}$, $\overset{1\,2\,3\,4}{T_p..E_p}$, and so on. In other words, the second member of the two cipher equivalents in the 934 $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$ cases can be any one of the 26 letters of the alphabet except Y and D. (An exception will be discussed in par. 83, sec. XV.) *That is, in the 934 cases of* $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$, *the* ${}_{nr}\theta_c$*'s or cipher letters which are the second members of the pairs representing cases of nonrepetitions, are distributed over 24 letters of the alphabet,* and assuming a perfect homogeneity of text, $\overset{4}{\theta_c}$ in those 934 cases will be every one of the 24 letters an equal number of times, viz., 934 ÷ 24, or approximately 39 times. But in the same 1,000 cases of $\overset{1\,2\,3\,4}{Y_c..{}_r\theta_c}$, the 66 $\overset{4}{{}_r\theta_c}$ cases, or cipher letters which are the second members of the pairs representing cases of repetitions, are not distributed throughout the alphabet, but always yield the same cipher letter, which in this case is D_c. That is, the frequency of $\overset{4}{\theta_c}$ in $\overset{1\,2\,3\,4}{Y_c..{}_r\theta_c}$ is 66, whereas the frequency of $\overset{4}{\theta_c}$ in $\overset{1\,2\,3\,4}{Y_c..{}_{nr}\theta_c}$ is only 39, practically only two-thirds as large. It follows, therefore, that D should stand out prominently among all the other letters when a tabulation of 1,000 cases of $\overset{1\,2\,3\,4}{Y_c..\theta_c}$ occurrences is made. Or, stated in other words, the letter which may be taken as $\overset{4}{{}_r\theta_c}$ will be distinguishable by a frequency that theoretically will be one and two-thirds times as great as the frequency for any $\overset{4}{{}_{nr}\theta_c}$.

The same reasoning applies to the $\overset{1\,2\,3\,4\,5}{Y_c...\theta_c}$ occurrences. Here $\overset{5}{{}_r\theta_c}$ must be the letter S, which in the tabulation, should have a frequency greater than that for any other letter, because the basic sequence is $\overset{1\,2\,3\,4\,5}{\underline{\text{YONDS}}}$. . . . Theoretically, the entire basic sequence can be built up in the same manner, by tabulating all the cases in which Y_c appears as the initial letter of a basic sequence and distributing the 1st, 2d, 3d, . . . 25th letters after Y_c into separate frequency tables. In each case, theoretically, the letter which is of highest frequency will be the correct letter, and the process should ultimately yield the complete sequence

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

What has been detailed above as regards the YOND. . . sequence, applies equally well to any other basic cipher-text sequence; any one of them or, in fact, all of them could be reconstructed by the procedure indicated.

In actual practice, however, to have at hand a sufficient volume of text so that there will be 1,000 lines with A_c as the initial letter, another 1,000 lines with B_c as the initial letter, and so on, up to Z_c, would mean having about 26,000 lines of text, each 26 letters in length, an enormous quantity of about 80,000 words. But in reality not quite so much text would be necessary for it is really not essential that the ratio of the frequency of the correct letter to that of any of the incorrect letters in each case be as great as 66 is to 39, that is, as 1.7 is to 1. Ratios of 1.3 to 1 have in actual cases been found to be significant. For example, if the frequency of one particular letter is 15 occurrences, and the frequencies of all other letters vary from zero to approximately 9 or 10 occurrences, the difference is of sufficient degree to warrant the selection of the letter of highest frequency as being the correct letter. In an actual test, in over 50 percent of the cases the letter of highest frequency was found to be the correct letter, and in 75 percent of them the correct letter was found to be among the three highest in frequency.

The theoretical minimum number of cases or tabulations necessary to establish ${}_r\theta_c$ in actual practice may be regarded as being about 250, for theoretically in this number the frequency of ${}_r\theta_c$ in actual practice will be 16.5 as against $\frac{233.5}{24}=9.7$ for ${}_{nr}\theta_c$; the ratio is approximately 17:10. Now 250 cases of any initial letter in a homogeneous text would require 250 × 26 lines of letters, or 6,500 lines. Since each line contains 26 letters, a total of 169,000 letters of text, or approximately 25,000 words would be required. This is considerably below an average day's traffic when the amount of traffic is rather high, as in active operations.

Granting 25,000 words of traffic are available for study it may be said that all the basic sequences applicable to the cipher wheel which acts as CW5 may be reconstructed. (Further details of reconstruction will be given under sec. VII.) Having reconstructed the table, the cryptanalyst is at once in position to decompose the lines of cryptographic text into a series of single mixed-alphabet substitution ciphers, as explained in paragraph 26, section V, which may readily be solved, as will be illustrated very soon.

SECTION VII

RECONSTRUCTION OF TABLE OF BASIC CIPHER-TEXT SEQUENCES

30. **Preliminary remarks.**—It has been shown by the author in previous papers [1] that two differently mixed primary alphabets from which a series of 26 secondaries are derived can be reconstructed from but two of the derived secondary alphabets. It was shown in paragraph 24, section IV, that the table of basic cipher-text sequences is merely a table of secondary alphabets produced by the sliding of two primary mixed alphabets against each other; one of them is RFS, the other, MAL5. It would seem, therefore, that these secondary alphabets are all interrelated in some manner which ought to permit of the reconstruction of all of them having given only two of them. Only a slight modification of the process is really necessary in order to apply it to the case in hand. First, RFS must be reconstructed; from it and one of the basic cipher-text sequences the entire table can be reconstructed; finally, MAL5 can be reconstructed from RFS and any one of the basic cipher-text sequences.

31. **Reconstruction of right fixed sequence from two basic cipher-text sequences.**—In order to explain the method, use will be made of the first and second basic sequences of table 1, assuming that they have been reconstructed as a result of the application of the principles elucidated in the preceding sections.

```
Sequence 1----  Y O N D S W M A U Z X F L Q K G X V H R B T E C J P
Sequence 2----  Q I S F T D P J V A W N Y J B L G H E X R K O U M C
```

It will be noted first of all that each of the two sequences contains only 25 different letters, X being repeated in the YOND... sequence and J in the QISF... sequence. It is obvious then, that some letter is omitted in each sequence. In the former, I is the letter omitted from the sequence, in the latter, Z. As mentioned once before, and as explained in paragraph 83 of section XV, this repetition phenomenon is unavoidable in this system, and in every case, at least one letter will be repeated, and one will therefore be missing. It is also to be noted that the distance between the repeated letters is always the same in all the sequences of the same table of basic cipher-text sequences.

Now superimpose the two sequences, and, by shifting one relative to the other, make the repeated letters of one sequence occupy positions directly opposite the repeated letters of the other sequence. Thus:

```
Sequence 1----  Y O N D S W M A U Z X F L Q K G X V H R B T E C J P  (I missing).
Sequence 2----  U M C Q I S F T D P J V A W N Y J B L G H E X R K D  (Z missing).
```

Construct a chain of equivalents, beginning with any letter of Sequence 1, for example, Y. Thus, YU, UD, DQ, and so on, and then join the pairs eliminating the second occurrence of the

[1] See footnote to p. 20.

common letters. This yields the partial sequence, YUDQWSI. This is as far as one gets with this process in this case, because the continuing letter, I, is missing from the upper sequence. However, if I were present it would seem logical that it would have as its equivalent Z, the missing letter of the lower sequence. It thus would seem permissible to continue the sequence by adding the letter Z and then proceeding as before. This yields the complete sequence

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

If examination of this complete sequence of 26 letters is made, it will be found that it contains in regular order, but with a constant difference of three intervals, the letters of RFS. Thus, the RFS proceeds YOEUMXDFVQ... and the reconstructed sequence proceeds YUDQ... and so on.

Now, the reconstructed sequence seems to be equivalent to the real RFS, but with a constant difference of three intervals. What is the cause of this difference? Is it not connected with the fact that the initial point at which the measuring circle, CW5, is applied to RFS in the first case is different from that at which it is applied in the second by three intervals? Reference to the sliding strips will show this to be actually the case, for in the YOND sequence R is the first letter of MAL5 involved in producing this basic sequence; in the QISF sequence, U is the first letter of MAL5 involved in producing that basic sequence.

Now it is important to have the reconstructed RFS coincide exactly with the real RFS. Do the two basic sequences used above give in themselves any indication as to what the interval relation between the elements of the reconstructed RFS should be? The answer is that they do, by virtue of the relative positions occupied by the pairs of repeated letters in each basic sequence. In the QISF... sequence the position occupied by the first occurrence of the repeated letter, J, is three intervals to the left of that occupied by the first occurrence of the repeated letter, X in the YOND sequence, and in order to superimpose the two basic sequences, the lower one was shifted three letters to the right of its original position. This gives the clue to the correct interval relation between the letters of the reconstructed RFS. If the elements of the latter are therefore distributed over 26 spaces, leaving three intervals between sequent letters of the original reconstructed sequence, then the real RFS will be reconstructed. This yields the sequence

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

It should be added in passing that when the two basic sequences that are available for this reconstruction have their repeated letters at an even number of intervals apart, then a complete equivalent RFS cannot be reconstructed. In this case, two half-sequences result, which must be united into one sequence. Thus, for example, when the first and seventh basic sequences are selected for experiment, the following results are obtained:

```
Sequence 1----  Y O N D S W M A U Z X F L Q K G X V H R B T E C J P
Sequence 7----  P T W M B V E R O L U X C F Q Z U J N I K G Y S D A
```

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

Since the second basic sequence had to be displaced 24 letters to the right, in order to bring about coincidence of repeated letters with the first basic sequence in superimposing, then the elements of the two half-sequences must be separated by the interval indicated, 24, yielding the following:

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

These two half-sequences must now be assembled properly. By this is meant that one of the sequences must be inserted in the spaces presented by the other so as to make the entire sequence coincide with the real RFS. Whether O of the second half-sequence should be inserted between Y and E or between E and M or between M and D, or between any of the other pairs cannot be determined from the sequences alone. The determination must be made by means of a subterfuge explained further on. (See p. 38.)

A complete RFS can only be reconstructed from two sequences whose repeated letters are in positions separated by an odd number of intervals other than thirteen, and any two such sequences will do. It should be added that certain sequences will yield neither a complete equivalent RFS nor two half-sequences. These are the sequences in which the repeated letter in one sequence occupies a position 13 intervals removed from that occupied by the repeated letter of the other sequence. Here 13 independent pairs of equivalents can be established, but how they should be joined is not indicated. Note, for example, the following:

Sequence 1____ Y O N D S W M A U Z X F L Q K G X V H R B T E C J P
Sequence 4____ B N O L E T C Q H J I R D A P V I G U F Y W S M Z K

Here Y = B and B = Y; O = N and N = O, and so on. Thus no chain can be constructed. All that one can say is that in the real RFS, Y and B are 13 intervals apart, O and N likewise, and so on.

It is obvious that the cryptanalyst will not know, when he is reconstructing the two basic sequences from a detailed analysis of the cipher text, whether or not he is working upon two sequences such as will permit of reconstructing a complete equivalent RFS after he has finished their construction. If he is fortunate, he may strike it the first time, but if not, he may find it necessary to construct several basic sequences before a pair available for a complete reconstruction of the RFS turns up. But having found such a pair, reconstruction is rapid.

32. **Reconstruction of entire table of basic cipher-text sequences.**—Once two such sequences and the real RFS have been isolated, the entire table of basic cipher-text sequences can speedily be reconstructed in a manner which may best be described by detailed study of table 1.

Refer now to the set of sliding alphabets equivalent to CW1 to 5, and note what letter of NAL5 is concerned in producing Y, the first letter of the YOND. . . sequence. It is R. Now determine what sequence is produced when S, the letter following R in NAL5 is concerned, keeping AL5 in the same position. The sequence is the 19th shown in table 1, beginning ESFH.

Let us superimpose these two sequences:

Sequence 1____ Y O N D S W M A U Z X F L Q K G X V H R B T E C J P
Sequence 19____ E S F H B X G M A D J R V W P D K C Z N Y U I Q T O

Now study the sequences formed by oblique lines slanting toward the right, and passing through the superimposed sequences, such as

. O . N . D . S . W
E . S . F . H . B .

It will be seen that these coincide exactly with the sequences in RFS. By following the order of the letters in the known RFS, and completing the oblique lines of letters, the entire table can speedily be reconstructed. Thus:

TABLE 5.—BASIC CIPHER-TEXT SEQUENCES REARRANGED ACCORDING TO SEQUENCE IN RFS

1	Y	O	N	D	S	W	M	A	U	Z	X	F	L	Q	K	G	X	V	H	R	B	T	E	C	J	P
19	E	S	F	H	B	X	G	M	A	D	J	R	V	W	P	D	K	C	Z	N	Y	U	I	Q	T	O
14	H	J	C	N	D	P	X	G	F	Q	Z	K	B	T	F	W	I	A	S	O	M	L	V	Y	E	U
2	Q	I	S	F	T	D	P	J	V	A	W	N	Y	J	B	L	G	H	E	X	R	K	O	U	M	C
9	L	H	J	Y	F	T	Q	K	G	B	S	O	Q	N	R	P	C	U	D	Z	W	E	M	X	I	V
5	C	Q	O	J	Y	V	W	P	N	H	E	V	S	Z	T	I	M	F	A	B	U	X	D	L	K	R
16	V	E	Q	O	K	B	T	S	C	U	K	H	A	Y	L	X	J	G	N	M	D	F	R	W	Z	I
3	U	V	E	W	N	Y	H	I	M	W	C	G	O	R	D	Q	P	S	X	F	J	Z	B	A	L	K
8	K	U	B	S	O	C	L	X	B	I	P	E	Z	F	V	T	H	D	J	Q	A	N	G	R	W	M
18	M	N	H	E	I	R	D	N	L	T	U	A	J	K	Y	C	F	Q	V	G	S	P	Z	B	X	W
10	S	C	U	L	Z	F	S	R	Y	M	G	Q	W	O	I	J	V	K	P	H	T	A	N	D	B	X
20	I	M	R	A	J	H	Z	O	X	P	V	B	E	L	Q	K	W	T	C	Y	G	S	F	N	D	H
24	X	Z	G	Q	C	A	E	D	T	K	N	U	R	V	W	B	Y	I	O	P	H	J	S	F	C	L
4	A	P	V	I	G	U	F	Y	W	S	M	Z	K	B	N	O	L	E	T	C	Q	H	J	I	R	D
25	T	K	L	P	M	J	O	B	H	X	A	W	N	S	E	R	U	Y	I	V	C	Q	L	Z	F	G
15	W	R	T	X	Q	E	N	C	D	G	B	S	H	U	Z	M	O	L	K	I	V	R	A	J	P	Y
12	Z	Y	D	V	U	S	I	F	P	N	H	C	M	A	X	E	R	W	L	K	Z	G	Q	T	O	B
13	O	F	K	M	H	L	J	T	S	C	I	X	G	D	U	Z	B	R	W	A	P	V	Y	E	N	A
23	J	W	X	C	R	Q	Y	H	I	L	D	P	F	M	A	N	Z	B	G	T	K	O	U	S	G	E
21	B	D	I	Z	V	O	C	L	R	F	T	J	X	G	S	A	N	P	Y	W	E	M	H	P	U	Q
26	F	L	A	K	E	I	R	Z	J	Y	Q	D	P	H	G	S	T	O	B	U	X	C	T	M	V	N
6	R	G	W	U	L	Z	A	Q	O	V	F	T	C	P	H	Y	E	N	M	D	I	Y	X	K	S	J
11	P	B	M	R	A	G	V	E	K	J	Y	I	T	C	O	U	S	X	F	L	O	D	W	H	Q	Z
22	N	X	Z	G	P	K	U	W	Q	O	L	Y	I	E	M	H	D	J	R	E	F	B	C	V	A	T
7	D	A	P	T	W	M	B	V	E	R	O	L	U	X	C	F	Q	Z	U	J	N	I	K	G	Y	S
17	G	T	Y	B	X	N	K	U	Z	E	R	M	D	I	J	V	A	M	Q	S	L	W	P	O	H	F

Thus, given any one of the basic cipher-text sequences, and a knowledge of RFS, the entire table can be reconstructed within a very few minutes.

33. **Reconstruction of MAL5.**—Having reconstructed the table of basic sequences, it is advisable for the next step to reconstruct the mixed component of Alphabet 5. For this, RFS and any basic sequence will do. Of course, one does not yet know what the initial letter of RFS really is, but it is a matter of no consequence, as will be shown.

Taking a sliding strip with the normal alphabet written upon it, and space below it for the insertion of the letters of the mixed component, set it against the reconstructed RFS. Thus:

```
AL5----  {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
         {. . . . . . . . . . . . . . . . . . . . . . . . . .
RFS----    Y O E U M X D F J Q V K W B N S H C I L R Z A G P T
```

Take the basic sequence YOND and insert the letters which would be successively involved in producing this basic sequence, using any letter, say X, as an initial letter. Thus:

```
                                                   ↓
AL5----  {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
         {|_____________________________________________|
         {X . . . . . . . . . . . . . . . . . . . . . . . . .
RFS----   Y O E U M X D F J Q V K W B N S H C I L R Z A G P T
```

Sliding the strip one space to the left, and considering that the second letter of the basic sequence is O, the letter Y must be inserted in the position shown herewith:

```
                                                 ↓
         {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
AL5--    {  |___________________________________________|
         {X . Y . . . . . . . . . . . . . . . . . . . . . . .
RFS--      Y O E U M X D F J Q V K W B N S H C I L R Z A G P T
```

When this process is completed, the following sequence results:

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

This sequence is an *equivalent mixed component* and will produce exactly the same results as the real mixed component, so far as the basic sequences are concerned. In fact, it is the same as the real mixed component so far as the relative values of its sequence of elements are concerned, as is evident when the sequence is "run down" according to the normal alphabet. Thus:

TABLE 6

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

Note the generatrix beginning RISY. . . , and compare it with the real MAL5. It is identical with it, except as regards its initial letter.

The process described above, for reconstructing MAL5, may be used to determine how the two equal halves of a reconstructed RFS should be united (see p. 34) and at the same time reconstruct MAL5. By employing each half-sequence of RFS in connection with one of the basic cipher-text sequences, two partial MAL5 sequences are produced. For example, applying the process of reconstruction to the half-sequence,

```
Y . E . M . D . J . V . W . N . H . I . R . A . P .
```

in connection with the YOND... basic sequence, the following partial MAL5 is constructed (using X as a starting point):

```
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
X O   E     V R P A D     Q     Z C           W T
```

Applying a similar process to the other half-sequence,

```
O . U . X . F . Q . K . B . S . C . L . Z . G . T .
```

still in connection with the YOND... basic sequence, the following partial MAL5 is constructed:

```
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
  Y   G J           F M   U H     I B S N K     L
```

These two partial MAL5 sequences are now to be united.

Now it will be found that there is one and only one way in which these two sequences may be united properly, so as to make one sequence—they must be "dovetailed" into each other, the vacant positions in the first half being exactly filled by letters in the second half, and vice versa. This union is as follows, where the letters underlined with dots belong to the one partial sequence and those underlined with dashes belong to the other partial sequence:

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

This sequence is complete, and contains no repetitions. Comparison with the MAL5 sequence derived above will show their identity.

With MAL5 completed, it is only a simple step to unite the two half-sequences of the RFS, from which this MAL5 was constructed.

It is obvious, of course, that if RFS and MAL5 are known sequences to start with (say as the result of espionage), then not even one of the basic sequences need be constructed from the laborious process of text analysis. All the basic sequences may be established directly from the two known sequences, RFS and MAL5.

When the entire table of basic sequences has been reconstructed the cryptanalyst is in a position to decompose the lines of cipher text into the elements of a series of single mixed-alphabet substitution ciphers, which can be solved in a comparatively short time. It will be unnecessary to demonstrate the process at this point as it will come up again later in practically the same form.

34. **Reconstruction of table of basic cipher-text sequences from a few lines of cipher text and their equivalent plain text.**—It should be apparent from what has preceded, that if a few lines of cipher text with their letter-for-letter decipherments are at hand, it would be a very easy matter to reconstruct two basic sequences from which the entire table could then be derived. Such a case of having the cipher text with its plain text equivalent is not at all rare in practice, where such blunders as repeating a message in clear, after it has been transmitted in cipher or the reverse, sometimes occur. Or often, a plain-text dispatch is captured, whereupon it can be compared with its cryptographic form; or a paraphrased version of a dispatch is given to the press, and the paraphrase is a very poor one. Only five or six lines of 26 letters are necessary to establish the entire table of basic sequences, whereupon the secrecy of all other messages produced by the same machine is at once reduced to practically nothing.[1]

[1] See par. 84, sec. XV for such a case.

SECTION VIII

GENERAL OBSERVATIONS

35. **Résumé of preceding analysis.**—It has been shown thus far how the table of basic cipher-text sequences, when once it has been reconstructed, may immediately be used to decipher the text of dispatches. At least two basic sequences are necessary for the reconstruction, because it was first necessary to reconstruct the RFS, from which MAL5 could be reconstructed. If MAL5 and the RFS were previously known it would be unnecessary to reconstruct one of the basic sequences by that long process of analysis.

36. **Fundamental assumption for military cryptography.**—A fundamental assumption with regard to the use of any device for cryptographic purposes in military operations is this: It must be granted that the enemy cryptanalysts are in possession of full knowledge as to the mechanics of the device and, in fact sooner or later, come into possession of one, by capture, or even legitimately, by purchase, in the case of machines for sale upon the open market. Hence, in the case of the present machine, even if it be granted that the wiring of all the machines for use in the military service be absolutely secret to begin with, it must be assumed that the enemy already is thoroughly familiar with the mechanico-electrical operation of the machine, or will soon capture one or more of the machines upon the field of operations, and will thus learn the secret wiring.

37. **Deductions from fundamental assumption.**—Now it goes without saying that the capture or loss of a single machine would necessitate an immediate change in the wiring of all the machines in service. This could be accomplished in one of two ways. (1) The operators in the field could change the wiring according to directions from higher headquarters, or (2) new cipher wheels could be issued by higher headquarters. It is the opinion of the writer that the former case may be ruled out at once, for it would be entirely impractical in the field. A single error in wiring (182 connections must be established) would make all messages unintelligible; the time necessary for the change to be made would hardly be available, nor would the personnel with the requisite training always be available. The latter case, where new wheels are distributed from a central office is more feasible, but even in this case there are many difficulties, as may be attested to by the experience of G–2 in distributing small code books to all organizations in the Theater of Operations. Granting the second case, however, the wiring or circuits established in the plate at the rear of the machine, referred to in paragraph 10, section II, which determines the left and right fixed sequences, would still be unchanged, unless directions for the change emanate from the central office. Now there are 52 connections established in the rear plate; it is a practical certainty that many errors would be made by troops in the field working under difficulties, from written instructions. The process cannot be done in less than two hours, and skillful fingers are necessary. Practically, therefore, the change could not be made by troops in the field, and the wiring in the rear would remain permanent. The capture of one machine will disclose to the enemy the two important sequences, the LFS and RFS.

Having RFS at hand, it is apparent from what has gone before, that only a single basic sequence would be necessary in order to reconstruct the entire table of basic sequences. Or if MAL5 could be reconstructed by some process of analysis of the cipher text itself, not even one of the basic cipher-text sequences would be necessary.

The process whereby one of the basic sequences can be reconstructed from an analysis of the cipher text itself has been explained in detail. If a knowledge of the RFS is assumed, ought not the process be rendered more easy? Common sense would lead one to answer in the affirmative. Perhaps one could reconstruct MAL5 directly from an analysis of a comparatively small amount of text, and thus eliminate the necessity of having available the considerably larger volume of text required to build up one of the basic sequences first. This possibility forms the subject of the next section.

Section IX

RECONSTRUCTION OF ALPHABET 5

38. **Further analysis of the nature of Alphabet 5.**—If Alphabet 5 is set against RFS at the initial point, so that A of NAL5 is above T (the initial letter of RFS), it will be seen that Y, the first letter of the basic cipher-text sequence YOND. . . is under B of NAL5. Sliding Alphabet 5 one interval to the left, O, the second letter of the basic sequence YOND. . . is under D of NAL5, and so on. The whole sequence of letters of NAL5, that are successively concerned in the production of the YOND. . . sequence, as seen by noting the letters above the successive letters of the YOND. . . basic sequence, as Alphabet 5 is slid to the left is as follows:

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

Now take another basic cipher text sequence, say the second one of table 1, QISF. . . and repeat this process and write down the sequence of letters given by noting the letters of NAL5 that appear above the successive letters of the QISF. . . basic sequence as Alphabet 5 is slid to the left. It is as follows:

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

Comparing the two NAL5 sequences obtained from these two basic sequences it is noted that they are the same sequence—merely their initial points are different. In fact, one and only one sequence results when all the basic cipher-text sequences are treated in the same way.

What is this sequence? It seems to be some fundamental sequence that has not been encountered before this. It does not appear as any one of the alphabets of the diagrams given so far.

Consider once more the juxtaposition of Alphabet 5 and RFS for the YOND. . . basic sequence, and find the point at which the current enters CW5 in order to produce this basic sequence. It is at the point designated by the arrow in the following diagram: the eighteenth contact of BS5:

```
                                       ↓
         ⎧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 . .
AL5----⎨   ┌─────────────────────────────────┘
         ⎩. R . . . . . . . . . . . . . . . . . . . . . . . . . .
            |
RFS----  T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

The LHC of CW5 at which the current enters to produce the Y is R. But the fact that Y is the cipher resultant, and the fact that the letter of NAL5 that is over Y in the RFS is B, may when taken together be regarded as equivalent to assuming that R is converted into B and B is then converted into Y. In short, it would appear as though an "R current" is converted into a "B current" by the wiring of CW5, and further, that at the position indicated, the "B current" finally emerges as a "Y current." Hence, considered independently, and only with regard to the cipher mechanics involved, Alphabet 5 might be written, so far as only R and its conversion-equivalent are concerned, as follows:

```
                                          ↓
        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 . . .
AL5----{
        . . . . . . . . . . . . . . . . . B . . . . . . . . .
RFS---- T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Now repeat the process for the second letter of the YOND. . . basic sequence, having slid Alphabet 5 one space to the left.

```
                                      ↓
      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 . . .
AL5--{
      . . . . . . . . . . . . . . . . . . . . . . . . . . .
RFS--   T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Here an "S current" is converted into a "D current": the latter, into an "O current."

Hence, the placement of D is as follows:

```
                                      ↓
      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 . . .
AL5--{
      . . . . . . . . . . . . . . . . . . D . . . . . . . . . .
RFS--   T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

The next letter, N, of the YOND. . . basic sequence, is the result of the interaction of T, R, and N, as follows:

```
                                     ↓
    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 . . .
AL5{
    . . . . . . . . . . . . . . . . . . . . . . . . . . .
RFS     T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

from which follows:

```
                                     ↓
    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 . . .
AL5{
    . . . . . . . . . . . . . . . . . . R . . . . . . . . .
RFS     T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Combine the conversion results of Y, O, and N into one sequence:

```
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
. . . . . . . . . . . . . . . . . . B D R . . . . . .
```

The mysterious sequence which started this train of reasoning began with BDR. Continuing the process, the identity of the sequence of conversion-equivalents with the sequence BDRK. . . will be established, and so far as the cipher mechanics of CW5 are concerned, Alphabet 5 may be written as follows:

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


The Alphabet 5 which has heretofore been used, and the new or conversion Alphabet 5 may be placed in juxtaposition for study.

```
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 }
F R I S Y A D P L J U X Z G K O B T W C V M H E Q N } Alphabet 5.

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 } Converted
F Q T G X A N W C J O I V Z P H Y B D R K U S L E M } Alphabet 5.
```

These two alphabets manifest the simple enciphering-deciphering relationship of one and the same mixed alphabet: If the enciphering alphabet is at hand, the deciphering alphabet can be constructed, and vice versa, just as is the case with any ordinary mixed alphabet used in cryptography.

For ease in reference, the letter C will be used as a prefix to an alphabet designation to indicate that it is the converted equivalent of the real alphabet. Thus, CAL5 refers to the second of the two alphabets above, and NCAL5 refers to its normal component, MCAL5, to its mixed component.

In this case, either AL5 or CAL5 can be used in encipherment. In using the real Alphabet 5 (AL5) one proceeds from a letter in the normal component to the same letter in the mixed component and then takes the letter directly under it in the right fixed sequence (RFS). In using the CAL5 one takes as the cipher equivalent of a letter in its normal component that letter which is directly under it in its mixed component, and then notes the letter of RFS above which the cipher equivalent, *as it is located in the normal component*, falls. Thus, for example, for Y of the YOND. . . sequence, the chain is as follows: R of NCAL5 is converted into B of NAL5; but B of NCAL5 is now opposite Y of RFS. For the second letter, O, of the YOND. . . sequence, the chain is as follows: S of NCAL5 is converted into D of NCAL5; but D of NCAL5 is now opposite O of RFS. For the third letter, N, of the YOND. . . sequence, the chain is initiated with the letter T of NCAL5; for the fourth letter, D, of the YOND. . . sequence, the chain is initiated with the letter U of NCAL5, and so on, according to the sequence of the normal alphabet.

Similar relations will be found to obtain with respect to the other four alphabets, converted equivalent alphabets yielding the same results in encipherment as the real alphabet, providing one is consistent in their use as guides in encipherment.

Inasmuch as certain important relations are disclosed only when reference is made to the converted equivalent alphabets, from this point on all the cipher alphabets will be arranged and treated as converted equivalent alphabets, and in a subsequent section the relation between the real alphabets and the converted equivalents will be demonstrated.

The set of converted alphabets is as follows:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
GADBOCTKNOZXIWHFQYJVPMELSRGADBOCTKNUZXIWHFQYJVPMELSR } CAL 1.
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
IZNCTKUDPJEVOWLFHXSMGQAYBRIZNCTKUDPJEVOWLFHXSMGQAYBR } CAL 2.
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
PJXFWLTAUGYBMHROVNCKSEQIZDPJXFWLTAUGYBMHROVNCKSEQIZD } CAL 3.
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
FLVARGWCMQBXNYIOTJUPSKEDHZFLVARGWCMQBXNYIOTJUPSKEDHZ } CAL 4.
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ }
FQTGXANWCJOIVZPHYBDRKUSLEMFQTGXANWCJOIVZPHYBDRKUSLEM } CAL 5.
```

39. **Use of CAL5.**—Returning now to the example of encipherment using the phrase "THE ELEMENTS OF THE SCIENCE OF", let those letters of NCAL5 which are above the letters of RFS and which constitute the cipher letters of the cryptogram in each case be set down. The enciphered text is as follows:

I U O J U V J P F P J S C L V I K S D B M Z D J S K

The first letter of the cryptogram is I_c. Referring to the sliding strips it will be seen that I_c as it occurs in RFS is directly under T of NCAL5. Thus:

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

(The identity of T, the plain-text letter, with T, the letter of NCAL5 directly over I, the cipher letter is, of course, merely a coincidence.)

Alphabet 5 must be slid one space to the left, for the next letter.

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

The second cipher letter is U, and this letter of RFS is now beneath F of NCAL5.

Again Alphabet 5 is slid to the left, and the letter in NCAL5 above O (the third cipher letter) in RFS is found to be E. This process continued, results in the following:

Plain	T H E E L E M E N T S O F T H E S C I E N C E O F C
Cipher	I U O J U V J P F P J S C L V I K S D B M Z D J S K
Letters of NCAL5	T F E M I Q P G Q I T B E H Z I C H Z H Z R D G O L

The letters of the sequence TFEM . . . may be designated as the cipher-text equivalents of the normal component of converted Alphabet 5; this long designation will hereafter be referred to as the $NCAL5_c$ equivalents.

Now apply MCAL5 to these $NCAL5_c$ equivalents (TFEM . . .) making T the first letter coincide with T of MCAL5 and underline the coincidences. Thus:

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

It is noted that the 1st, 10th, and 14th letters coincide.

Now apply MCAL5 to the $NCAL5_c$ equivalents so that F, the second letter of the latter coincides with F of the former. Thus:

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

It is noted that the 2d and 15th letters coincide.

If the same process is applied with respect to the third letter of the series of $NCAL5_c$ equivalents, coincidences of the 3d, 4th, 6th, 8th, 16th, 20th, and 23d letters are noted. When the process is completed for the whole line of equivalents, the following results are obtained, in which identical numbers indicate coincidences yielded by the successive applications of MCAL5 to the $NCAL5_c$ equivalents:

I	U	O	J	U	V	J	P	F	P	J	S	C	L	V	I	K	S	D	B	M	Z	D	J	S	K
T	F	E	M	I	Q	P	G	Q	I	T	B	E	H	Z	I	C	H	Z	H	Z	R	D	G	O	L
1	2	3	3		3		3	4	1	5	6	7	1	2	3	5	8		3	4	8	3	6	7	8

Now apply the numerically distributed sequence to the plain text. Thus:

T	H	E	E	L	E	M	E	N	T	S	O	F	T	H	E	S	C	I	E	N	C	E	O	F	C
T	F	E	M	I	Q	P	G	Q	I	T	B	E	H	Z	I	C	H	Z	H	Z	R	D	G	O	L
1	2	3	3		3		3	4	1	5	6	7	1	2	3	5	8		3	4	8	3	6	7	8

It will be noted that similarly numbered letters of the $NCAL5_c$ sequence here also indicate coincidences of plain-text letters. This is not an isolated phenomenon applying only to the single line of cipher text under consideration but is a fundamental and general principle that applies to all lines of the cipher text produced by this machine. (Let the reader prove this by enciphering a phrase and applying the process indicated above.) In other words, if MCAL5 were at hand, and if the cipher text can be converted into its $NCAL5_c$ equivalents through a knowledge of the RFS, then all letters of the cipher text representing identical letters in every line of the plain-text of 26 letters of the cipher text can be found and indicated by properly assigned reference numbers. Each line of cipher-text will thus be decomposed into the elements of a simple, mixed-alphabet substitution cipher, just as was the case in the preceding method using the table of basic cipher-text sequences. Having assumed a knowledge of RFS in this section, the only unknown factor is MCAL5. If that can be reconstructed by analysis, the problem is solved.

40. **Relation existing between CAL5 and the table of basic cipher-text sequences.**—Whereas in section VI, all 26 basic sequences are necessary to effect this decomposition of each line of cipher text into its sets of identical elements, in this case one and only one sequence is necessary.

Take, for example, the two letters F. . .X (1 2 3 4 5) of MCAL5. Whenever any two identical plain-text letters separated by four intervals are so enciphered that the $NCAL5_c$ equivalent of the first letter is F, the $NCAL5_c$ equivalent of the second cipher letter will be X, no matter where this pair of plain-text letters happens to fall within the line of 26 letters. Why this must be so can readily be seen by referring to an actual encipherment.

Consider CAL5 in the position indicated below, assume that the first E of plain-text E. . .E (1 2 3 4 5) is being enciphered at the seventeenth displacement of CW5 from its initial point, and assume that the electric current enters CW5 at the point indicated by the arrow. The cipher resultant will be B.

NCAL5 . . . . P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T . . .
MCAL5 . . . . H Y B D R K U S L E M F Q T G X A N W C J O I V Z P H Y B D R . . .
RFS . . . . T Y O E U M X D F J Q V K W B N S H C I L R Z A G P

For the second E of E. . .E (1 2 3 4 5), the sliding alphabet will be in this position, the twenty-first displacement of CW5:

NCAL5 . . . . T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X . . .
MCAL5 . . . . R K U S L E M F Q T G X A N W C J O I V Z P H Y B D R K U S L . . .
RFS . . . . T Y O E U M X D F J Q V K W B N S H C I L R Z A G P

The cipher resultant will be O.

In the first case the current entered CW5 at the LHC of A, in the second case it entered at the LHC of E. From A to E in the normal alphabet there is an interval of four letters: from

56973—34——4

the first E of the plain-text $\overset{1\,2\,3\,4\,5}{\text{E}\ldots\text{E}}$ to the second, there happens to be an equivalent interval. The first phenomenon (distance from A to E in the normal alphabet) is a constant one; the second, is an accidental one, and the two phenomena are, of course, not causally related; they merely coincide as a matter of chance. But in the first instance, the current entering CW5 as an E current was changed into an F current, but F was then opposite B of the RFS; in the second instance, the current entering CW5 as an E current was changed into an X current, but X was then opposite O of the RFS. B and O are therefore causally related through the intermediacy of the measuring circle, CW5, that is, specifically through the intermediacy of the distance from F to X on MAL5, which happens to be four intervals. Whatever the cipher resultants be, so long as the two letters $\overset{1\,2\,3\,4\,5}{\text{F}\ldots\text{X}}$ of MAL5, are the ones that are involved in the encipherment of two letters four intervals removed from each other, and so long as no displacement of CW1, 2, 3, or 4 has occurred between the two encipherments, these different cipher resultants will represent encipherments of the *same* plain-text letter. There can be only 26 different pairs of cipher resultants for this measuring interval $\overset{1\,2\,3\,4\,5}{\text{F}\ldots\text{X}}$. They are as follows:

Position of CW5	Cipher resultants	Position of CW5	Cipher resultants
1. . . 5	M. . .I	14. . .18	C. . .X
2. . . 6	U. . .C	15. . .19	H. . .M
3. . . 7	E. . .H	16. . .20	S. . .U
4. . . 8	O. . .S	17. . .21	N. . .E
5. . . 9	Y. . .N	18. . .22	B. . .O
6. . .10	T. . .B	19. . .23	W. . .Y
7. . .11	P. . .W	20. . .24	K. . .T
8. . .12	G. . .K	21. . .25	V. . .P
9. . .13	A. . .V	22. . .26	Q. . .G
10. . .14	Z. . .Q	23. . . 1	J. . .A
11. . .15	R. . .J	24. . . 2	F. . .Z
12. . .16	L. . .F	25. . . 3	D. . .R
13. . .17	I. . .D	26. . . 4	X. . .L

Similarly, there can be only 24 other sets of such 26 pairs of resultants for the distances between F and all the other letters on MAL5, for there are only 24 intervals between F and the other 25 letters of the alphabet, viz, those between F and A, F and B, F and C, and so on.

For each letter of the alphabet there will be a total of 25 sets of 26 pairs of cipher resultants, yielding a grand total of 650 sets of 26 pairs. These, with a peculiar arrangement among themselves, form the table of basic cipher-text sequences. For example, $\overset{1\,2\,3\,4\,5}{\text{M}\ldots\text{I}}$ will be found in the 1st and 5th positions of the 18th sequence of table 1; $\overset{1\,2\,3\,4\,5}{\text{U}\ldots\text{C}}$ will be found in the 2d and 6th positions of the 8th sequence; $\overset{1\,2\,3\,4\,5}{\text{E}\ldots\text{H}}$, in the 3rd and 7th positions of the third sequence, and so on. Table 1 has 676 elements, capable of forming 676 sets of 26 pairs, but examination will show that there are two identical letters in each sequence and one letter always missing. This has been referred to before.

If the interval relations between one letter and all the other letters in MCAL5 can be established, that is all that is necessary to establish the whole mixed component, for then the position of each letter in the mixed component relative to all the letters can be definitely fixed, and this will then automatically give the interval relations between any letter and all the other letters. For example, having established the sequence FQIGX in a hypothetical MCAL5, the interval relations between F and Q, F and T, F and G, F and X, Q and T, Q and G, Q and X, and so on are automatically given.

Now then, can the interval relations between any one letter and all other letters in an unknown MCAL5 be established by an analysis of the cipher text alone? In other words, assuming a knowledge of RFS can MCAL5 be reconstructed very easily from the cipher text itself? This is the kernel of the problem.

41. **A dilemma.**—It has been shown how the letters of each line of cipher text can be converted into their $NCAL5_c$ equivalents through a knowledge of RFS. *If in each line there were some indication that would lead to identifying those conversion equivalents which represent encipherments of the same letter*, then obviously MCAL5 could be quickly constructed. For example, if in the following diagram applying to the cipher message on page 44 knowledge of the existence and position of identities were available, then one would say that MCAL5 is made up of the partial sequences shown:

(Similar numbers indicate repetitions of plain-text equivalents)

```
    T F E M I Q P G Q I T B E H Z I C H Z H Z R D G O L
    1 2 3 3   3   3 4 1 5 6 7 1 2 3 5 8   3 4 8 3 6 7 8
1   T . . . . . . . . I . . . H . . . . . . . . . . . .
2   . F . . . . . . . . . . . . Z . . . . . . . . . . .
3   . . E M . Q . G . . . . . . . I . . . H . . D . . .
4   . . . . . . . . Q . . . . . . . . . . . Z . . . . .
5   . . . . . . . . . . T . . . . . C . . . . . . . . .
6   . . . . . . . . . . . B . . . . . . . . . . . G . .
7   . . . . . . . . . . . . E . . . . . . . . . . . O .
8   . . . . . . . . . . . . . . . . . H . . . R . . . L
```

Assembling these partial sequences by the principle of direct symmetry of position, the following result is obtained:

T G . . . . C . O I . Z . H . B D R . . . L E M F Q

Over half of the sequence has been reconstructed from but one line of cipher text.

The reconstruction of MCAL5 resolves itself therefore into the problem of finding merely those letters in each line of the cipher text which represent encipherments of identical letters, that is, simply locating repetitions within horizontal lines. But, unfortunately, it would seem that the reasoning is in a circle: if repetitions can be located, MCAL5 can be reconstructed; but in order to locate repetitions it would seem that MCAL5 must be known. How can this dilemma be solved?

42. **Application of mathematical theory.**—Reference is now made to the mathematical theory concerning the effects of repetition and nonrepetition as set forth in section VI.

It was shown therein that the basic cipher-text sequences can be reconstructed by a mathematical analysis based upon the mere existence of repetition, but in such reconstruction each basic sequence represents a separate problem and the data pertaining to each one must be carefully isolated from those pertaining to all other basic sequences. Hence in reconstructing basic sequences by the application of the mathematical theory it was necessary that the reconstruction be based upon the initial letter of each particular basic sequence being reconstructed, and a total of 26 such separate reconstructions, corresponding to the 26 individual basic sequences, is possible. It will be noted that there are absolutely no repetitions of letters within *columns* of table 1, and a thorough understanding of the machine will show why it is impossible. A letter, θ, in any individual basic sequence has as its successors letters which depend solely upon the position θ occupies in that basic sequence. For example, take the first basic sequence, YON. . .CJP.

In compiling the frequency tables necessary to reconstruct this sequence by the mathematical theory of repetition only cases in which Y appears as the very first letter in the line can be used to build up the sequence; a Y in any other position in the line will belong to a different sequence, and hence the data based upon Y in the first position cannot be linked with those based upon Y in any other position. Similarly, an O in the second position in a line will belong to a sequence that is different from all other sequences in which O appears in any other position. Hence it is clear that a great deal of text is necessary to permit of reconstructing by this method a basic sequence, and as was shown in the last two paragraphs of section VI text consisting of approximately 25,000 words must be available for analysis before any basic cipher-text sequences can be reconstructed.

But in the case of the MCAL5 one and only one sequence is involved, and there will therefore be but one case of $\overset{1\,2\,3\,4\,5}{\mathtt{Y}\ldots\theta}$ regardless of where the Y occurs in each line. Hence all the data with respect to the $\overset{1\,2\,3\,4\,5}{\mathtt{Y}\ldots\theta}$, for example, can be placed in a single table, and all the data with respect to all other pairs of letters separated by the same interval, can be grouped into the same table. Thus, for example, a single frequency table which shows all the pairs of the formula $\overset{1}{\theta_1}\overset{2}{\theta_2}$ (sequent letters) would be made regardless of where $\overset{1}{\theta_1}$ is located in each line of 26 cipher-text-normal-alphabet-converted-equivalents; another table would be made for pairs of the formula $\overset{1}{\theta_1}\ \overset{3}{\theta_2}$ (i.e., separated by two intervals); another for the formula $\overset{1}{\theta_1}\ \overset{4}{\theta_2}$ (i.e., separated by three intervals), and so on up to those of the formula $\overset{1}{\theta_1}\ \overset{26}{\theta_2}$. If a sufficient amount of text were available, 25 such individual or separated tabulations based solely upon the cases in which A_c is selected as $\overset{1}{\theta_1}$ and showing what θ_2 is for all the 25 positions after A_c, would be all that would be required. In reality only 13 tabulations would be necessary for $\overset{1}{\mathtt{A}}\ \overset{14}{\theta_2}$ would be the same as $\overset{1}{\theta_1}\ \overset{14}{\mathtt{A}}$, $\overset{1}{\mathtt{A}}\ \overset{15}{\theta_2}$ would be the same as $\overset{1}{\theta_1}\ \overset{13}{\mathtt{A}}$, and so on. These 13 tabulations can really be grouped into one table in which all the data for all cases of $\overset{1\,2\,3\,4\ldots}{\mathtt{A}\ldots\ldots}\overset{26}{\theta_2}$ will be included.

The mathematical theory as here applied would be as follows:

> In every 1,000 pairs of $NCAL5_c$ equivalents separated by a constant interval, but taken from the same horizontal line of text, there will be 66 cases in which both members of the pair are the $NCAL5_c$ equivalents of the same plain-text letter; there will be 934 cases in which they are the $NCAL5_c$ equivalents of two different plain-text letters. Let the members of a pair be represented by the symbols θ_1 and θ_2. In the 66 cases of repetition, θ_2 will always be the same letter; in the 934 cases of nonrepetition θ_2 can be any one of 24 other letters, thus giving each of the 24 letters an average frequency of 39. Reasoning conversely, therefore, when the θ_2's of 1,000 cases of $\theta_1\ \theta_2$ are distributed over a frequency table, that letter (or θ_2) which is characterized by a frequency of 66, when all others have a frequency of only 39, will be the $NCAL5_c$ equivalent of the same letter of which θ_1 is the $NCAL5_c$ equivalent.

For example, in a tabulation of the cases of the formula $\overset{1}{\mathtt{G}}\ \overset{5}{\theta_2}$ among the $NCAL5_c$ equivalents of approximately 2,000 letters of cipher text, enciphered by the alphabets used in this demonstration, the following distribution of 69 $\overset{5}{\theta_2}$'s was obtained:

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
//	/	////	////	///	///	////	///	//	//	//	/	/			//	//	////	///	/////	/////	//	///// ///	/	////	/

(See line G, table 7.)

Reference to MCAL5 (p. 43) shows that the sequence $\overset{1\,2\,3\,4\,5}{\mathtt{G}\ldots\mathtt{W}}$ is correct. Here only a total of 69 observations are recorded, and yet the correct letter, W, manifested itself. Had 1,000 cases been observed there is absolutely no doubt about what the result would have been. The whole table for the fourth interval after A, B, C, . . . , Z ($\overset{1}{\theta_1}\ \overset{5}{\theta_2}$) based upon only the 2,000 letters of cipher text mentioned above, is shown in the accompanying table 7.

Even in this small number of observations the actual results are in fair conformity with the theoretical expectancy. In each case the correct letter is indicated by a circle. In certain cases the correct letter is among the very lowest in frequency, as for example in the case of the H distribution, but in 15 cases the correct letter is either the highest or second highest in frequency.

TABLE 7.—DISTRIBUTION OF $\overset{1}{\theta_1}\ \overset{5}{\theta_2}$ IN 2,000 LETTERS OF TEXT

	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	3	4	4	3	2	0	0	2	2	(3)	4	1	1	5	1	2	1	1	4	1	2	5	3	3	4	2	A
B	2	2	4	3	1	3	2	2	4	4	3	2	3	6	1	1	0	1	3	1	(6)	1	4	2	2	5	B
C	0	1	3	9	4	1	1	3	3	2	4	1	2	1	4	2	4	1	3	1	5	(7)	3	6	2	7	C
D	3	0	4	1	4	3	2	2	6	2	1	5	4	3	2	3	2	0	(7)	1	2	6	0	2	7	0	D
E	1	4	3	2	2	3	3	2	3	1	2	3	1	6	4	1	4	2	2	(4)	2	4	3	0	1	1	E
F	2	4	1	1	3	1	4	3	3	1	4	4	2	3	2	4	0	3	1	4	1	2	4	(3)	0	2	F
G	2	1	4	4	3	3	4	3	2	2	2	1	1	0	0	2	2	4	3	5	5	2	(8)	1	4	1	G
H	3	6	8	3	2	1	1	3	3	8	0	2	2	4	2	3	2	(1)	3	3	2	3	1	3	3	1	H
I	3	2	3	2	4	4	5	(5)	3	6	2	5	3	6	1	1	4	0	2	1	0	6	1	5	4	6	I
J	1	1	3	4	1	4	2	2	3	0	3	2	2	1	0	1	7	1	4	4	3	1	5	5	4	(7)	J
K	7	3	3	4	(3)	3	3	9	3	1	2	4	5	4	2	0	5	0	6	5	2	2	4	2	3	6	K
L	1	2	4	1	2	1	3	3	4	2	3	2	1	2	3	4	(3)	3	2	5	1	4	2	1	7	2	L
M	2	1	0	6	4	0	(5)	3	2	1	6	2	4	8	2	3	4	4	1	3	3	1	2	1	6	2	M
	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	
N	3	8	2	3	3	2	1	1	1	3	5	5	7	3	(8)	4	3	2	4	0	5	6	1	5	5	1	N
O	1	3	0	1	1	1	5	3	3	0	4	4	4	3	2	(1)	3	4	3	3	5	2	2	4	3	3	O
P	1	2	4	(1)	2	2	3	2	2	2	3	2	1	3	2	4	3	5	3	0	2	2	0	3	2	4	P
Q	(4)	0	0	2	2	3	7	3	5	3	5	2	1	2	4	2	0	2	5	2	2	4	2	2	3	5	Q
R	4	6	2	1	3	1	4	4	1	5	2	(3)	4	3	6	1	2	5	2	3	3	0	1	2	4	1	R
S	1	1	7	3	4	(7)	4	1	4	3	5	3	4	7	3	4	3	1	4	6	4	4	3	4	3	4	S
T	1	2	1	0	4	5	2	1	3	4	0	4	2	(7)	4	1	2	1	5	3	2	4	3	4	3	1	T
U	2	3	4	2	2	1	1	2	3	1	4	3	(5)	4	4	2	0	4	5	1	1	2	3	3	2	4	U
V	1	5	6	4	1	2	2	4	4	1	3	1	7	3	5	1	2	6	1	0	1	6	1	1	(3)	5	V
W	4	0	3	0	1	1	5	3	(6)	4	4	1	2	3	3	1	3	2	5	1	3	2	0	4	0	3	W
X	5	4	(5)	3	3	3	2	1	2	3	3	1	3	3	2	0	5	0	6	5	2	2	8	3	5	2	X
Y	2	5	4	3	4	3	1	5	5	1	(6)	1	2	4	2	3	2	4	3	3	6	0	7	4	2	5	Y
Z	0	(2)	5	3	1	3	9	2	3	1	5	1	5	4	5	1	3	5	5	2	2	3	2	3	6	0	Z
	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	

43. **Theoretical considerations relative to tables to be constructed.**—The accompanying table was based upon a study of pairs of the formula $\overset{1}{\theta_1}\,\overset{5}{\theta_2}$ and the question may be raised as to whether one and only one table is sufficient to permit of a reconstruction of MCAL5, or whether several tables are necessary. If one table will suffice, upon what interval relationship of pairs should it be based for the most conclusive results? Theoretical consideration will show that if a large volume of text is at hand, one table will suffice if the interval used is an odd interval, other than 13. If the interval is even, the best that can be expected is two half-sequences of 13 letters each. For example, suppose the fourth interval table is made, and suppose further that the table covers a sufficiently large number of observations so that the results in each case may be regarded as positive in that the letter of highest frequency will always be the correct letter. Then by constructing a chain of the letters of highest frequency, two sequences of 13 letters in MCAL5 can be established. For example, in this case suppose that in the $\overset{1}{A}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{.}\ \overset{5}{\theta_2}$ distribution J shows up as highest in frequency for $\overset{5}{\theta_2}$; in the $\overset{1}{J}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{.}\ \overset{5}{\theta_2}$ distribution Z shows up as highest in frequency for $\overset{5}{\theta_2}$; in the $\overset{1}{Z}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{.}\ \overset{5}{\theta_2}$ distribution B shows up as highest in frequency for $\overset{5}{\theta_2}$, and so on, this chain establishes itself: $\overset{1}{A}\ \overset{2}{.}\ \overset{3}{.}\ \overset{4}{.}\ \overset{5}{J}\ \overset{6}{.}\ \overset{7}{.}\ \overset{8}{.}\ \overset{9}{Z}\ \overset{10}{.}\ \overset{11}{.}\ \overset{12}{.}\ \overset{13}{B}$, etc. The seventh placement, G, falls into this position:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
A . . . J . . . Z .  .  .  B  .  .  .  U  .  .  .  M  .  .  .  G  .
```

The next placement, W, would fall into this position:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
A . W . J . . . Z .  .  .  B  .  .  .  U  .  .  .  M  .  .  .  G  .
```

Continuing the process a sequence of 13 letters in MCAL5 may thus be established from one table. The second half-sequence would be obtained by starting with a letter not found in the first set. However, if the interval had been odd and not 13, the chain would have continued until all 26 letters had been properly placed. As a general rule, it may be said that it will be safer to compile several tables which will be mutually corroborative, as explained in paragraph 45.

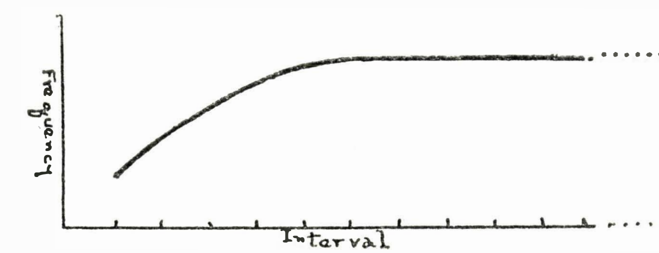
However, it is interesting to see whether or not, from theoretical considerations alone, there should be a certain single table which would give more conclusive results than any other single table. For example, if only one table were to be constructed, would it be best to base it upon pairs of the formula $\overset{1}{\theta_1}\,\overset{2}{\theta_2}$, or $\overset{1}{\theta_1}\,\overset{6}{\theta_2}$, or $\overset{1}{\theta_1}\,\overset{8}{\theta_2}$, or what formula?

The mathematical theory of repetition and nonrepetition, as developed in this paper, postulates that 66 out of 1,000 observations of *any* pair of letters will be repetitions, the remaining 934 will not be repetitions. In an actual test of the theory upon plain-text, the data shown in table 8 were obtained. Column 1 applies to observations made upon letters that were sequent, that is, separated by a single interval, formula $\overset{1}{\theta_1}\,\overset{2}{\theta_2}$; column 2 applies to observations made upon letters separated by two intervals, formula $\overset{1}{\theta_1}\,\overset{3}{\theta_2}$, and so on by increasing intervals.

TABLE 8

Interval	$\overset{1}{\theta_1}\,\overset{2}{\theta_2}$	$\overset{1}{\theta_1}\,\overset{3}{\theta_2}$	$\overset{1}{\theta_1}\,\overset{4}{\theta_2}$	$\overset{1}{\theta_1}\,\overset{5}{\theta_2}$	$\overset{1}{\theta_1}\,\overset{6}{\theta_2}$
Actual repetitions	7	11	14	20	19
Actual nonrepetitions	222	218	215	209	210
Repetitions per 1,000 cases	31	48	62	88	84

44. **Explanation of the discrepancy between mathematical theory and actual data.**—According to the mathematical theory the tabulations in table 8 should all be practically equal but it is seen that the actual results differ from the theoretical expectancy to a slight degree. These discrepancies are due to two causes: (1) An insufficient number of observations, and (2) whereas the mathematical theory postulates a purely random selection based upon a thorough mixture of the letters of the text, actually, letters forming intelligible text show a marked degree of association which tends to distort the theoretical expectancy. That is, for example, E tends to unite with R, either as ER or RE; I tends to unite with N as IN; I, N, and O tend to unite as ION; E, M, N, and T, as MENT, and so on. This will affect the data in such a way as to make intelligible text not equivalent to a strictly randomized or heterogeneous sequence of letters such as the mathematical theory postulates. The approximation to the theoretical is closest in the case of pairs of the formula $\overset{1}{\theta_1}\,\overset{4}{\theta_2}$, as shown in table 8. It is extremely probable that if an extensive study were made of this point, the relation between the interval separating repetitions and the frequency of the repetitions could be expressed in the form of a curve of the following nature:



The reason for this is not difficult to see. The closer together the members of any $\theta_1\,\theta_2$ pair stand in such intelligible text, the more likely is it that the natural affinities of letters will manifest themselves so as to distort the theoretical expectancies based upon a purely random selection; conversely, the further apart these members are, the less likely is it that such natural affinities will manifest themselves. Hence, it should follow theoretically, that tabulations based upon pairs of formulae greater than say $\overset{1}{\theta_1}\,\overset{6}{\theta_2}$ should most closely approximate the theoretically expected results because the intervals between each pair are great enough to overcome or suppress the natural affinities of letters constituting clear text.

45. **Necessity for additional tables.**—Tables based upon other intervals may be necessary to corroborate results obtained from the study of but one table. For example, having determined from a 4th interval table the sequence $\overset{1}{A}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{.}\,\overset{5}{J}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{.}\,\overset{5}{Z}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{.}\,\overset{5}{B}\,.\,.\,.$, a table based upon the 8th interval should show $\overset{1}{A}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{.}\,\overset{5}{.}\,\overset{6}{.}\,\overset{7}{.}\,\overset{8}{.}\,\overset{9}{Z}$; $\overset{1}{J}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{.}\,\overset{5}{.}\,\overset{6}{.}\,\overset{7}{.}\,\overset{8}{.}\,\overset{9}{B}$; and so on. Thus, corroboration of placements can be obtained. With the definite placement of each letter, the possibilities for the placements of the remaining letters become more and more limited, until with the last letter, but one position is left for its placement. Thus, with a few correct placements, the work involved in establishing MCAL5 becomes progressively easier and easier, providing no mistakes are made due to insufficient data, or inaccurate work.

46. **Procedure after MCAL5 has been reconstructed.**—Once MCAL5 has been reconstructed one can proceed immediately to underline by distinctive colors in each line of text the $NCAL5_c$ equivalents (and thus the cipher letters) which represent identical plain-text letters, or, one can proceed to reconstruct the table of basic cipher-text sequences by using the reconstructed MCAL5 and RFS in the manner illustrated in paragraph 32, section VII. Then one

can underline the cipher letters themselves, in distinctive colors, to represent identical plain-text letters. From this point on, one is confronted with a slightly modified form of a single mixed alphabet substitution cipher as stated in the previous sections. With certain short cuts to be explained later, solution of all messages is then readily achieved.[1]

[1] Instead of underlining, by distinctive colors, NCAL5 equivalents representing identical plain-text letters, one may designate the identities by some other method, for example, by the numeration method shown in paragraph 25, where the cipher letters representing identical plain-text letters in the phrase "The elements of the science of cryptanalysis" are assigned identical numbers.

SECTION X

PRACTICAL APPLICATION OF PRINCIPLES

47. **Nature of the test.**—Attention will now be directed to the application of the foregoing principles to the analysis of an actual problem. The Code and Signal Section of the Navy Department, in collaboration with whom the practical tests of the various theories developed by the author were made, presented the writer with a series of ten cipher messages enciphered by a machine in which they had changed the wiring of the cipher wheels, so that this wiring was entirely secret, so far as the present author was concerned, but in which the wiring of the LFS and RFS remained the same as before and was, of course, known to the writer.[1] The text of the ten messages and the key settings applying to the wheels, *except the 2d and 4th cipher wheels, the settings of which were different for each dispatch and were kept secret from the writer*, are given in the appendix. The theory behind the secrecy as regards cipher wheels two and four is that each station was supposed to have a different setting as regards these two wheels so as to avoid all chances of two or more dispatches from different stations being enciphered by exactly the same key.

48. **Arrangement of dispatches.**—The dispatches as presented for analysis were written out in lines of 26 letters each corresponding to the initial position of CW5 at its encipherment. For example, Dispatch No. 1 was enciphered by the key AGRAM. This means that the initial apparent setting was as follows:

LAW	CW1	CW2	CW3	CW4	CW5	RAW
A	G	?	R	?	A	M

The initial effective setting was therefore as follows:

LAW	CW1	CW2	CW3	CW4	CW5	RAW
A	G	?	R	?	B	N

One letter was enciphered, whereupon (RAW being at N for the first letter) LAW and CW1 were advanced one step to the following position:

LAW	CW1	CW2	CW3	CW4	CW5	RAW
B	H	?	R	?	C	O

Then CW5 and RAW were both automatically advanced, one step per letter for 26 letters, whereupon, at the 26th letter (the 27th of the dispatch) the wheels were in this position:

LAW	CW1	CW2	CW3	CW4	CW5	RAW
B	H	?	R	?	B	N

[1] The Hebern Company furnished the Navy Code and Signal Section with a pair of machines about a year before this office received similar ones. The wiring in the rear switching plate of the Navy machines was identical with that in the machines furnished this office although the wiring of the cipher wheels was altogether different. Apparently the manufacturers had in mind a standard wiring of the rear switching plate for all machines, and considered that the degree of secrecy based upon the cipher wheels alone was sufficient to thwart all efforts of cryptanalysts.

The next letter was enciphered in this position:

LAW	CW1	CW2	CW3	CW4	CW5	RAW
C	I	?	R	?	C	O

Since each series of 26 letters immediately following the advance of CW1 forms a single mixed-alphabet substitution cipher of its own, and conversely since each such single mixed alphabet is initiated by the displacement of CW1, it is advisable for this and other reasons to be detailed later, to have the dispatches in such a form that the initial letter of each line of cryptographic text is the first letter that was enciphered just after CW1 was displaced. Since CW1 is displaced when N of RAW is at SET, the dispatches were written down on cross-section paper so that the key letter N of RAW applies to the last letter of each line, and the key letter O of RAW applies to the first letter of each line. Thus having fixed the position of the initial letters of lines, the key letters of CW5 applicable to the columns can then be indicated by the letters of a normal alphabet beginning at the correct point, and applicable to the correct columns. For example, if the apparent key setting for CW5 is A (as in the keyword AGRAM), then the effective key setting of CW5 for the initial letter of the dispatch is B, and the normal alphabet is written above the dispatch so that the letter B is above that column in which the initial letter of the dispatch falls. Thus, Dispatch No. 1 took the following form, in which the key setting for the initial letter in each line is shown:

DISPATCH NO. 1

Key: AGRAM (Effective key: AGRBN)

(Reading of key at the beginning of each line of text is shown at the left of each line)

					RAW	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
					CW5	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
LAW	CW1	CW3	CW5	RAW	CW1																										
					g																										J
B	H	R	C	O	h	N	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S
C	I	R	C	O	i	U	F	C	D	S	U	F	M	O	V	K	C	N	K	Y	N	N	G	A	U	W	Y	L	I	Q	Z
D	J	R	C	O	j	U	T	L	W	B	Y	D	G	O	W	K	H	R	X	T	C	J	C	S	V	G	J	J	F	Y	V
E	K	R	C	O	k	J	S	R	C	E	Z	U	Q	K	D	O	Y	T	X	V	T	V	C	A	S	N	Q	P	G	E	C
F	L	R	C	O	l	A	R	U	C	W	L	D	D	C	U	Q	D	X	F	L	C	B	K	D	B	E	C	H	X	D	G
G	M	R	C	O	m	V	A	Y	E	E	U	Z	H	W	R	W	V	V	P	V	D	V	M	G	E	N	J	W	V	U	U
H	N	R	C	O	n	E	N	M	O	Q	J	P	U	M	V	K	G	W	Q	C	Z	W	K	R	I	I	X	M	J	A	C
I	O	R	C	O	o	L	N	S	W	E	A	M	I	A	U	U	V	W	V	B	L	E	M	B	O	S	P	X	F	R	R
J	P	R	C	O	p	S	G	O	W	C	J	L	V	M	H	Y	A	J	E	Z	G	F	Y	B	U	D	A	Z	L	O	Q
K	Q	R	C	O	q	U	M	T	Z	T	O	V	T	B	D	K	W	H	A	C	H	Y	N	Y	O	B	N	P	I	H	R
L	R	R	C	O	r	T	K	S	X	F	G	W	M	N	L	N	G	O	H	Y	M	K	H	P	G	W	I	E	B	E	L
M	S	R	C	O	s	A	B	L	Z	C	J	U	C	L	J	X	S	C	U	D	L	W	U	T	A	F	I	A	R	T	U
							↓ Key: OTSDP																								
N	T	R	C	O	t	S |	N	G	X	A	Z	B	O	H	G	W	P	Y	G	Z	R	V								

It will be noted that the initial setting for the last line of text is NTRCO. Remembering that when N appears on LAW the next encipherment will advance LAW and CW3, a bar is used to separate the first letter of the line (S) from the rest, to indicate that a displacement of CW3 occurred at that point. The letter S represents a single occurrence in the particular mixed alphabet to which it belongs, because when CW3 shifts, a new alphabet is introduced. All the dispatches were written out in a similar manner.

Another point in connection with the method of writing out the dispatches must be mentioned. Each column of the dispatch when written as is the one directly above, is designated by a letter which corresponds to the position of CW5 in the encipherment of the dispatch, and, of course, letters in the same horizontal line represent the 26 encipherments with one position of CW1. These designatory letters may, therefore, well serve as coordinates to indicate any letter to which reference is made in the subsequent analysis. The position occupied by a letter will be referred to as its *locus*, which may then be given by a capital letter, indicating the column in which the letter occurs, and a small letter, indicating the horizontal line in which it occurs. Thus, locus Gi designates that position occupied by the letter in column G, line i; the letter accompanying this locus in the case of the foregoing dispatch is S_c.

49. **Finding NCAL5$_c$ equivalents.**—The first step was to determine the NCAL5$_c$ equivalents and write them down under the cipher letters, as explained in paragraph 38, section IX. All that was necessary was a fixed alphabet corresponding to RFS and a sliding normal alphabet. J is the first cipher letter. When it was enciphered, the letter B of CW5 was at SET (this from the key setting, AGRAM). Hence, the sliding alphabet was set so that B of NAL5 was directly above T of RFS.

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

J of RFS was seen to be under K of the normal alphabet. Hence, K was written under J, as the NCAL5$_c$ equivalent of J of the cipher text. Now CW5 was in exactly the same position for every letter of the column in which J is located. Hence, the NCAL5$_c$ equivalents for all the letters in that column were at once written down by referring to the fixed and sliding alphabets above. Thus, S, the second letter in the column is seen to be under R; Z, the third letter, is under X, and so on, all the way down. The second letter of the dispatch, N, was enciphered when C of CW5 was at SET. Hence the normal alphabet strip was slid one space to the left. Thus:

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

N is now under R, and all the letters in the same column with N can be converted. Thus the process was continued until all the cipher letters were converted into their NCAL5$_c$ equivalents.

50. **Constructing the necessary tables.**—It was then necessary to construct frequency tables of the kind described in paragraph 42, section IX. Five tables were constructed. They are for pairs with the formulas $\overset{1}{\theta_1}\,\overset{4}{\theta_2}$, $\overset{1}{\theta_1}\,\overset{6}{\theta_2}$, $\overset{1}{\theta_1}\,\overset{7}{\theta_2}$, $\overset{1}{\theta_1}\,\overset{10}{\theta_2}$, $\overset{1}{\theta_1}\,\overset{13}{\theta_2}$; these are all given in the appendix (tables 15–19). Note should be made of one fact in connection with the construction of these tables.

Consider the *h* line of NCAL5$_c$ equivalents as follows:

R H E L X S E Z E P R H K O H X J V L W K S Q T F R

In compiling the first table, recording pairs with the formula $\overset{1}{\theta_1}\,\overset{4}{\theta_2}$, when Q, the 23d letter in the line is reached, its third interval successor is R, which terminates the line. But since each basic sequence may be regarded as being in the nature of an unbroken chain, or cycle, and since these NCAL5$_c$ equivalents are merely normal alphabet expressions of the basic sequence, it is perfectly legitimate to continue the tabulation of 3d interval pairs by taking the second members of pairs $\overset{24}{\theta_1}\,\overset{1}{\theta_2}$, $\overset{25}{\theta_1}\,\overset{2}{\theta_2}$, and $\overset{26}{\theta_1}\,\overset{3}{\theta_2}$, from the *beginning of the same line*. Thus, $\overset{Zh}{\text{T}}\,.\,.\,\overset{Ch}{\text{R}}$, $\overset{Ah}{\text{F}}\,.\,.\,\overset{Dh}{\text{H}}$, and $\overset{Bh}{\text{R}}\,.\,.\,\overset{Eh}{\text{E}}$ complete the tabulations for this line. (Loci are shown above the letters.) Hence, each line of 26 letters yields 26 observations as regards pairs separated by any constant interval, that is, with any formula whatever.

DISPATCH NO. 1

Key: AGRAM. (Effective key: AGRBN)

	RAW..	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	CW5...	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	
LAW CW1 CW3 CW5 RAW	CW1																											
AGRBN	g																											J—Text. K—NCAL5$_c$ eq.
BHRCO	h	N	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S	—Text.
		R	H	E	L	X	S	E	Z	E	P	R	H	K	O	H	X	J	V	L	W	K	S	Q	T	F	R	—NCAL5$_c$ eq.
CIRCO	i	U	F	C	D	S	U	F	M	O	V	K	C	N	K	Y	N	N	G	A	U	W	Y	L	I	Q	Z	
		G	L	W	M	W	L	Q	O	M	W	Y	F	D	B	R	G	H	R	R	Z	J	Y	S	S	K	X	
DJRCO	j	U	T	L	W	B	Y	D	G	O	W	K	H	R	X	T	C	J	C	S	V	G	J	J	F	Y	V	
		G	D	Y	S	U	I	P	H	M	Y	Y	F	J	V	Q	J	B	L	K	G	U	G	H	H	B	M	
EKRCO	k	J	S	R	C	E	Z	U	Q	K	D	O	Y	T	X	V	T	V	C	A	S	N	Q	P	G	E	C	
		L	T	Z	X	J	D	M	T	W	S	Q	O	O	V	B	R	D	L	R	L	L	H	X	X	D	T	
FLRCO	l	A	R	U	C	W	L	D	D	C	U	Q	D	X	F	L	C	B	K	D	B	E	C	H	X	D	G	
		Z	Y	I	X	T	B	P	Q	C	P	W	U	U	X	K	J	G	F	B	J	Z	P	P	F	H	Z	
GMRCO	m	V	A	Y	E	E	U	Z	H	W	R	W	V	V	P	V	D	V	M	G	E	N	J	W	V	U	U	
		N	A	F	I	J	L	E	A	X	G	Z	Y	Z	O	B	Y	D	Y	S	Y	L	G	L	K	E	F	
HNRCO	n	E	N	M	O	Q	J	P	U	M	V	K	G	W	Q	C	Z	W	K	R	I	I	X	M	J	A	C	
		F	S	J	H	Q	Q	H	N	P	W	Y	L	B	Z	I	N	F	F	P	O	P	D	D	I	X	T	
IORCO	o	L	N	S	W	E	A	M	I	A	U	U	V	W	V	B	L	E	M	B	O	S	P	X	F	R	R	
		W	S	U	S	J	E	N	C	H	P	Q	Y	B	A	E	L	V	Y	I	X	M	W	E	H	V	W	
JPRCO	p	S	G	O	W	C	J	L	V	M	H	Y	A	J	E	Z	G	F	Y	B	U	D	A	Z	L	O	Q	
		S	B	G	S	Y	Q	C	U	P	C	N	K	X	S	M	P	A	U	I	Z	D	U	U	T	C	L	
KQRCO	q	U	M	T	Z	T	O	V	T	B	D	K	W	H	A	C	H	Y	N	Y	O	B	N	P	I	H	R	
		G	I	E	B	G	J	T	J	Y	S	Y	A	F	M	I	I	T	I	V	X	K	M	X	S	R	W	
LRRCO	r	T	K	S	X	F	G	W	M	N	L	N	G	O	H	Y	M	K	H	P	G	W	I	E	B	E	L	
		C	P	U	L	O	F	V	O	Z	F	B	L	Q	G	R	W	E	K	T	T	J	Q	B	N	D	V	
MSRCO	s	A	B	L	Z	C	J	U	C	L	J	X	S	O	U	D	L	W	U	T	A	F	I	A	R	T	U	
		Z	R	Y	B	Y	Q	M	B	E	U	S	D	Q	T	X	L	F	X	U	S	E	Q	V	U	A	F	
			↓ OTSDP																									
NTRCO	t	S	N	G	X	A	Z	B	O	H	G	W	P	Y	G	Z	R	V										
		S	S	C	L	D	D	W	L	B	J	Z	M	P	N	M	M	D										

As pointed out once before, it is really unnecessary to make tabulations of pairs with formulas greater than $\overset{1}{\theta_1}\,\overset{14}{\theta_2}$ because of the reversible relation existing between pairs of the formula

$\overset{1}{\theta_1}\,\overset{15}{\theta_2}$ and $\overset{1}{\theta_1}\,\overset{13}{\theta_2}$, $\overset{1}{\theta_1}\,\overset{16}{\theta_2}$ and $\overset{1}{\theta_1}\,\overset{12}{\theta_2}$, and so on. Thus, for example, $\overset{1}{\text{A}}\,\overset{15}{\text{X}}$ is the same as $\overset{1}{\text{X}}\,\overset{13}{\text{A}}$; $\overset{1}{\text{B}}\,\overset{16}{\text{K}}$ is the same as $\overset{1}{\text{K}}\,\overset{12}{\text{B}}$, etc.

51. Study of tables and reconstruction of MCAL5.—Now comes the most difficult part of the analysis—that concerned with the reconstruction of MCAL5 from the interval tables. In the table of pairs with the formula $\overset{1}{\theta_1}\,\overset{4}{\theta_2}$, the letter T was indicated 16 times as the third interval successor of D (the pair DT = 16 occurrences), the most frequent pair in all the tables. According to the theory of solution, this meant that $\overset{1}{\text{D}}\,\overset{2}{.}\,\overset{3}{.}\,\overset{4}{\text{T}}$ was a sequence in MCAL5. This was assumed to be correct.

In the same table, the following possibilities for the third interval successor of T are noted (D can be omitted at once as a possibility, for a letter can appear but once in a sequence):

T---- A B E G J K O P Q R S U V W Y

According to theory, $\overset{1}{\text{T}}\,\overset{4}{\text{B}}$, with 12 occurrences, should be correct, but $\overset{1}{\text{T}}\,\overset{4}{\text{U}}$, with 10 occurrences, runs a very close second. How can one distinguish between them or in fact, between $\overset{1}{\text{T}}\,\overset{4}{\text{B}}$, $\overset{1}{\text{T}}\,\overset{4}{\text{U}}$, $\overset{1}{\text{T}}\,\overset{4}{\text{W}}$, and $\overset{1}{\text{T}}\,\overset{4}{\text{Y}}$? In such a relatively small amount of text a difference of three or four occurrences may not be significant.

Consider the relationship existing between the $\overset{1}{\theta_1}\,\overset{4}{\theta_2}$ table and the $\overset{1}{\theta_1}\,\overset{7}{\theta_2}$ table. Assuming both $\overset{1}{\text{D}}\,\overset{4}{\text{T}}$ and $\overset{1}{\text{T}}\,\overset{4}{\text{B}}$ to be correct, then the $\overset{1}{\theta_1}\,\overset{7}{\theta_2}$ table should show $\overset{1}{\text{D}}\,\overset{7}{\text{B}}$ as highest in frequency. If $\overset{1}{\text{T}}\,\overset{4}{\text{U}}$ is correct, then $\overset{1}{\text{D}}\,\overset{7}{\text{U}}$ should be highest in frequency. But upon reference to the table it will be seen that neither $\overset{1}{\text{D}}\,\overset{7}{\text{B}}$ nor $\overset{1}{\text{D}}\,\overset{7}{\text{U}}$ is of greatest frequency, for the pair $\overset{1}{\text{D}}\,\overset{7}{\text{O}}$ occurs 15 times. Which is the most probable sequence, $\overset{1}{\text{D}}\,\overset{7}{\text{B}}$, $\overset{1}{\text{D}}\,\overset{7}{\text{U}}$, or $\overset{1}{\text{D}}\,\overset{7}{\text{O}}$?

Now there is no reason why the data of two or more tables cannot be combined, providing the work is done correctly. For example, if $\overset{1}{\text{D}}\,\overset{4}{\text{T}}$ is correct, and if $\overset{1}{\text{T}}\,\overset{4}{\text{B}}$ is correct, then $\overset{1}{\text{D}}\,\overset{7}{\text{B}}$ must be correct, and the sum total obtained by adding their respective frequencies should be higher than that obtained by adding incorrect frequencies. The sum in this case is 20, for the frequency of TB is 12, plus that for DB, 8, equals 20. The following sums are noted:

$\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{A}} = \overset{1}{\text{T}}\,\overset{4}{\text{A}}\ (6) + \overset{1}{\text{D}}\,\overset{7}{\text{A}}\ (7) = 13$
D T B = T B (12) + D B (8) = 20
D T E = T E (6) + D E (4) = 10
D T G = T G (8) + D G (2) = 10
D T J = T J (7) + D J (6) = 13

$\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{K}} = \overset{1}{\text{T}}\,\overset{4}{\text{K}}\ (7) + \overset{1}{\text{D}}\,\overset{7}{\text{K}}\ (3) = 10$
D T O = T O (7) + D O (15) = 22
D T P = T P (8) + D P (4) = 12
D T Q = T Q (6) + D Q (4) = 10
D T R = T R (8) + D R (6) = 14

$\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{S}} = \overset{1}{\text{T}}\,\overset{4}{\text{S}}\ (8) + \overset{1}{\text{D}}\,\overset{7}{\text{S}}\ (6) = 14$
D T U = T U (10) + D U (1) = 11
D T V = T V (7) + D V (1) = 8
D T W = T W (9) + D W (2) = 11
D T Y = T Y (9) + D Y (4) = 13

According to these summations, the evidence seems to be in favor of $\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{O}}$, for it has a cumulative value of 22 occurrences, as against 20 for $\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{B}}$, and only 11 for $\overset{1}{\text{D}}\,\overset{4}{\text{T}}\,\overset{7}{\text{U}}$. It is to be recognized, of course, that a difference of only two or three units of frequency may not be significant at all, and such a contingency must continually be borne in mind throughout this work. But since some starting point must be established, in order that the process may be continued, the sequence $\overset{1}{\text{D}}\ \overset{4}{\text{T}}\ \overset{7}{\text{O}}$ will tentatively be assumed to be correct.

What about the sequence $\overset{1}{\text{D}}\ \overset{4}{\text{T}}\ \overset{7}{\text{O}}\ \overset{10}{\theta}$? For this determination, three corroborative sources of data are available, viz, the $\overset{1}{\theta_1}\ \overset{4}{\theta_2}$ table, the $\overset{1}{\theta_1}\ \overset{7}{\theta_2}$ table, and the $\overset{1}{\theta_1}\ \overset{10}{\theta_2}$ table. First, examine the $\overset{1}{\theta_1}\ \overset{4}{\theta_2}$ table to see what are the likely candidates for the position $\overset{1}{\theta}\ \overset{4}{\theta}$. Even considering only those whose frequencies are five or over, there are 12 candidates: B, C, F, H, J, K, L, Q, U, V, X, and Y. (It is to be noted that as a letter becomes firmly fixed in its position in the MCAL5 sequence, it can automatically be eliminated as a possible candidate for any other position. Thus, D, O, and T having tentatively been fixed into position, they may be eliminated as candidates for any other positions in the succeeding calculations. It is for this reason that $\overset{1}{\text{O}}\ \overset{4}{\text{D}}$ (frequency 6) is eliminated as a candidate in the attempt to continue the $\overset{1}{\text{D}}\ \overset{4}{\text{T}}\ \overset{7}{\text{O}}$ sequence.)

The calculations are as follows:

1 4 7 10		1 4			1 7			1 10			
D T O B	=	O B	(6)	+	T B	(8)	+	D B	(8)	=	22
D T O C	=	O C	(8)	+	T C	(8)	+	D C	(3)	=	19
D T O F	=	O F	(9)	+	T F	(6)	+	D F	(6)	=	21
D T O H	=	O H	(5)	+	T H	(5)	+	D H	(4)	=	14
D T O J	=	O J	(5)	+	T J	(5)	+	D J	(2)	=	12
D T O K	=	O K	(5)	+	T K	(5)	+	D K	(2)	=	12
D T O L	=	O L	(5)	+	T L	(3)	+	D L	(7)	=	15
D T O Q	=	O Q	(11)	+	T Q	(6)	+	D Q	(7)	=	24
D T O U	=	O U	(5)	+	T U	(10)	+	D U	(1)	=	16
D T O V	=	O V	(6)	+	T V	(5)	+	D V	(2)	=	13
D T O X	=	O X	(6)	+	T X	(5)	+	D X	(5)	=	16
D T O Y	=	O Y	(8)	+	T Y	(11)	+	D Y	(11)	=	30

Very clearly, the sequence is indicated as $\overset{1}{\text{D}}\ \overset{4}{\text{T}}\ \overset{7}{\text{O}}\ \overset{10}{\text{Y}}$. For the next position, there are 14 candidates, according to the $\overset{1}{\theta_1}\ \overset{4}{\theta_2}$ table. They are A, B, G, H, I, K, L, M, N, P, Q, R, V, and W; four corroborative sources of data are available, viz, the $\overset{1}{\theta_1}\ \overset{4}{\theta_2}$, $\overset{1}{\theta_1}\ \overset{7}{\theta_2}$, $\overset{1}{\theta_1}\ \overset{10}{\theta_2}$, and $\overset{1}{\theta_1}\ \overset{13}{\theta_2}$ tables. The calculations are as follows:

1 4 7 10 13		1 4			1 7			1 10			1 13			
D T O Y A	=	Y A	(10)	+	O A	(8)	+	T A	(2)	+	D A	(3)	=	23
D T O Y B	=	Y B	(6)	+	O B	(6)	+	T B	(2)	+	D B	(6)	=	20
D T O Y G	=	Y G	(5)	+	O G	(4)	+	T G	(4)	+	D G	(2)	=	15
D T O Y H	=	Y H	(5)	+	O H	(3)	+	T H	(1)	+	D H	(4)	=	13
D T O Y I	=	Y I	(13)	+	O I	(4)	+	T I	(6)	+	D I	(3)	=	26
D T O Y K	=	Y K	(8)	+	O K	(3)	+	T K	(3)	+	D K	(7)	=	21
D T O Y L	=	Y L	(15)	+	O L	(8)	+	T L	(7)	+	D L	(11)	=	41
D T O Y M	=	Y M	(8)	+	O M	(1)	+	T M	(3)	+	D M	(5)	=	17
D T O Y N	=	Y N	(5)	+	O N	(3)	+	T N	(5)	+	D N	(2)	=	15
D T O Y P	=	Y P	(5)	+	O P	(3)	+	T P	(8)	+	D P	(6)	=	22
D T O Y Q	=	Y Q	(7)	+	O Q	(7)	+	T Q	(6)	+	D Q	(2)	=	22
D T O Y R	=	Y R	(6)	+	O R	(4)	+	T R	(6)	+	D R	(6)	=	22
D T O Y V	=	Y V	(8)	+	O V	(7)	+	T V	(10)	+	D V	(4)	=	29
D T O Y W	=	Y W	(5)	+	O W	(5)	+	T W	(6)	+	D W	(6)	=	22

Again the evidence is very clear. The sequence is $\overset{1}{\text{D}}\ \overset{4}{\text{T}}\ \overset{7}{\text{O}}\ \overset{10}{\text{Y}}\ \overset{13}{\text{L}}$.

The calculations for the succeeding placements were made in the same manner, and in the majority of cases the evidence in favor of each placement was very clear-cut. Only in two or three cases was there doubt, and these were determined by special methods which suggested themselves in each case. Suffice it to say that the entire MCAL5 was reconstructed from the ten test messages, and was found to be as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
D	P	G	T	B	Z	O	H	R	Y	M	S	L	A	J	I	W	C	K	U	Q	F	N	V	X	E

What the initial letter of the sequence is, in other words, which letter should be placed under A of the normal alphabet in order to give a complete CAL5 is not indicated by the sequence itself. But it has been found that it makes no difference with what letter the sequence begins, for it expresses only a relative relationship between the letters composing it. Hence, CAL5 may be written as follows:

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

In fact, the mixed sequence may be set under the normal alphabet at any one of the 26 points of coincidence, with similar results so far as encipherment or decipherment is concerned. The reader may prove this to his own satisfaction by trying out two alphabets based upon the same sequence but beginning at different points.

52. **Reconstructing the table of basic cipher-text sequences.**—Having at last reconstructed the sequence of MCAL5, the next step was to proceed at once to the reconstruction of the table of basic cipher-text sequences. It has been stated that for this purpose only a knowledge of RFS and MCAL5 is necessary. Following the procedure outlined in section VII, the first sequence of the table was obtained by setting CAL5 above the RFS so that A of NCAL5 was opposite T, the first letter of RFS. Thus:

↓
NCAL5 -- |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 . . .
MCAL5 -- |D P G T| B Z O H R Y M S L A J I W C K U Q F N V X E D P G . . .
RFS -- T Y O E U M X D F J Q V K W B N S H C I L R Z A G P

Assuming that the current enters CW5 from the first contact of BS5 (A of NCAL5), the cipher equivalent would be E_c, since the A current is converted into a D current, and D is then opposite E of RFS, as shown above.

Sliding CAL5 one space to the left, and still assuming that the current enters CW5 from the first contact of BS5 (now B of NCAL5), the cipher equivalent would be B_c, as shown below.

↓
NCAL5 -- A |B C E D F G H I J K L M N O P| Q R S T U V W X Y Z A B C . . .
MCAL5 -- D |P G T B Z O H R Y M S L A J I| W C K U Q F N V X E D P G . . .
RFS -- T Y O E U M X D F J Q V K W B N S H C I L R Z A G P

This gives the pair of letters E B as the beginning of the first basic sequence. Continuation of the process results in establishing the following sequence:

Basic sequence 1---- E B U S A L F T J N O D P W R I X V C Y Z Q H G P M

It is to be noted that in establishing this sequence the current is always assumed to enter CW5 from the first contact of BS5. It would of course be possible to reconstruct all the sequences by the same process, but there is a much shorter method.

Having reconstructed one of the basic cipher-text sequences, and having already at hand RFS, the reconstruction of the entire table followed very speedily, according to the procedure detailed in paragraph 32, section VII. The entire table is as follows:

TABLE 9

	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
1	E	B	U	S	A	L	F	T	J	N	O	D	P	W	R	I	X	V	C	Y	Z	Q	H	G	P	M
2	N	M	H	G	R	J	Y	Q	S	E	F	T	B	Z	L	D	K	I	O	A	V	C	P	T	X	U
3	X	C	P	Z	Q	O	V	H	U	J	Y	N	A	R	F	W	L	E	G	K	I	T	Y	D	M	S
4	I	T	A	V	E	K	C	M	Q	O	S	G	Z	J	B	R	U	P	W	L	Y	O	F	X	H	D
5	Y	G	K	U	W	I	X	V	E	H	P	A	Q	N	Z	M	T	B	R	O	E	J	D	C	F	L
6	P	W	M	B	L	D	K	U	C	T	G	V	S	A	X	Y	N	Z	E	U	Q	F	I	J	R	O
7	B	X	N	R	F	W	M	I	Y	P	K	H	G	D	O	S	A	U	M	V	J	L	Q	Z	E	T
8	D	S	Z	J	B	X	L	O	T	W	C	P	F	E	H	G	M	X	K	Q	R	V	A	U	Y	N
9	H	A	Q	N	D	R	E	Y	B	I	T	J	U	C	P	X	D	W	V	Z	K	G	M	O	S	F
10	G	V	S	F	Z	U	O	N	L	Y	Q	M	I	T	D	F	B	K	A	W	P	X	E	H	J	C
11	K	H	J	A	M	E	S	R	O	V	X	L	Y	F	J	N	W	G	B	T	D	U	C	Q	I	P
12	C	Q	G	X	U	H	Z	E	K	D	R	O	J	Q	S	B	P	N	Y	F	M	I	V	L	T	W
13	V	P	D	M	C	A	U	W	F	Z	E	Q	V	H	N	T	S	O	J	X	L	K	R	Y	B	I
14	T	F	X	I	G	M	B	J	A	U	V	K	C	S	Y	H	E	Q	D	R	W	Z	O	N	L	K
15	J	D	L	P	X	N	Q	G	M	K	W	I	H	O	C	U	V	F	Z	B	A	E	S	R	W	Y
16	F	R	T	D	S	V	P	X	W	B	L	C	E	I	M	K	J	A	N	G	U	H	Z	B	O	Q
17	Z	Y	F	H	K	T	D	B	N	R	I	U	L	X	W	Q	G	S	P	M	C	A	N	E	V	J
18	O	J	C	W	Y	F	N	S	Z	L	M	R	D	B	V	P	H	T	X	I	G	S	U	K	Q	A
19	Q	I	B	O	J	S	H	A	R	X	Z	F	N	K	T	C	Y	D	L	P	H	M	W	V	G	E
20	L	N	E	Q	H	C	G	Z	D	A	J	S	W	Y	I	O	F	R	T	C	X	B	K	P	U	V
21	S	U	V	C	I	P	A	F	G	Q	H	B	O	L	E	J	Z	Y	I	D	N	W	T	M	K	R
22	M	K	I	L	T	G	J	P	V	C	N	E	R	U	Q	A	O	L	F	S	B	Y	X	W	Z	H
23	W	L	R	Y	P	Q	T	K	I	S	U	Z	M	V	G	E	R	J	H	N	O	D	B	A	C	X
24	R	Z	O	T	V	Y	W	L	H	M	A	X	K	P	U	Z	Q	C	S	E	F	N	G	I	D	B
25	A	E	Y	K	O	B	R	C	X	G	D	W	T	M	A	V	I	H	U	J	S	P	L	F	N	Z
26	U	O	W	E	N	Z	I	D	P	F	B	Y	X	G	K	L	C	M	Q	H	T	R	J	S	A	G

The specific use to which this table was put will be explained later, but the general use may here be indicated. Suppose that after MCAL5 has been reconstructed from the data afforded by a few dispatches in which the NCAL5$_c$ equivalents had to be determined, a few more dispatches are intercepted. It is obvious that it will be unnecessary to set down the NCAL5$_c$ equivalents of the text of the new messages in order to establish repetitions in lines. The basic cipher-text sequences can be used directly on the lines of cipher text themselves, and thus, repetitions can be determined.

53. Solution of the first line of cipher text.—All of the analysis accomplished thus far has for its purpose the ultimate reduction of the individual lines of cipher text into single-mixed alphabet substitution ciphers. This purpose is now to be achieved by the application of the appropriate basic cipher-text sequences to the cryptograms.

The first step is to assign, to the letters of each line of text, numbers indicating the basic sequences to which they belong. This will show what repetitions occur within each line. The process when applied to Dispatch No. 1, for example, yields the following:

DISPATCH NO. 1

Key: AGRAM (Effective key: AGRBN)

CW5	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
LAW CW1 CW3 CW5 RAW																										J 18
BHRCO	N	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S
	7	5	22	8	19	5	18	23	16	17	23	21	5	18	18	8	23	5	19	22	23	15	23	5	22	8
CIRCO	U	F	C	D	S	U	F	M	O	V	K	C	N	K	Y	N	N	G	A	U	W	Y	L	I	Q	Z
	1	10	13	6	11	6	13	24	1	6	24	9	13	16	19	12	16	16	15	11	19	13	14	13	19	24

Etc. Etc. Etc.

The entire dispatch was then treated in the same manner. Referring now to the first complete line of text, after about 45 minutes experiment, the following decipherment was obtained:

																									J 18 P
N	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S
7	5	22	8	19	5	18	23	16	17	23	21	5	18	18	8	23	5	19	22	23	15	23	5	22	8
r	e	s	i	d	e	n	t	o	f	t	h	e	n	n	i	t	e	d	S	t	a	t	e	s	i
													(Ū)												

Note that the encipherer made an error in regard to the U of United. The analysis showed that the cipher letter X was to be assigned the number 18, which is the same as that for the next letter H. But the decipherment shows that the letter X should not belong to the same basic sequence as does the letter H, for $X_c = U_p$ and $H_c = N_p$. However, the presence of this error did not retard the decipherment.

Now it is obvious that the deciphered clear text of each line will suggest assumptions for deciphering the next line, with the aid given by the indicated repetitions. In this case it was somewhat unfortunate that only one letter of the next word was given, I, but it nevertheless offered a clue to the word. It seemed that the word should be IS, or IN, or should at least begin with the syllable IS or IN, possibly ID. Experiment soon showed, however, that the word was INVITATION. Continuation of the process of decipherment as here outlined yielded the five lines of decipherment shown below:

CW5	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	
																										J	Line g
																										18	
LAW CW1 CW3 CW5 RAW																										P	
BHRCO	N	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S	Line h
	7	5	22	8	19	5	18	23	16	17	23	21	5	18	18	8	23	5	19	22	23	15	23	5	22	8	
	r	e	s	i	d	e	n	t	o	f	t	h	e	U	n	i	t	e	d	S	t	a	t	e	s	i	
CIRCO	U	F	C	D	S	U	F	M	O	V	K	C	N	K	Y	N	N	G	A	U	W	Y	L	I	Q	Z	Line i
	1	16	13	6	11	6	13	24	1	6	24	9	13	16	19	12	16	16	15	11	19	13	14	13	19	24	
	n	v	i	t	a	t	i	o	n	t	o	d	i	s	c	u	s	s	P	a	c	i	f	i	c	O	
DJRCO	U	T	L	W	B	Y	D	G	O	W	K	H	R	X	T	C	J	C	S	V	G	J	J	F	Y	V	Line j
	1	24	6	7	14	9	20	25	1	25	24	13	1	9	5	24	13	20	25	8	24	6	10	9	5	10	
	c	e	a	n	p	o	l	i	c	i	e	s	c	o	m	e	s	l	i	k	e	a	b	o	m	b	
EKRCO	J	S	R	C	E	Z	U	Q	K	D	O	Y	T	X	V	T	V	C	A	S	N	Q	P	G	E	C	Line k
	11	1	2	20	9	20	3	21	7	1	21	20	19	9	15	18	9	20	15	18	17	11	1	26	1	3	
	t	o	J	a	p	a	n	w	h	o	w	a	s	p	r	e	p	a	r	e	d	t	o	c	o	n	
FLRCO	A	R	U	C	W	L	D	D	C	U	Q	D	X	F	L	C	B	K	D	B	E	C	H	X	D	G	Line l
	4	7	12	20	24	24	20	12	8	17	5	7	6	10	3	24	11	3	11	20	10	5	4	23	8	5	
	s	i	d	e	r	r	e	d	u	c	t	i	o	n	a	r	m	a	m	e	n	t	s	b	u	t	
GMRCO	V	A	Y	E	E	U	Z	H	W	R	W	V	V	P	V	D	V	M	G	E	N	J	W	V	U	U	Line m
	21	11	18	11	9	6	18	5	15	18	20	23	18	18	15	19	9	17	18	15	17	6	15	20	26	21	
HNRCO	E	N	M	O	Q	J	P	U	M	V	K	G	W	Q	C	Z	W	K	R	I	I	X	M	J	A	C	Line n
	20	9	13	3	15	14	26	14	18	6	24	26	17	17	26	6	4	3	8	12	6	4	3	17	25	3	
IORCA	L	N	S	W	E	A	M	I	A	U	U	V	W	V	B	L	E	M	B	O	S	P	X	F	R	R	Line o
	15	9	16	7	9	19	15	9	24	17	9	23	17	25	10	22	6	17	22	4	15	20	2	9	24	16	
JPRCO	S	G	O	W	C	J	L	V	M	H	Y	A	J	E	Z	G	F	Y	B	U	D	A	Z	L	O	Q	Line p
	10	2	25	7	4	14	10	11	18	7	11	6	11	23	21	11	22	1	22	11	5	23	22	5	18	12	
KQRCO	U	M	T	Z	T	O	V	T	B	D	K	W	H	A	C	H	Y	N	Y	O	B	N	P	I	H	R	Line q
	1	13	22	26	23	8	22	6	26	1	24	1	8	22	26	25	12	23	4	4	23	14	1	13	9	16	
LRRCO	T	K	S	X	F	G	W	M	N	L	N	G	O	H	Y	M	K	H	P	G	W	I	E	B	E	L	Line r
	16	25	16	8	1	15	16	24	22	11	19	26	7	14	19	26	8	26	10	9	19	24	7	24	1	23	
MSRCO	A	B	L	Z	C	J	U	C	L	J	X	S	O	U	D	L	W	U	T	A	F	I	A	R	T	U	Line s
	4	6	6	26	4	14	3	22	16	9	26	14	7	15	9	22	4	6	26	17	4	24	26	21	14	21	
NTRCO	S	N	G	X	A	Z	B	O	H	G	W	P	Y	G	Z	R	V										Line t
	9	14	21	4	1	2	26	13	20	21	5	12	3	21	2	10	6										

It is obvious that one could proceed along the lines followed, and decipher the rest of the dispatch in the same more or less laborious manner, for the solution of each line would still present the difficulties inherent in analyzing a single-mixed alphabet substitution cipher only 26 letters in length. Furthermore, the solution of one dispatch would carry with it no suggestions or aids for the solution of any other, except that of having the same MCAL5 and table of basic cipher-text sequences applicable. But previous experience teaches the cryptanalyst that once an entering wedge has been forced into the apparently impregnable wall of cryptographic secrecy, the whole structure may be quickly undermined by judicious use of such instruments, devices, and methods as his ingenuity can discover.

The succeeding sections will give in detail some of the more important methods which were developed by the author after these first five lines of text had been deciphered. Their usefulness as aids in facilitating analysis of subsequent dispatches will become apparent as they are being set forth.

Section XI

FURTHER STEPS IN ANALYSIS

54. **Reconstruction of Alphabet 1.**—In each column of cipher text, when the dispatch is arranged in horizontal lines of 26 letters each, the cipher letters represent encipherments at exactly the same position of CW5. In successive horizontal lines, only CW1 has undergone displacement one step, providing the "key" has not been such as to displace CW3 also. In Dispatch No. 1, CW3 remains stationary until the very last line of text, hence only the successive displacements of CW1 need be considered in studying the successive lines up to the last one.

Now note that in column C of Dispatch No. 1, for example, the initial letter of the i and j lines is U_c in both cases. Decipherment showed that in the first case, $U_c = N_p$; in the second, $U_c = C_p$. Only a single displacement of CW1 has brought this about, for CW2, 3, 4, and 5 are in exactly similar positions in the two cases. This means, in other words, that the current originated by N in the first case enters the fixed contact in BS2 at exactly the same point as the current originated by C in the second case, for both of them must of necessity have traversed exactly the same path through CW2, 3, 4, and 5 in order to produce U_c at RFS. The two positions of NAL1 may be diagrammatically illustrated as follows:

									↓																		
LFS	B	S	X	R	Z	T	K	D	N	G	C	H	M	V	O	L	Y	Q	E	U	P	W	J	A	I	F	For line i
NCAL1	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
										↓																	
LFS	B	S	X	R	Z	T	K	D	N	G	C	H	M	V	O	L	Y	Q	E	U	P	W	J	A	I	F	For line j
NCAL1	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	

In the first case N_p is over Q of NAL1; in the second case C_p is over T of NAL1. For convenience in reference, letters found in this way will be designated hereafter as the plain-text NAL1 equivalents. Between the two cases CW1 has advanced one interval. Hence T follows Q in MAL1, that is, QT forms a pair of sequent letters in MAL1. Searching for other cases of a similar nature, in loci Ki and Kj it is found that O_c occurs in the two lines concerned as superimposed loci: in the first instance it represents N_p, in the second C_p. Reference to the positions of NAL1 will show that this, however, is but a corroboration of the first case above described, showing the sequence QT to occur in MAL1. In loci Mi and Mj the letter K_c occurs, in the first instance representing O_p, in the second E_p. Referring to the diagram of alphabets immediately above, it will be seen that in the first case the $NAL1_p$ equivalent of O_p is W, and that for E_p is B in the second instance. Hence WB forms a sequence in MAL1.

In loci Ph, Pj, and Pk, the letter X_c occurs. Attention was called to the fact that the first-named X is an error; hence, it cannot be considered in establishing values in MAL1. But

X_c in locus Pj represents O_p, and in locus Pk, P_p. The two positions of NAL1 in these cases are as follows:

LFS-------	B S X R Z T K D N G C H M V O L Y Q E U P W J A I F	For line <u>i</u>
NCAL1----	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I	
LFS-------	B S X R Z T K D N G C H M V O L Y Q E U P W J A I F	For line <u>k</u>
NCAL1----	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J	

In the first case the $NAL1_p$ equivalent of O_p is X; in the second case, the $NAL1_p$ equivalent of P_p is E. It therefore follows that XE forms in sequence in MAL1. The following additional sequences in MAL1 are established by analyzing these five lines of deciphered text of Dispatch No. 1:

C_c {locus Fk = A_p; locus Fl = E_p} giving sequence HD in MAL1

D_c {locus Ij = L_p; locus Il = E_p} giving sequence Y.D in MAL1

U_c {locus Lh = F_p; locus Ll = C_p} giving sequence G...V in MAL1

C_c {locus Rj = E_p; locus Rl = R_p} giving sequence B.O in MAL1

C_c {locus Tj = L_p; locus Tk = A_p} giving sequence YH in MAL1

A_c {locus Ui = P_p; locus Uk = R_p} giving sequence C.N in MAL1

Thus far the following sequences have been established:

QT	XE	HD	Y.D	B.O
WB	YH	C.N	G...V	

By virtue of the letter common to the two pairs YH and HD, they may be joined, making YHD. Confirmation is seen in the sequence Y.D, established independently. No other unions can be made.

It is obvious that if there were a sufficient number of repetitions of cipher letters in the columns of these five lines of text, the entire sequence could be established. But there is, in reality, a way of overcoming this insufficiency of repetition. The process is somewhat complicated, but useful.

Suppose we approach the problem from a somewhat novel viewpoint. Take the case of $R_p = N_c$ in locus Ch. If there were another R_p in locus Ah, what would the cipher letter be? Reference to the table of basic sequences is made. Applying that sequence in which N occupies the first position (to correspond with column A of the dispatch) it is found that B_c would be the letter. That is, if there were an R_p in locus Ah, it would equal B_c.

Now if there were a B_c in any one of the loci Ag, Ai, Aj, Ak, or Al (i.e., within the body of already deciphered text) its plain-text equivalent would, of course, be known. Now there is no B_c in any of these loci, but if it were present, and if its plain-text equivalent were repeated in any other column of any of these five lines, then, of course, a coincidence of the repeated plain-text letter's cipher equivalent with a letter of the basic sequence initiated by B would

occur. Therefore, let this basic sequence initiated by B be applied to the five lines of deciphered text to see if any such coincidences can be found. Thus:

	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	
BHRCO----	<u>N</u>	U	T	X	H	V	Z	S	L	U	M	L	Z	X	H	X	H	O	H	Y	B	R	C	L	M	S	Line <u>h</u>
	r	e	s	i	d	e	n	t	o	f	t	h	e	U	n	i	t	e	d	S	t	a	t	e	s	i	
	<u>N</u>	R	F	W	M	I	Y	P	K	H	G	D	O	S	A	U	M	V	J	L	Q	Z	E	T	B	X	
CIRCO----	U	F	C	D	S	U	F	M	O	V	K	C	N	K	Y	N	N	G	A	U	W	Y	L	I	Q	Z	Line <u>i</u>
	n	v	i	t	a	t	i	o	n	t	o	d	i	s	c	u	s	s	P	a	c	i	f	i	c	O	
	N	R	F	W	M	I	Y	P	K	H	G	D	O	S	A	U	M	V	J	L	Q	Z	E	T	B	X	
DJRCO----	U	T	L	<u>W</u>	B	Y	D	G	O	W	K	H	R	X	T	C	J	C	S	V	G	J	J	F	Y	V	Line <u>j</u>
	c	e	a	<u>n</u>	p	o	l	i	c	i	e	s	c	o	m	e	s	l	i	k	e	a	b	o	m	b	
	N	R	F	<u>W</u>	M	I	Y	P	K	H	G	D	O	S	A	U	M	V	J	L	Q	Z	E	T	B	X	
EKRCO----	J	S	R	C	E	Z	U	Q	<u>K</u>	D	O	Y	T	X	V	T	V	C	A	S	N	Q	P	G	E	C	Line <u>k</u>
	t	o	J	a	p	a	n	w	<u>h</u>	o	w	a	s	p	r	e	p	a	r	e	d	t	o	c	o	n	
	N	R	F	W	M	I	Y	P	<u>K</u>	H	G	D	O	S	A	U	M	V	J	L	Q	Z	E	T	B	X	
FLRCO----	A	<u>R</u>	U	C	W	L	D	D	C	U	Q	<u>D</u>	X	F	L	C	B	K	D	B	E	C	H	X	D	G	Line <u>l</u>
	s	<u>i</u>	d	e	r	r	e	d	u	c	t	<u>i</u>	o	n	a	r	m	a	m	e	n	t	s	b	u	t	
	N	<u>R</u>	F	W	M	I	Y	P	K	H	G	<u>D</u>	O	S	A	U	M	V	J	L	Q	Z	E	T	B	X	

The following coincidences are noted:

R_c in locus Dl ($= I_p$) D_c in locus Nl (also $= I_p$)
W_c in locus Fj ($= N_p$) K_c in locus Kk ($= H_p$)

That is, B_c equals, successively in loci Ah, Aj, Ak, and Al, the letters R_p, N_p, H_p, and I_p.

Determining the plain-text normal-alphabet converted equivalents, as before, for the successive displacements of AL1, the sequence K.RVJ is obtained.

Take the second letter of line h, viz, $U_c = E_p$. If E_p occurred in locus Ah, its equivalent would be Y_c. Applying the basic sequence in which Y is the initial letter to the lines of deciphered text, the following coincidences are found:

Q_c in locus Ml ($= T_p$) and T_c in locus Qj ($= M_p$).

That is, Y_c equals successively in loci Ah, Aj, and Al, the letters E_p, M_p, and T_p.

Determining the plain-text normal-alphabet converted equivalents, as before, for the successive displacements of AL1, the sequence Z.V.Q is obtained.

When all of the text is analyzed in the same manner, the results shown in the table below are found. In this table the top line gives the cipher letters that would result if the plain-text letters under the corresponding cipher letters occurred in loci Ag, Ah, Ai, Aj, Ak, and Al.

TABLE 10

	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
g															P											
h		R		I		O				A			S		N		D		H				T		E	F
i			U		N	S	V	D		P	A					T	C	O		F		I				
j	I	N		K	C		B	O				L				A		E		P		S			M	
k		H			O			P		R	T	A		J	E		S		W		C			N	.	D
l		I	D	U			N		S		M	E				O		R						A	T	C

Determining the plain-text normal-alphabet converted equivalents for each placement of NAL1, the following sequences are established:

	Sequence in MAL1		Sequence in MAL1
For B_c(R.NHI) :	K.RVJ	For O_c(PN..E) :	AP..C
For C_c(U..D) :	B..S	For Q_c(DC.S) :	OS.L
For D_c(I.K.U) :	F.P.E	For R_c(OE.R) :	WB.O
For E_c(NCO) :	QTY	For S_c(H..W) :	S..F
For F_c(OS) :	VJ	For T_c(FP) :	HD
For G_c(VB.N) :	VJ.T	For V_c(IS) :	GK
For H_c(DOP) :	PXE	For X_c(NA) :	SI
For J_c(AP.R) :	EC.N	For Y_c(E.M.T) :	Z.V.Q
For K_c(A.TM) :	F.PX	For Z_c(F..DC) :	G..RV
For L_c(LAE) :	YHD		

Assembling and joining sequences, the following result is obtained:

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

The entire sequence of MAL1, with the exception of two letters, has been reconstructed. The two missing letters are M and U, which must be inserted between B and O, and C and N. Only two possibilities exist, BMO or BUO, and CUN or CMN. The exact placements were easily found later by trial on text, and the completed sequence was established as follows:

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

This sequence is, of course, the converted equivalent of the real MAL1, and in order to produce the latter it is only necessary to make use of the enciphering-deciphering relationship existing between such alphabets. By setting the sequence under the normal alphabet (the first alphabet below) and finding reciprocal equivalents, the second alphabet is obtained:

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
E C U N G K Z R V J Q T Y H D W B M O S I L F A P X } Converted equivalent of MAL1

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
X Q B O A W E N U J F V R D S Y K H T L C I P Z M G } Equivalent of MAL1

This equivalent of the real MAL1 (it is only an equivalent because it may not coincide letter-for-letter with the real MAL1, though it will work just as well) may be used for enciphering or deciphering by means of the sliding strips.

55. **Using the reconstructed Alphabet 1 as an aid to further decipherment.** Once Alphabet 1 has been reconstructed in the manner described above, from a few lines of deciphered text, this alphabet may be employed to aid in the further decipherment of the dispatches. To illustrate the method, consider the p line of Dispatch No. 1, in which, as shown by the numbers beneath, the 8th, 11th, 13th, 16th, and 20th letters represent the same plain-text letter. One of the cipher

equivalents, U, in locus Vp, also appears in the same column, line i, where it represents A_p. The diagrams of the position of Alphabet 1 for the two cases are as follows:

LFS....	B	S	X	R	Z	T	K	D	N	G	C	H	M	V	O	L	Y	Q	E	U	P	W	J	A	I	F
AL1....	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	U	J	F	V	R	D	S	Y	K	H	T	L	C	I	P	Z	M	G	X	Q	B	O	A	W	E	N
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

LFS....	B	S	X	R	Z	T	K	D	N	G	C	H	M	V	O	L	Y	Q	E	U	P	W	J	A	I	F
AL1....	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Y	K	H	T	L	C	I	P	Z	M	G	X	Q	B	O	A	W	E	N	U	J	F	V	R	D	S
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

In the first case, A_p in the LFS is over F of NAL1 which is converted into W of MAL1, and W is then opposite the fifteenth fixed contact of BS2. Since the cipher letter U is the same for both cases, it means that in the second case the current must enter CW2 at exactly the same point as it does in the first case. This will be at D of NAL1, which is the conversion equivalent of N of NAL1, and the latter is under I of LFS. The letter I is, therefore, the plain-text letter that U_c represents in the second case. Hence, the 8th, 11th, 13th, 16th, and 20th letters in line p all represent I_p. No assumptions based upon frequency were necessary, the results being positive and definite when Alphabet 1 has been reconstructed. The relations between all similar letters in columns can likewise be established. Thus, decipherment is considerably facilitated.

56. **Reconstructing a single-alphabet equivalent of Alphabets 2, 3, and 4.**—It will now be shown how the subsequent decipherment of the message can be still more facilitated by reconstructing a single alphabet which will serve to give all the final results that the combined effect of the interaction of Alphabets 2, 3, and 4 produces. It will be obvious that providing no displacement of CW2, 3, or 4 occurs during the encipherment of a message a current entering any given LHC of CW2 will always emerge from the same RHC of CW4. Hence, so far as the results in the case of each single message are concerned, Alphabets 2, 3, and 4 act as a single unit. Now consider the encipherment of a message of say 300 letters, during which CW2, 3, and 4 undergo no displacement. The different cipher equivalents of the same letter in each column will be due only to the displacement of CW1. If Alphabets 1 and 5 have already been reconstructed, it should be possible to construct a single alphabet which will be the resultant of the interaction of Alphabets 2, 3, and 4. Such an equivalent alphabet will, of course, have a rather limited application, being applicable only to that one message from which it has been reconstructed and then only to that portion of the message during the encipherment of which no displacement of CW2, 3, or 4 occurs. Within these limits, however, it will often be useful in hastening decipherment.

The process of reconstruction is as follows:

Set Alphabets 1 and 5 in positions to correspond to their respective positions when the letter N_c in locus Ch of Dispatch No. 1 was enciphered, and between them place the normal alphabet, set at the proper letter so far as the setting of CW3 was concerned. Thus:

```
                            ↓
LFS--------       B S X R Z T K D N G C H M V O L Y Q E U P W J A I F
                 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 G H I...
AL1--------
                 W E N U J F V R D S Y K H T L C I P Z M G X Q B O A W E N U...
Equivalent       P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S...
of AL2-3-4-
                 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...
AL5--------
                 D P G T B Z O H R Y M S L A J I W C K U Q F N V X E D P G T...
RFS--------          T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
                                                   ↑
```

The case under discussion is that where R_p equals N_c. R in LFS is over K of NAL1, which is converted into F of MAL1, but F of NAL1 is then opposite P of the normal component of the single-alphabet equivalent of AL2-3-4, hereafter abbreviated NEAL2-3-4. Now N of RFS is under R of NAL5 and R was produced by the conversion of I of NAL5 into R of MAL5. It will be seen that in order to enter NAL5 at I, the current had to emerge from X of NEAL2-3-4. It follows, therefore, that P of NEAL2-3-4 is converted into X, and this letter may be written under P in NEAL2-3-4. Thus the position of a letter of MEAL2-3-4 has been determined.

By tracing other letters through in the same manner, using only the first two lines of deciphered material, the following additional placements in MEAL2-3-4 are determined:

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

This reconstructed MEAL2-3-4 will very greatly facilitate the decipherment of all the succeeding lines up to that in which CW3 has advanced, whereupon a new MEAL2-3-4 becomes effective.

57. **Application of foregoing principles to another dispatch.**—Having shown how MEAL2-3-4 may be reconstructed from but two lines of deciphered text, the use of such a reconstructed alphabet in deciphering further material will now be demonstrated, using Dispatch No. 2. The first two lines, deciphered by the application of basic principles (indication of repetitions and solution of single-mixed alphabet lines) are as follows:

Key: COBAN

```
         B J E N F C A D D A Y G K N S F R B H W L U K J P Q–Cipher
DPBBO--  P L G T N Y E P Q H M K Z D F Y M G K H P A J H Y K–NCAL5c equiv.
         z e p p l i n c o m p a n y a c c e p t a l l g e n–Plain

         U Q I S A H S V I H S W D T I D Y A B J G T K K M Y–Cipher
EQBBO--  F M W U C X X T C B B Z U O I X S P H D T W J K E B–NCAL5c equiv.
         e r a l c o m p r e s s i o n r e q u i r e m e n t–Plain
```


From these two lines the following MEAL2-3-4 can be reconstructed:

```
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
  Y H   V   Q N   T S   O E W   U R P A J B K L M
```

Applying this reconstructed alphabet, in conjunction with the other alphabets, to the next line of cipher text, the following decipherment is obtained:

```
X O L D Y N V H C B Q T J O N I Y X J M J D O D T B
S A N D A R – A N X I – U S T – P R – C – – D A S S
```

The missing letters are easily inserted by context, and at the same time the letters lacking in previously incomplete MEAL2-3-4 can be inserted.

It becomes apparent, therefore, that when only a very few lines, say 4 or 5, of one message have been deciphered by basic processes, the decipherment of all the rest of the messages may be attained almost directly, as a result of the reconstruction of MCAL5, MCAL1, and MEAL2-3-4.

Section XII

SOLUTION WITHOUT PRELIMINARY ANALYSIS OF ANY LINE OF TEXT

58. **Introductory statement.**—In the preceding paragraphs it was shown how the decipherment of a message could be facilitated after only 2 or 3 lines of text of the dispatch had been solved more or less laboriously by first principles. It will now be shown how a message can be solved as a unit without a preliminary decipherment of several lines of text. The procedure is so novel that it has been considered necessary to devote a separate section to its explanation, although it is not very complex. In brief, the procedure is as follows: The letters of the message are all distributed or grouped into but 26 classes or categories corresponding to the 26 basic sequences. By virtue of a relationship existing between basic cipher-text sequences, to be explained, the solution of a single letter in each category yields the equivalents of all other letters in that category; and the solution of but three or four categories yields solution of all the other categories.

59. **Grouping the letters of the text into categories.**—When the table of basic cipher-text sequences has been completely reconstructed it becomes possible to determine the position occupied in the table by every cipher letter of the cryptographic text of a dispatch. Now since there are but 26 basic cipher-text sequences in the table, it follows that all of the elements of the cryptographic text can be allocated to but 26 different classes or categories. Thus, if the successive sequences are numbered arbitrarily from 1 to 26, then a certain number of cipher letters will fall into class 1, another number into class 2, and so on. For example, taking the first *column* of the cipher-text of Dispatch No. 1, reading NUUJAVELSUTAS, and referring to column C of table 9, the reconstructed table of basic cipher-text sequences applying to the dispatches submitted for solution, the letter N is found in the seventh basic sequence, the letter U in the first, the letter J in the eleventh, and so on. Taking the second *column* of the cipher text reading UFTSRANNGMKB, and referring to column D of table 9, the letter U is found in the fifth basic sequence, the letter F in the tenth, the letter T in the twenty-fourth, and so on. Let these basic-sequence numbers be written beneath the cipher letters of the text. It is obvious that a continuation of the process with respect to the rest of the columns of the cipher-text will result in assigning a number to each letter of the text, and these numbers will correspond to the particular basic cipher-text sequence in which each letter in the cipher-text belongs. Thus, there will finally result a distribution of the elements of the text into the 26 different classes or categories mentioned above.[1]

60. **Identifying the values of members in the same category.**—Now it has been shown above that through a knowledge of MCAL1, a relation of such a nature exists between similar cipher letters in the same column of cipher text that if the plain-text equivalent of one of the cipher letters is known, those for all the other similar cipher letters *in that column* can be derived. Take the three U's in column C of Dispatch No. 1, for example. If the value of the first U, locus Ci,

[1] This is only another way of looking at the process, already described, of assigning numbers to cipher letters in the same line to indicate that their plain-text equivalents are identical.

is known to be N_p, then the value of the second U, locus Cj, can be found through the intermediacy of Alphabet 1, to be C_p, and that of the third U, locus Cq, I_p. Now, having thus determined that $U_c = C_p$ in locus Cj the value of O_c in locus Kj and of R_c in locus Oj, *in the same horizontal line*, must also be C_p, because these cipher letters coincide with the letters of the basic cipher-text sequence in which U, the first letter of that line, is found (by application of the basic cipher-text sequence to that line of cipher text). Again, in the case of the third U, which is in locus Cq, the value of these other letters of that line which fall into the same basic cipher-text sequence with U, must also be I_p. These letters are D in locus Lq; W in locus Nq; and P in locus Yq.

Now let us assume for a moment that every horizontal line of the cipher text began with U_c. By virtue of the foregoing process the values of all those letters of each line which belong to the same basic cipher-text sequence could readily be derived. But such an assumption unfortunately carries us little further. However, does it really make any difference whether all the lines begin with U_c? Is it not still true that those letters of the line which do belong to the same basic alphabet cipher-text sequence as does the U have the same value that the U_c would have, *if it were present?* For example, if the letter in locus Ck were also a U (instead of a J_c), by reference to Alphabet 1, its value would be found to be O_p. Now set that basic cipher-text sequence in which U occupies the third position against the line of upper cipher text and observe what coincidences are present. Thus:

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

Note the four coincidences. Does it not follow that the D, S, P, and E of the line of cipher-text must all equal O_p, even though U_c does not begin that line of text? And does it not follow that the value of any S_c in column D, of any A_c in column E, of any L_c in column F, and so on can be derived in the same manner, by finding what U_c would equal if it were present as the first letter of the line in which each identity is found? Identification of every member of the category was thus made possible through the identification of but one letter, U_c in locus Ci.

A thorough comprehension of this principle will show that if the value of a single member of one category of letters (those that belong to the same basic cipher-text sequence) *no matter in what horizontal line of cipher text that single member occurs*, can be correctly determined, the value of all other members of the same category can be derived through the relationship herewith disclosed. It also follows that the correct determination of the values of but 3 or 4 members of different categories will soon result in producing combinations of high degree of probability (syllables and the skeletons of words of plain text), which will soon lead to a complete resolution of the text to be deciphered.

61. **The initial determination of the value of a member of any category.**—But the question is this: How can one determine the initial 3 or 4 correct values upon which all this depends? The answer is not difficult to find. After the letters have all been distributed into their respective categories (and they will therefore have assigned to them, or will be indicated by some number in the cipher text), then that category which has the greatest number of representatives is studied intensively in the following manner: If the value of one of the members of that category is assumed to be E_p, what are the values of all the other members in that category? Obviously, since almost 75 percent of plain text consists of but 10 letters (E, T, R, I, N, O, A, S, D, L) *the plain-text values derived from the initial assumption should form a good assortment of these high-frequency letters.* If, therefore, the derived values, based upon the assumption for E_p, gives a good assortment of high-frequency letters, then the assumption is likely to be correct. If the basic assumption does not yield a good assortment of high-frequency letters, then another basic assumption is made, and its derived assortment determined. It is clear that

the assumption which yields the best assortment of high-frequency letters is most likely to be the correct one.

Now it will, of course, be a great advantage to be able quickly to determine the values derived from a number of assumptions. Heretofore, it has been necessary to refer to the sliding strips for each derivation, and the process takes considerable time. If a more direct method can be devised it would, of course, greatly facilitate the process of analysis. The method which was devised is described below.

62. **Constructing a table of basic plain-text sequences.**—It was shown in paragraph 60 how the plain-text equivalents of similar cipher letters in columns could be found through the intermediacy of Alphabet 1 and LFS. It is obvious that the plain-text equivalents for similar cipher letters in columns can be determined once and for all for a given Alphabet 1 and LFS. It may be advisable to review the reason for this being the case. It will be recalled that providing no displacement of CW2, 3, or 4 occurs during the encipherment of the same dispatch, then the difference in cipher equivalents for two or more identical plain-text letters *in the same column* is due solely to the displacement of CW5. On the other hand, under the same circumstances as regards the absence of displacement of CW2, 3, or 4, the difference in plain-text equivalents for two or more identical cipher letters *in the same column* is due solely to the displacement of CW1. If, in the latter case, Alphabet 1 and LFS are both known, then the plain-text equivalents for such identical cipher letters can easily be determined. Looked at from the point of view of decipherment, there are only 26 contact points through which current emerges from BS2 and passes into the RHC's of CW1, and if Alphabet 1 and LFS are known, then it follows that a *table of basic sequences for plain-text letters*, similar in its nature to that for cipher-text letters can be constructed.

For illustration, suppose Alphabet 1 is in its initial position, with A of its normal component opposite SET. Thus:

```
LFS----     B S X R Z T K D N G C H M V O L Y Q E U P W J A I F
          { 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
AL1-----  {
          { X Q B O A W E N U J F V R D S Y K H T L C I P Z M G
AL2----   { 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
            . . . . . . . . . . . . . . . . . . . . . . . . . .
```

In this case, suppose in encipherment, a current enters the A of NAL2. What is the plain-text letter involved? Tracing it backward, it will be found that Z_p is the letter involved. Now advance Alphabet 1 to the next position, with B at SET, and see what plain-text letter will bring the current to A of NAL2. It is S_p. Continuing the process, the entire sequence of plain-text letters which will bring the current to A of NAL2, as CW1 is advanced consecutively is as follows:

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

That is, for example, when CW1 is set at R, then W_p will bring the current to A of NAL2.

Now there are, of course, 26 points to which a current can be brought to the letters of NAL2 from the letters of MAL1, and for each of these points a different series of plain-text letters will apply. All the sequences may be determined in exactly the same manner as that illustrated above for the first sequence. They are given below.

TABLE 11.—TABLE OF BASIC PLAIN-TEXT SEQUENCES

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

Now it is obvious that the ZSEC sequence, for example, does not necessarily apply only to those cases in which the current is brought to A of NAL2. Exactly to which contact point the current is brought depends upon the position of CW2. But the point is *that no matter to what letter of NAL2 the current is brought for any position of CW2, the sequence of plain-text letters* ZSEC. . . *will always bring the current to the same letter of NAL2, and, providing no displacement of CW2, 3, or 4 takes place, the cipher resultant will always be the same for the column to which that cipher resultant applies.* The cipher resultant will, of course, be different for different rotatory permutations of CW2, 3, and 4, but whatever it happens to be, it will be the same for that column for the successive equivalents of the plain-text sequence ZSEC. . . . The same applies to all the other sequences of table 11.

Now recall what has been said about the 26 categories of letters discussed under paragraph 59. Any one of these categories may apply to any one of the sequences in table 11. But the correct assumption for the value of one member of one category will give the values for all other members of the same category. For example, suppose a category bearing the number 6 is being examined, and suppose that in that line which corresponds to the placement of L of CW1 at SET, a letter bearing the number 6 is assumed to equal E_p. Then the value of any letter bearing the number 6 in a line corresponding to the placement of M of CW1 at SET will have the value C_p; the value of any letter bearing the number 6 in a line corresponding to the placement of N of CW1 at SET will have the value 0_p, and so on, because in table 11, the column in which E is situated in the L line reads . . . ECOIFXQ. . . . (See column D, table 11, p. 73.)

Perhaps the application of these principles to an actual example will best serve to clarify the process described.

63. **Application of principles to an actual example.**—For this purpose, Dispatch No. 3 of the series submitted for test will be employed.

First, all the letters of the text were assigned numbers applicable to the categories to which they belong. This was done, of course, by reference to the table of basic cipher-text sequences, table 9. The results are as follows:

DISPATCH NO. 3

Key: BLOIS

LAW	CW1	CW3	CW5	RAW																											
				RAW..	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
				CW5...	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	
B	L	O	E	O						P	Z	X	X	O	Z	W	T	S	R	S	F	F	B	X	K	H	Y	X	B	Y	Line l
										7	19	24	26	15	5	3	5	17	5	22	24	6	23	4	21	22	5	7	19	23	
C	M	O	E	O	J	N	I	R	N	L	I	F	K	V	O	R	A	R	B	V	Z	U	G	V	A	C	C	N	B	T	Line m
					19	15	26	11	17	18	17	19	24	23	7	4	7	20	11	7	1	11	24	19	26	10	12	20	19	24	
D	N	O	E	O	Y	L	P	C	W	T	O	L	Q	D	V	H	A	Z	Z	G	Z	P	G	J	P	F	E	R	M	Q	Line n
					18	1	16	25	16	6	1	11	5	7	18	14	7	6	15	16	1	25	24	6	1	9	1	16	6	20	
E	O	O	E	O	U	D	P	K	F	K	Q	E	M	D	S	O	D	L	M	O	K	R	T	D	U	V	C	A	N	L	Line o
					12	6	16	23	13	15	10	22	23	7	12	20	9	22	7	5	9	26	21	3	20	20	12	9	7	22	
F	P	O	E	O	Z	Q	B	O	R	W	I	U	P	F	H	Q	O	O	G	X	M	T	M	I	J	M	V	U	B	Z	Line p
					10	23	14	8	19	8	17	17	1	11	8	17	22	13	3	13	12	3	9	24	10	1	13	21	19	3	
G	Q	O	E	O	G	A	H	P	N	G	Q	R	J	F	T	L	S	I	P	N	L	W	C	K	I	E	T	H	I	K	Line q
					14	13	19	22	17	25	10	18	12	11	19	26	13	2	17	23	13	21	11	18	11	19	14	11	22	25	
H	R	O	E	O	O	S	E	R	O	I	B	J	O	P	H	X	S	V	X	G	L	Y	U	F	Y	A	E	L	G	K	Line r
					25	19	9	11	11	9	26	9	21	24	8	9	13	1	18	16	13	22	18	25	8	18	1	23	12	25	
I	S	O	E	O	O	L	A	L	F	V	E	F	H	R	N	Z	D	X	I	X	Z	K	V	B	G	I	Q	P	M	L	Line s
					25	1	21	24	13	11	13	19	15	3	13	24	9	8	21	13	1	13	12	16	19	13	19	13	6	22	
J	T	O	E	O	R	Y	H	A	Q	H	Q	U	G	Q	X	O	U	K	C	M	P	A	Q	U	R	N	Z	E	A	C	Line t
					2	24	19	19	4	5	10	17	7	12	6	20	4	10	1	17	10	17	7	8	6	8	17	25	4	21	
K	U	O	E	O	X	N	T	X	I	C	L	R	S	Z	O	A	A	P	H	B	I	K	S	D	C	H	R	Y	R	S	Line u
					15	15	23	16	23	22	16	18	6	2	7	22	7	4	23	15	3	13	15	3	23	22	24	17	23	1	
L	V	O	E	O	W	W	D	Y	C	Q	S	K	K	U	B	J	I	Q	W	Q	F	J	H	N	U	K	Z	U	S	D	Line v
					5	7	17	9	6	21	4	14	24	22	4	21	25	14	4	8	24	5	1	14	20	14	17	21	10	16	
M	W	O	E	O	R	I	B	N	W	M	S	C	S	F	M	N	H	Q	D	U	P	P	U	Q	L	U	U	R	A	H	Line w
					2	5	14	10	16	24	4	16	6	11	16	11	18	14	14	6	10	25	18	11	14	2	26	16	4	17	
						↓ Key: OXPFP																									
N	X	O	E	O	X	N	G	Q	E	D	J	M	R	W	X	X	K	R	Y	S	V										Line x
					15	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.										

It will be noted that only the first letter of the last line is assigned a number, because with the encipherment of the next letter, CW3 has advanced one space. (Refer to the key for the dispatch.) Only letters belonging to the text enciphered during the nondisplacement of CW2, 3, or 4 can be distributed into the same set of categories.

Then a frequency table is compiled in order to find those categories which have the most representatives. In addition to this feature of the work it is well to prepare an index giving the exact locus of each member of each category, so that it can quickly be found when necessary. The table or index of locations, giving the exact locus of each member of each category is shown below:

TABLE 12

1	UFKUYAMZRAFUSDW mnnnnnpprrsstuv
2	RENEZ qtuww
3	PXSVDNUX lopppsuu
4	XPIQCRKOSKC lmtttuvvvww
5	OQSAMTJEVF llllnotvvw
6	VJRXCFCOYMIMT lnnnnosttuvww
7	JBOQTNQNSCMWOQF llmmmnnoootttuuv
8	HJOOYRXZT ppprrsttv
9	ZQUBWGJLPQH nooooprrrrsv
10	ZKEYKKRUCHU moppqtttvww
11	HSVLNNWYBHIJNPX mmmnpqqqqrrswww
12	AEOAUMCWN mooopqrst
13	IRTAFQUQUIKOTBZBV opppqqqrrsssssssu
14	PGEALRXZGRSY npqqvvvvwwww
15	NFSJMEFTWE lmnosuuuux
16	GITBGTXHKDILOB nnnnorsuuvwwww
17	RIKKLPISLTVABGAD lmmpppqqttttuvvw
18	JEOLXSWZLQW mnnqqrrruww
19	KCELXCICGOZFLYAGH llmmmmppqqqrssstt
20	RBDPYZPY mmnoootv
21	YWBVMGSDJPB lopqrsstvvv
22	TZLRDQHCVDJPZN llooopqqrsuuuv
23	WDNHMFTEGISYC llmoopqruuuuu
24	LUMWDWXNHPFAMUJ llmmmnprsstuvvw
25	HVJDEXDEBQV nnqqrrrstvw
26	MGYVPKA lmmoqrw

Another table is now prepared, to show the prefix and suffix to every member of each category. This is exactly analogous to any ordinary trigraphic frequency table used in cryptanalysis. It is shown on page 76.

TABLE 13

1	7	18	6	16	6	9	17	10	13	18	25	13	10	23	5		
	11	16	11	25	7	16	11	13	18	23	21	13	17	5	14		
2	13	22	6	16	14												
	17	24	7	5	26												
3	5	21	13	12	19	15	15	15									
	5	20	13	9	14	13	13	23									
4	23	7	19	20	25	7	21	22	14	24	16						
	21	7	5	10	21	23	14	21	8	16	17						
5	15	3	17	22	11	7	4	1	24	2							
	3	17	22	7	7	9	10	7	1	14							
6	24	16	7	24	16	12	13	12	8	18	9	16	14				
	23	1	15	1	20	16	22	20	8	2	21	11	10				
7	–	5	23	4	11	5	14	23	22	9	17	17	2	22	5		
	19	19	4	20	1	18	6	12	5	22	12	8	22	4	17		
8	14	19	11	24	25	9	7	6	4								
	19	17	17	9	18	21	6	17	24								
9	1	20	5	12	3	19	11	26	8	24	17						
	1	22	26	7	24	11	26	21	13	8	6						
10	26	15	22	24	25	5	4	17	21	14	6						
	12	22	23	1	18	17	1	17	16	16	25						
11	26	20	1	1	1	12	21	18	14	9	11	13	6	16	18		
	17	7	24	5	8	19	18	19	22	11	9	13	16	18	14		
12	10	20	7	20	13	18	23	13	7								
	20	6	20	9	3	11	25	16	6								
13	23	22	3	1	14	26	23	9	16	24	11	3	21	1	19	19	3
	15	3	12	21	19	2	21	1	22	11	19	24	1	12	19	6	15
14	18	23	3	19	4	25	1	20	5	18	14	11					
	7	8	13	11	24	4	20	17	10	14	6	2					
15	26	19	6	13	19	21	15	23	13	17							
	5	26	16	10	3	15	23	3	3	-							
16	1	25	15	1	6	18	12	23	22	10	10	4	11	26			
	25	6	1	6	23	13	19	23	18	2	24	6	11	4			
17	5	11	18	8	17	8	22	2	10	1	10	8	24	7	14	4	
	5	18	19	17	1	22	25	23	7	10	7	25	23	9	21	15	
18	17	24	7	10	11	1	22	8	16	11	25						
	17	1	14	12	11	16	25	1	6	14	11						
19	7	7	23	17	24	20	8	21	13	11	11	25	13	16	13	24	19
	24	23	15	24	26	24	8	3	22	26	14	9	15	13	13	19	4
20	7	12	6	12	3	20	6	14									
	11	19	12	9	20	12	4	14									
21	4	26	13	3	9	1	8	4	6	4	17						
	22	3	19	11	24	24	13	15	4	25	10						
22	5	21	10	9	7	17	19	11	13	6	23	7	23	24			
	24	5	23	7	10	13	17	25	18	2	16	7	24	4			
23	6	19	24	16	22	10	17	1	15	16	4	3	17				
	4	19	7	13	7	14	13	12	16	22	15	22	1				
24	19	22	19	11	19	25	9	21	21	13	2	22	14	8	16		
	26	6	23	19	18	6	10	8	13	9	19	17	22	5	4		
25	16	1	17	22	25	18	12	25	17	21	10						
	16	24	10	25	19	8	25	1	4	14	18						
26	24	15	19	9	19	9	2										
	15	11	10	21	13	9	16										

Refer now to table 12 and it will be seen that categories 13 and 19 are of the greatest frequency, and they will therefore be selected for experiment. Now, it will be noted that of the 17 members of category 13, 7 of them occur in line *s*. It is extremely probable that in this line the number 13 represents one of the letters of highest frequency in normal plain-text, but which one?

Assume it to represent E_p. Then what will the plain-text values of the other 10 members of this category be? Those 10 other members are as follows:

One in line *o;* three in line *p;* three in line *q;* two in line *r;* and one in line *u.*

Refer now to table 11 and determine what plain-text values are indicated, upon the assumption that the seven representatives of category 13 in line *s* represents E_p. Proceeding along the *s* line of the table to E, the following values will be found in the same column in which E is located:

Line *o*—plain-text value is O_p
Line *p*—plain-text value is T_p
Line *q*—plain-text value is A_p
Line *r*—plain-text value is L_p
Line *u*—plain-text value is A_p

In other words, if the number 13 in line *s* represents E_p, then the other members of category 13 would represent the letters O, T, A, and L, all letters of high frequency. If numerical values be assigned to these plain-text equivalents in accordance with their frequency in normal text (based upon table 2), the total value of the hypothesis that the number 13 in line *s* represents E_p is 158.6 units, determined as follows:

Weighted Numerical Frequency Value of Category 13 upon assumption that $13=E_p$ in line *s*.

Line in text	Plain-text value	Frequency of occurrence	Numerical frequency value	Weighted numerical frequency value
o	O	1	7.4	7.4
p	T	3	9.0	27.0
q	A	3	7.2	21.6
r	L	2	3.5	7.0
s	E	7	12.6	88.2
u	A	1	7.2	7.2
				Total = 158.4

But suppose the number 13 in line *s* does not represent E_p. Suppose it represents T_p. Then what is the total weighted numerical frequency value of this hypothesis? It is as follows:

Weighted Numerical Frequency Value of Category 13 upon assumption that $13=T_p$ in line *s*.

Line in text	Plain-text value	Frequency of occurrence	Numerical frequency value	Weighted numerical frequency value
o	A	1	7. 2	7. 2
p	Y	3	2. 1	6. 3
q	C	3	3. 4	10. 2
r	I	2	7. 6	15. 2
s	T	7	9. 0	63. 0
u	N	1	7. 6	7. 6
				Total = 109. 5

The value of this hypothesis is only 109.5 units. In other words, the first hypothesis, with a total of 158.4 units, is half again as probable as the second hypothesis, with a total of only 109.5 units. A condensed table of total values based upon the fixed hypotheses with respect to the value of the number 13 in line *s* (viz, that it equals E, T, R, I, and N) is as follows:

Line in text	Freq. of occ.	P.-t. value ($13=E_p$ in line *s*)	Wtd. value ($13=E_p$ in line *s*)	P.-t. value ($13=T_p$ in line *s*)	Wtd. value ($13=T_p$ in line *s*)	P.-t. value ($13=R_p$ in line *s*)	Wtd. value ($13=R_p$ in line *s*)	P.-t. value ($13=I_p$ in line *s*)	Wtd. value ($13=I_p$ in line *s*)	P.-t. value ($13=N_p$ in line *s*)	Wtd. value ($13=N_p$ in line *s*)
o	1	O	7. 4	A	7. 2	E	12. 6	H	3. 3	Z	. 1
p	3	T	27. 0	Y	6. 3	W	4. 2	X	1. 5	U	9. 0
q	3	A	21. 6	C	10. 2	G	5. 4	T	27. 0	W	4. 2
r	2	L	7. 0	I	15. 2	B	2. 2	E	25. 2	O	14. 8
s	7	E	88. 2	T	63. 0	R	58. 1	I	54. 6	N	53. 2
u	1	A	7. 2	N	7. 6	J	. 2	Z	. 1	R	8. 3
			158. 4		109. 5		81. 7		111. 7		89. 6

It is seen that the first hypothesis is by far the most probable one, and it will be assumed to be correct. The plain-text values derived from it are at once inserted in the text, wherever a member of category 13 is present.

Now refer to table 13, and particularly to the prefixes and suffixes of the numbers of category 13. They are as follows:

$$13\begin{cases} 23\ \ 22\ \ \ 3\ \ \ 1\ \ 14\ \ 26\ \ 23\ \ 9\ \ 16\ \ 24\ \ 11\ \ \ 3\ \ 21\ \ \ 1\ \ 19\ \ 19\ \ \ 3 \\ 15\ \ \ 3\ \ 12\ \ 21\ \ 19\ \ \ 2\ \ 21\ \ 1\ \ 22\ \ 11\ \ 19\ \ 24\ \ \ 1\ \ 12\ \ 19\ \ \ 6\ \ 15 \end{cases}$$

A member of category 19 occurs twice as a prefix, and three times as a suffix, five times in all. Find them in the cipher-text. They are as follows:

Column----	F	G	Column----	K	L	Column----	Y	Z	A	B
Line *q*-----	13	19	Line *s*-----	13	19	Line *s*-----	19	13	19	13

It is certain that in the line *s*, 19 represents a consonant, R, N, S, or T, most probably R, on account of its frequency of combination with E. Assume then, that in line *s*, number 19 represents R_p. What will the other diagraph of 13 and 19 in line *q* be? Referring to table 11, it will be found that if 19 in line *s* of the table is R_p, then in line *q* it is G_p, thus giving the digraph 13–19 in line *q* of the text the value E G_p.

Assume that 19 represents N_p. Then in line *q*, 13–19 = E W_p.
Assume that 19 represents S_p. Then in line *q*, 13–19 = E U_p.
Assume that 19 represents T_p. Then in line *q*, 13–19 = E C_p.

There is not much choice to be made based upon any of these hypotheses. Perhaps more light can be gained by determining what all the values of 19 would be upon the following hypotheses:

Line in text	Freq. of occ.	P.-t. value (19 in line $s=R_p$)	Wtd. value (19 in line $s=R_p$)	P.-t. value (19 in line $s=N_p$)	Wtd. value (19 in line $s=N_p$)	P.-t. value (19 in line $s=S_p$)	Wtd. value (19 in line $s=S_p$)	P.-t. value (19 in line $s=T_p$)	Wtd. value (19 in line $s=T_p$)
l	2	Q	0. 6	Y	4. 2	W	2. 8	R	16. 6
m	4	N	30. 4	B	4. 4	I	30. 4	K	1. 6
p	2	W	2. 8	U	6. 0	K	. 8	Y	4. 2
q	3	G	5. 4	W	4. 2	U	9. 0	C	9. 9
r	1	B	1. 1	O	7. 4	F	3. 0	I	7. 6
s	3	R	24. 9	N	22. 8	S	17. 4	T	27. 0
t	2	Y	2. 1	J	. 4	T	9. 0	H	6. 6
			67. 3		49. 4		72. 4		73. 5

Line in text	Freq. of occ.	P.-t. value (19 in line $s=D_p$)	Wtd. value (19 in line $s=D_p$)	P.-t. value (19 in line $s=L_p$)	Wtd. value (19 in line $s=L_p$)	P.-t. value (19 in line $s=C_p$)	Wtd. value (19 in line $s=C_p$)
l	2	M	5. 0	O	14. 8	A	14. 4
m	4	E	50. 4	T	36. 0	F	12. 0
p	2	I	15. 2	S	11. 6	B	2. 2
q	3	Y	6. 3	R	24. 9	D	12. 0
r	1	U	3. 0	D	4. 0	V	1. 3
s	3	D	12. 0	L	10. 5	C	9. 9
t	2	I	15. 2	C	3. 3	S	11. 6
			107. 1		105. 1		63. 4

Of all these hypotheses, only two seem probable, viz., the ones which assume 19 in line *s* to equal D_p and L_p, respectively. They give totals which are so close together that it is impossible to tell which of the two is correct. But if reference is made to the cipher text, in line *t*, columns G and H, the combination 19–19 occurs. According to the hypothesis 19 in line $s = D_p$, then in line *t* the 19–19 combination would equal I I_p, which is extremely rare in English; whereas, according to the hypothesis that 19 in line $s = L_p$, then in line *t* the 19–19 combination would equal C C_p, a very frequent doublet.

It would seem then that the hypothesis that 19 in line $s = L_p$ is the best one of the lot. Insertion of the values of 19 and 13 throughout yields the following:

DISPATCH NO. 3

Key: BLOIS

	RAW..	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
LAW CW1 CW3 CW5 RAW	CW5...	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	
B L O E O							P	Z	X	X	O	Z	W	T	S	R	S	F	F	B	X	K	H	Y	X	B	Y	Line l
							7	19	24	26	15	5	3	5	17	5	22	24	6	23	4	21	22	5	7	19	23	
								O																		O		
C M O E O		J	N	I	R	N	L	I	F	K	V	O	R	A	R	B	V	Z	U	G	V	A	C	C	N	B	T	Line m
		19	15	26	11	17	18	17	19	24	23	7	4	7	20	11	7	1	11	24	19	26	10	12	20	19	24	
		T							T												T					T		
D N O E O		Y	L	P	C	W	T	O	L	Q	D	V	H	A	Z	Z	G	Z	P	G	J	P	F	E	R	M	Q	Line n
		18	1	16	25	16	6	1	11	5	7	18	14	7	6	15	16	1	25	24	6	1	9	1	16	6	20	
E O O E O		U	D	P	K	F	K	Q	E	M	D	S	O	D	L	M	O	K	R	T	D	U	V	C	A	N	L	Line o
		12	6	16	23	13	15	10	22	23	7	12	20	9	22	7	5	9	26	21	3	20	20	12	9	7	22	
						O																						
F P O E O		Z	Q	B	O	R	W	I	U	P	F	H	Q	O	O	G	X	M	T	M	I	J	M	V	U	B	Z	Line p
		10	23	14	8	19	8	17	17	1	11	8	17	22	13	3	13	12	3	9	24	10	1	13	21	19	3	
						S									T		T							T		S		
G Q O E O		G	A	H	P	N	G	Q	R	J	F	T	L	S	I	P	N	L	W	C	K	I	E	T	H	I	K	Line q
		14	13	19	22	17	25	10	18	12	11	19	26	13	2	17	23	13	21	11	18	11	19	14	11	22	25	
			A	R								R		A				A					R					
H R O E O		O	S	E	R	O	I	B	J	O	P	H	X	S	V	X	G	L	Y	U	F	Y	A	E	L	G	K	Line r
		25	19	9	11	11	9	26	9	21	24	8	9	13	1	18	16	13	22	18	25	8	18	1	23	12	25	
			D											L				L										
I S O E O		O	L	A	L	F	V	E	F	H	R	N	Z	D	X	I	X	Z	K	V	B	G	I	Q	P	M	L	Line s
		25	1	21	24	13	11	13	19	15	3	13	24	9	8	21	13	1	13	12	16	19	13	19	13	6	22	
						E		E	L			E					E		E			L	E	L	E			
J T O E O		R	Y	H	A	Q	H	Q	U	G	Q	X	O	U	K	C	M	P	A	Q	U	R	N	Z	E	A	C	Line t
		2	24	19	19	4	5	10	17	7	12	6	20	4	10	1	17	10	17	7	8	6	8	17	25	4	21	
				C	C																							
K U O E O		X	N	T	X	I	C	L	R	S	Z	O	A	A	P	H	B	I	K	S	D	C	H	R	Y	R	S	Line u
		15	15	23	16	23	22	16	18	6	2	7	22	7	4	23	15	3	13	15	3	23	22	24	17	23	1	
																			A									
L V O E O		W	W	D	Y	C	Q	S	K	K	U	B	J	I	Q	W	Q	F	J	H	N	U	K	Z	U	S	D	Line v
		5	7	17	9	6	21	4	14	24	22	4	21	25	14	4	8	24	5	1	14	20	14	17	21	10	16	
M W O E O		R	I	B	N	W	M	S	C	S	F	M	N	H	Q	D	U	P	P	U	Q	L	U	U	R	A	H	Line w
		2	5	14	10	16	24	4	16	6	11	16	11	18	14	14	6	10	25	18	11	14	2	26	16	4	17	
N X O E O		X	N	G	Q	E	D	J	M	R	W	X	X	K	R	Y	S	V										Line x
		15	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.										

Only two categories have been thus far determined. One more will be determined.

Take the C C_p in line *t*. It must be preceded by a vowel, A, E, I, or O. The category number of the letter concerned is 24, one of high frequency. Here are the total different values for the four assumptions:

Line in text	Frequency	P.-t. value ($24 = A_p$)	P.-t. value ($24 = E_p$)	P.-t. value ($24 = I_p$)	P.-t. value ($24 = O_p$)
l	2	G	J	M	F
m	3	S	Q	E	V
n	1	U	G	L	Z
p	1	C	A	I	P
r	1	Z	S	U	X
s	2	Q	Y	D	K
t	1	A	E	I	O
u	1	F	H	S	G
v	2	R	T	O	S
w	1	H	U	P	T

It is unnecessary to establish weighted frequency values, for it is obvious that the third assumption is by far the best in its results. Insertion of these values at once enables assumptions to be made for certain words in the plain-text. For example, the dispatch is seen to start with the combination – O M; which suggests the trigraph C O M, or S O M, for the beginning of the dispatch. Only a little more experiment is necessary and the whole dispatch becomes readily solvable. It is as follows:

DISPATCH NO. 3

Key: BLOIS

LAW	CW1	CW3	CW5	RAW																											
				RAW	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
				CW5	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	
B	L	O	E	O						P	Z	X	X	O	Z	W	T	S	R	S	F	F	B	X	K	H	Y	X	B	Y	Line l
										7	19	24	26	15	5	3	5	17	5	22	24	6	23	4	21	22	5	7	19	23	
										C	O	M	P	L	E	T	E	G	E	R	M	A	N	F	I	R	E	C	O	N	
C	M	O	E	O	J	N	I	R	N	L	I	F	K	V	O	R	A	R	B	V	Z	U	G	V	A	C	C	N	B	T	Line m
					19	15	26	11	17	18	17	19	24	23	7	4	7	20	11	7	1	11	24	19	26	10	12	20	19	24	
					T	R	O	L	S	Y	S	T	E	M	A	V	A	I	L	A	B	L	E	T	O	U	N	I	T	E	
D	N	O	E	O	Y	L	P	C	W	T	O	L	Q	D	V	H	A	Z	Z	G	Z	P	G	J	P	F	E	R	M	Q	Line n
					18	1	16	25	16	6	1	11	5	7	18	14	7	6	15	16	1	25	24	6	1	9	1	16	6	20	
					D	S	T	A	T	E	S	F	O	R	D	I	R	E	C	T	S	A	L	E	S	Y	S	T	E	M	
E	O	O	E	O	U	D	P	K	F	K	Q	E	M	D	S	O	D	L	M	O	K	R	T	D	U	V	C	A	N	L	Line o
					12	6	16	23	13	15	10	22	23	7	12	20	9	22	7	5	9	26	21	3	20	20	12	9	7	22	
					E	M	P	L	O	Y	S	A	L	T	E	R	N	A	T	I	N	G	C	U	R	R	E	N	T	A	
F	P	O	E	O	Z	Q	B	O	R	W	I	U	P	F	H	Q	O	O	G	X	M	T	M	I	J	M	V	U	B	Z	Line p
					10	23	14	8	19	8	17	17	1	11	8	17	22	13	3	13	12	3	9	24	10	1	13	21	19	3	
					N	D	H	A	S	A	C	C	U	R	A	C	Y	T	O	T	W	O	M	I	N	U	T	E	S	O	
G	Q	O	E	O	G	A	H	P	N	G	Q	R	J	F	T	L	S	I	P	N	L	W	C	K	I	E	T	H	I	K	Line q
					14	13	19	22	17	25	10	18	12	11	19	26	13	2	17	23	13	21	11	18	11	19	14	11	22	25	
					F	A	R	C	S	T	O	P	G	E	R	M	A	N	S	H	A	V	E	P	E	R	F	E	C	T	
H	R	O	E	O	O	S	E	R	O	I	B	J	O	P	H	X	S	V	X	G	L	Y	U	F	Y	A	E	L	G	K	Line r
					25	19	9	11	11	9	26	9	21	24	8	9	13	1	18	16	13	22	18	25	8	18	1	23	12	25	
					E	D	A	P	P	A	R	A	T	U	S	A	L	O	N	G	L	I	N	E	S	N	O	W	B	E	
I	S	O	E	O	O	L	A	L	F	V	E	F	H	R	N	Z	D	X	I	X	Z	K	V	B	G	I	Q	P	M	L	Line s
					25	1	21	24	13	11	13	19	15	3	13	24	9	8	21	13	1	13	12	16	19	13	19	13	6	22	
					I	N	G	D	E	V	E	L	O	P	E	D	B	Y	G	E	N	E	R	A	L	E	L	E	C	T	
J	T	O	E	O	R	Y	H	A	Q	H	Q	U	G	Q	X	O	U	K	C	M	P	A	Q	U	R	N	Z	E	A	C	Line t
					2	24	19	19	4	5	10	17	7	12	6	20	4	10	1	17	10	17	7	8	6	8	17	25	4	21	
					R	I	C	C	O	M	P	A	N	Y	S	T	O	P	J	A	P	A	N	E	S	E	A	B	O	U	
K	U	O	E	O	X	N	T	X	I	C	L	R	S	Z	O	A	A	P	H	B	I	K	S	D	C	H	R	Y	R	S	Line u
					15	15	23	16	23	22	16	18	6	2	7	22	7	4	23	15	3	13	15	3	23	22	24	17	23	1	
					T	T	O	C	O	N	C	L	U	D	E	N	E	G	O	T	I	A	T	I	O	N	S	F	O	R	
L	V	O	E	O	W	W	D	Y	C	Q	S	K	K	U	B	J	I	Q	W	Q	F	J	H	N	U	K	Z	U	S	D	Line v
					5	7	17	9	6	21	4	14	24	22	4	21	25	14	4	8	24	5	1	14	20	14	17	21	10	16	
					P	U	R	C	H	A	S	E	O	F	S	A	M	E	S	T	O	P	G	E	N	E	R	A	L	D	
M	W	O	E	O	R	I	B	N	W	M	S	C	S	F	M	N	H	Q	D	U	P	P	U	Q	L	U	U	R	A	H	Line w
					2	5	14	10	16	24	4	16	6	11	16	11	18	14	14	6	10	25	18	11	14	2	26	16	4	17	
					E	S	C	R	I	P	T	I	O	N	I	N	A	C	C	O	R	D	A	N	C	E	W	I	T	H	
N	X	O	E	O	X	| N	G	Q	E	D	J	M	R	W	X	X	K	R	Y	S	V									Line x
					15	| .	.	.	.	.	.	.	.	.	.	.	.	.	.	.										
					M																										

Section XIII

RECONSTRUCTION OF OTHER ALPHABETS

64. **Purpose of reconstruction.**—Having reconstructed Alphabets 1 and 5, it is obvious that if Alphabets 2, 3, and 4 could be reconstructed, then any message could be solved directly from the sliding strips, providing the full keyword for each message were known. It will now be shown what the preliminary requirements for such a reconstruction are, and how, if these are met, the process can be accomplished.

65. **Preliminary requirements to the reconstruction.**—It may be stated at the outset, that a prerequisite to the reconstruction of Alphabets 2, 3, and 4 is a knowledge of the complete key setting for a certain number of dispatches. This is the case even though dispatches may be solved by detailed analysis with only a knowledge of the setting of LAW, CW1, 3, 5, and RAW. The principal purpose of reconstructing AL2, 3, and 4, is to eliminate the necessity for this detailed analysis along the lines indicated in the preceding section.

Another prerequisite to the reconstruction is the possession in the set of dispatches of certain ones enciphered by means of specific relative settings to be described below. Lacking such messages, the process cannot be accomplished, but failure to have the requisite dispatches, when a considerable amount of them are available for study, would be rather rare, as will be apparent when it is stated that in the set of but 10 dispatches herein studied there were found three cases which met the required conditions.

66. **Complete keys for the dispatches herein analyzed.**—It was stated in paragraph 47, section X, that the key settings for CW2 and 4 were not indicated for the set of 10 dispatches prepared by the Code and Signal Section, Navy Department. It may be well to state the reasons therefor.

It has been shown that the permutations of the automatically displaced CW1, 3, and 5 yield an enciphering key of 17,576 letters. Manual displacements of CW2 and 4 yield 676 sets of such keys. The theory behind the secrecy of CW2 and 4 was that each station could be assigned a different pair of key settings for these two wheels, and thus avoid the accidental enciphernent of two dispatches by different stations, in exactly the same key.

Now from a consideration of what has gone before, it will be obvious that such a procedure would be more or less futile. Firstly, it would really make the solution of dispatches from the same station easier, because all dispatches originating from it would be in the same setting as regards CW2 and 4. Secondly, in order to communicate with any station, a special key-setting code, showing what the settings for each station are, would have to be at hand at every station, and this list would have to be changed and distributed frequently, entailing many practical difficulties. Thirdly, so far as the writer can see, the chances of two stations enciphering two messages by exactly the same key (of seven letters, if given complete) would be somewhat remote, being in the ratio of 1: 26^7 or about 1 in 10 billion; even if it did occur, the solution of only 2 or

3 messages in identical keys, by the superimposition method, would be utterly impossible. At least 50 such dispatches would be a minimum for that method of solution. The chances for a set of stations selecting on the same day the same keyword 50 times are exceedingly remote.

Usage of the machines in the military service would require that the entire keyword of seven letters be indicated for each message, so that every station could communicate with every other one without reference to any code book giving key settings, or to any secret list giving the settings for any cipher wheels.

With this in mind, it was desirable to see how difficult the reconstruction of AL2, 3, and 4 would be under such circumstances. Having first satisfied himself that such a reconstruction is absolutely impossible without a knowledge of the key settings applicable, and having already recovered and demonstrated the plain text of all ten test dispatches the writer requested the Code and Signal Section to indicate the key settings for CW2 and 4 for the 10 messages. He was informed that the setting for CW2 was the same as for CW3, that for CW4 the same as that for CW5, in each respective keyword. For example, in the keyword AGRAM (Dispatch No. 1), CW2 was set to R, and CW4 to A. The list of complete keys is therefore as follows:

Dispatch	Keyword	Setting						
		LAW	CW1	CW2	CW3	CW4	CW5	RAW
1	AGRAM	A	G	R	R	A	A	M
2	COBAN	C	O	B	B	A	A	N
3	BLOIS	B	L	O	O	I	I	S
4	AGANA	A	G	A	A	N	N	A
5	CUNEO	C	U	N	N	E	E	O
6	DOVER	D	O	V	V	E	E	R
7	GENOA	G	E	N	N	O	O	A
8	HAGUE	H	A	G	G	U	U	E
9	MONTE	M	O	N	N	T	T	E
10	NEPAL	N	E	P	P	A	A	L

67. **Study of keys.**—This list was then carefully examined to find two messages which meet the following requirement, viz, that as regards CW2, 3, and 4 there should be a case in which the two dispatches should have the same pair of key letters indicating the initial setting for CW2 and 3, or for CW3 and 4. The purpose in finding such messages is, naturally, to be able to compare the cipher resultant of two specific cases wherein the differences in the cipher resultants for the same plain-text letter will be due solely to the displacement of a single cipher wheel. Three dispatches were found to conform to this requirement, viz, nos. 5, 7, and 9. In these three messages CW2 was initially set at N, and likewise CW3, although of course the similarity between the setting letter on CW2 and 3 was only a condition arbitrarily brought about by the system adopted by the Code and Signal Section, and is not a necessary condition to be met. The setting of CW2 and 3 in each dispatch can be different; it is only that for the purposes of this reconstruction the *pair* of settings for CW2 and 3 for one dispatch coincide with that for CW2 and 3 for another dispatch. Considering only nos. 5 and 7, it will be seen that whatever difference there be in the cipher resultants for the same plain-text letter enciphered in the same position as regards CW1, 2, 3, and 5, will be due solely in the difference in the position of CW4. In no. 5, CW4 is set at E, in no. 7, at O.

68. **Procedure in reconstruction of AL4.**—Set AL5 and RFS in juxtaposition, and prepare a strip for AL4, writing NCAL4 on the upper half of the strip. Above the AL4 strip place a sequence of numbers representing the series of contacts of the fourth bakelite separator, which is to act merely as a basis of reference, as will be explained presently.

Set the strips as shown below, where E of NCAL4 is at SET to correspond with the key letter applicable in CUNNEEO, and AL5 is arbitrarily set at A:

```
                      1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4---------          . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                      ↓
      {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 . . .
AL4.  {                        [______________________________]
      {. . . . . . . . . . . . A . . . . . . . . . . . . . . . . . . . . .
      {        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...
AL5.  {                                          [_____]
      {        H R Y M S L A J I W C K U Q F N V X E D P G T B Z O H R Y M...
RFS--------    T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

As a starting point for reconstructing MCAL4 insert the letter A under M of NCAL 4. Consider now some plain-text letter, θ, which enters the LHC's of AL4 from the ninth contact of BS4. The cipher resultant, with AL5 set at A, will be I_c.

Now apply the I basic cipher-text sequence of table 9 to the cipher letters of the first line of the CUNEO dispatch and try to find a coincidence between a letter of this basic sequence and a letter of the cryptogram. Thus:

CW5					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
Line U, CUNEO					H	K	W	Z	A	R	R	P	B	Q	B	I	V	Y	S	M	P	D	M	Q	M	V	U	D	C
Basic Sequence No. 4, Table 9	I	T	A	V	E	K	C	M	Q	O	S	G	Z	J	B	R	U	P	W	L	Y	O	F	X	H	D	I	T	A	V

No coincidence is found. Apply the basic sequence to the next line of text:

CW5					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
Line V, CUNEO					<u>E</u>	M	Z	X	D	P	I	D	L	I	A	W	W	U	B	Q	M	E	Z	P	I	X	<u>I</u>	S	N	H
Basic Sequence No. 4, Table 9	I	T	A	V	<u>E</u>	K	C	M	Q	O	S	G	Z	J	B	R	U	P	W	L	Y	O	F	X	H	D	<u>I</u>	T	A	V

Here it will be seen that the letter E_c of the cryptogram coincides with E of the basic sequence. Referring to the plain-text of the dispatch it is seen that E_c here equals G_p. The following equation may therefore be written:

CUNEO. E_c, key VNNEE, $= G_p$

It is necessary now to translate this E_c to some value present in the GENOA message. Since the key setting for CW1 in the CUNEO dispatch when the particular E_c under discussion was enciphered was V, and since the key setting for CW1 as regards the first line of the GENOA dispatch was E, it becomes necessary to find what plain-text letter E_c would represent in the CUNEO message if CW1 were at V. Hence, reference can be made to the table of basic plain-text sequences (table 11). It will be found that:

(CUNEO) If E_c in locus Ev $= G_p$, then
E_c in locus Ee $= T_p$. That is,
(CUNEO) E_c, key ENNEE, $= T_p$.

Refer now to the E line of the GENOA message to see if there happens to be a T_p in the line. It will be found that T_p in locus $Ye = S_c$. The following pair of equations is then at hand:

CUNEO. T_p, Key: ENNEE, = E_c
GENOA. T_p, Key: ENNOY, = S_c

These two equations are comparable except in two terms, viz, those concerning CW4 and CW5. It is easy enough to make them correspond as regards CW5. In the CUNEO dispatch the encipherment equation applies to the case where CW5 is set at E; in the GENOA dispatch, it is set at Y. The matter of reducing the second equation to the case where CW5 would be at E is merely one of reference to the table of basic cipher-text sequences. Thus:

GENOA. If T_p, key ENNOY, = S_c, then
T_p, key ENNOE, = D_c

Now there are at hand two equations in which the enciphering conditions are identical except as regards CW4. These equations are:

CUNEO. T_p, key ENNEE, = E_c (1)
GENOA. T_p, key ENNOE, = D_c (2)

These equations can now be used to give information with respect to MCAL4.

Refer to the sliding strips, and set them in the following positions:

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----   . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                          ↓
AL4---{ 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...
        . . . . . . . . . . . . A . . . . . . . . . . . . . . . . . . ....
AL5---{ 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...
        H R Y M S L A J I W C K U Q F N V X E D P G T B Z O H R Y M S L...
RFS---            T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

It will be seen that the enciphering current, in order to satisfy the first of the foregoing equations, must enter that LHC of CW4 which is arbitrarily designated, merely as a reference, by the number 9 of BS4. Bearing this in mind slide AL4 to the following position (to correspond with the key letter O, for CW4 in the GENOA dispatch).

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4--     . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                          ↓
AL4---{ K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P...
        . . A . . . . . . . . . . . . . . . . . . . . . . . . . A . . ....
AL5---{ 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...
        H R Y M S L A J I W C K U Q F N V X E D P G T B Z O H R Y M S L...
RFS---            T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```


It will be found that in order to produce the cipher letter D_c, given by the second equation, it will be necessary to insert the letter P under W of NCAL4. Thus:

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4--     . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                          ↓
AL4---{ K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P...
        . . A . . . . . . . . . P . . . . . . . . . . . . . . . A . . ....
AL5---{ 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...
        H R Y M S L A J I W C K U Q F N V X E D P G T B Z O H R Y M S L...
RFS---            T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

This means that in NCAL4 the letter P must be situated, relative to the letter A, in the position

```
1 2 3 4 5 6 7 8 9 10 11
A . . . . . . . . .  P.
```

Now move AL4 back to the key-letter E position, and AL5 back to the key-letter A position. Thus:

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4--     . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                   ↓
AL4---{ 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...
        . . . . . . . . . . . . A . . . . . . . . P . . . . . . . . . ....
AL5---{           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...
                  H R Y M S L A J I W C K U Q F N V X E D P G T B Z O H R...
RFS---            T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Assume a plain-text letter, θ, which in encipherment finally enters that LHC of CW4 designated by the number 19 in BS4, beneath which is the newly found value $\frac{W}{P}$ of AL4. The cipher resultant of θ_p would be Q_c, when CW5 is at A.

Now apply the Q basic cipher-text sequence to the CUNEO dispatch, and try to find a coincidence between a member of this sequence and one of the cryptographic text. The following case will be found:

CUNEO. L_c, key ZNNES, = U_p

By reference to the table of basic plain-text sequences, table II:

CUNEO. If L_c, key ZNNES, = U_p, then
L_c, key ENNES, = H_p

Referring to the GENOA message, line E, there is no case where the letter H_p occurs. But this does not put an end to the investigation by any means. It is merely necessary to translate the equation into terms of an F line of the GENOA dispatch, and this can be done by means of the table of basic plain-text sequences (table II). Thus:

CUNEO. If L_c, key ENNES, = H_p, then
L_c, key FNNES, = E_p. (3)

Referring to line F of the GENOA message, it will be found that

GENOA. E_p, key FNNOI, = X_c

It follows, therefore, that

GENOA. E_p, key FNNOS, $= U_c$ (4)

Putting together the two basic equations:

CUNEO. E_p, key FNNES, $= L_c$ (3)
GENOA. E_p, key FNNOS, $= U_c$ (4)

Set the sliding strips to the following position:

```
               1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----        . . . . . . . . . . . . . . . . . . . . . . . . . .
                                                    ↓
        {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 . . .
AL4-----{
        {. . . . . . . . . . . . A . . . . . . . . . P . . . . . . . . . . . .
        {O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T . . .
AL5-----{
        {F N V X E D P G T B Z O H R Y M S L A J I W C K U Q F N V X E D . . .
RFS-----               T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

It will be seen that equation (3) is satisfied, in that θ_p (which here enters into AL4 from the nineteenth contact of BS4) equals L_c.

Then moving AL4 to the following position:

```
               1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----        . . . . . . . . . . . . . . . . . . . . . . . . . .
                                                    ↓
        {K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P . . .
AL4-----{
        {. . A . . . . . . . . . P . . . . . . . . . . . . . . . A . . . . . .
        {O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T . . .
AL5-----{
        {F N V X E D P G T B Z O H R Y M S L A J I W C K U Q F N V X E D . . .
RFS-----               T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

and tracing U_c backward, it will be seen that F must be inserted under G of NCAL4 to satisfy equation (4). This gives the following placements in MCAL4:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
F . . . . . A . . .  .  .  .  .  .  .  P  .  .  .  .  .  .  .  .  .
```

As practice, let the reader corroborate the following cases:

CUNEO { C_c, key WNNEN, $= O_p$
CUNEO { C_c, key ENNEN, $= R_p$
R_p, key ENNOR, $= P_c$ } GENOA
R_p, key ENNON, $= J_c$ } GENOA

Result: In AL4: Place K under Q of NCAL4.

CUNEO { M_c, key VNNEF, $= C_p$
CUNEO { M_c, key FNNEF, $= P_p$
P_p, key FNNOR, $= T_c$ } GENOA
P_p, key FNNOF, $= F_c$ } GENOA

Result: In AL4: Place H under K of NCAL4.

Continuation of this process yields the following:

```
AL4----{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
       {Y . R . I . F . J . H . A . B . K . S . M . P . G .
```

Only half of the MCAL4 has been reconstructed, and it would seem as if nothing further can be done because one of those irritating circumstances in alphabet reconstruction, where only half of the cycle can be recovered, has here been encountered: the key settings for CW4 for the two messages are an even number of intervals apart, and only two half-cycles can be recovered.

It would, of course, be possible to construct the two halves independently, and then try to assemble them correctly, but the process of assembling is apt to be very difficult. Another way can be and was chosen out of the difficulty.

If only one letter of the second half-cycle can be inserted in its proper position, then reconstruction of this second half-cycle can be completed by reference to the same two messages, CUNEO and GENOA. But how can the correct position of this single letter be determined?

It will be remembered that there was another dispatch in which CW2 and 3 were at the same key settings as in the CUNEO and GENOA dispatches, viz, the MONTE, Dispatch No. 9. Fortunately, the two key settings for CW4 in the CUNEO and MONTE messages are an odd number of intervals apart (E to T = 15 intervals), so that any value derived from the application of a placement in AL4 from the CUNEO message will be sure to initiate the second half of the cycle at the proper point.

Set the strips to the following positions:

```
              1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----       . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                              ↓
AL4----{. . . 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 . . .
       {. . . I . F . J . H . A . B . K . S . M . P . G . Y . R . . . .
AL5----{      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 . . .
       {      H R Y M S L A J I W C K U Q F N V X E D P G T B Z O . . .
RFS----       T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Assuming a current to enter AL4 from the ninth contact of BS4, the cipher letter would be T_c. Applying the T basic cipher-text sequence to the CUNEO dispatch, the following case is found:

```
                                       EFGHIJKLMNOPQRSTUVWXYZABCD
Line 2, key V------------------        EMZXDPIDLIAWWUBQMEZPIXISNH
Basic sequence No. 14, table 9--  TFXIGMBJAUVK...
```

Referring to the plain text of the dispatch, it is seen that M_c in the position shown represents C_p. This yields the following:

CUNEO { M_c, key VNNEF, $= C_p$
CUNEO { M_c, key ONNEF, $= N_p$ . . . . (1)
N_p, key ONNTA, $= Y_c$ } MONTE
N_p, key ONNTF, $= I_c$ . . . (2) } MONTE

Place the sliding strips to correspond with the first equation; thus:

```
         1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----  . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                    ↑
AL4---- { . . . 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 . . .
        { . . . I . F . J . H . A . B . K . S . M . P . . G . Y . R . . . .

AL5---- { 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
        { L A J I W C K U Q F N V X E D P G T B Z O H R Y M S
RFS---- T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
                    ↑
```

On tracing the path taken by the current, backward from RFS, it is seen that the thirteenth contact in BS4 is the one involved.

Now moving AL4 to the key letter T (for MONTE), and tracing I_c backward, it will be found that Q must be inserted under F of NCAL4. Thus:

```
         1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS4----- . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                    ↓
AL4----- { T U V W X Y Z A B C D E F G H I J K L M N O P Q R S . . .
         { . M . P . G . Y . R . I . F . J . H . A . B . K . S . . .
AL5----- { 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
         { L A J I W C K U Q F N V X E D P G T B Z O H R Y M S
RFS----- T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
                                               ↑
```

From that point on, the two original CUNEO and GENOA dispatches may be used to complete the reconstruction. Thus:

CUNEO { A_c, key UNNEJ, $= H_p$
{ A_c, key FNNEJ, $= M_p$

M_p, key FNNOQ, $= T_c$ }
M_p, key FNNOJ, $= H_c$ } GENOA

Result: In AL4: Place L under P of NCAL4.

Continuation of this process soon yields the complete alphabet, which is as follows:

```
AL4----- { 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
         { Y E R T I Q F N J O H V A W B L K D S X M C P Z G U
```

69. **Procedure in reconstruction of AL3.**—Having reconstructed AL4 the next thing to do is to reconstruct AL3. For this, after AL4 (or AL2) has been reconstructed, only one dispatch is necessary, providing CW3 has been automatically displaced during the course of its encipherment. The GENOA dispatch was employed.

The following equations may be studied:

Since X_c, key FNNOD, $= S_p$, then
X_c, key LNNOD, $= T_p$ . . . . (1)
But T_p, key LNOOI, $= H_c$, hence
T_p, key LNOOD, $= T_c$ . . . . (2)

Here there are two encipherments of the same plain-text letter, T_p. In the first case CW3 was at N, in the second, at O, with all the other cipher wheels at the same positions in both cases.

Again a set of sliding strips is arranged, with AL4, AL5, and RFS as the knowns, AL3 the unknown which is to be reconstructed. As before, a series of numbers representing the contacts of a bakelite separator, BS3, may be used merely as a basis of reference.

Referring now to the foregoing equations, since in (1) AL3 is at N, and AL4 at O, with AL5 at D (key LNNOD), the cipher letter X_c, when traced backwards from RFS brings one to R in NCAL3. Assume as an arbitrary starting point that the current for this letter T_p enters CW3 from the 20th contact of BS3. The letter G of NCAL3 is found beneath this contact, and hence R may be inserted under the G. Thus:

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS3------ . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                        ↓
AL3------ { N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O . . .
          { . . . . . . . . . . . . . . . . . . . R . . . . . . . . . .

AL4------ { O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P . . .
          { B L K D S X M C P Z G U Y E R T I Q F N J O H V A W B L . . .
AL5------ { 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 . . .
          { M S L A J I W C K U Q F N V X E D P G T B Z O H R Y M S . . .
RFS------ T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
                      ↑
```

Now for the second equation: T_p, key LNOOD, $= T_c$. The current will again enter AL3 from contact 20 of BS3, but AL3 will now be at O. Tracing the cipher letter T_c backward from RFS, it will be found that B must be inserted under H of NCAL3 to satisfy the equation. Thus:

```
          1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS3------ . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                        ↓
AL3------ { O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
          { . . . . . . . . . . . . . . . . . . R B . . . . . .
AL4------ { O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
          { B L K D S X M C P Z G U Y E R T I Q F N J O H V A W
AL5------ { 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
          { M S L A J I W C K U Q F N V X E D P G T B Z O H R Y
RFS------ T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
          ↑
```

Then AL3 is again slid back to key letter N, AL5 back to A, and the new placement $\frac{H}{B}$ is used as a basis for determining the next insertion in MCAL3. Thus:

```
             1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS3------    . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                                 ↓
          ┌  N O P Q R S T U V W  X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M
AL3------ ┤
          └  . . . . . . . . . .  .  .  .  .  .  .  .  .  .  R  B  .  .  .  .  .
          ┌  O P Q R S T U V W X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M  N
AL4------ ┤
          └  B L K D S X M C P Z  G  U  Y  E  R  T  I  Q  F  N  J  O  H  V  A  W
          ┌  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
AL5------ ┤
          └  H R Y M S L A J I W  C  K  U  Q  F  N  V  X  E  D  P  G  T  B  Z  O
RFS------    T Y O E U M X D F J  Q  V  K  W  B  N  S  H  C  I  L  R  Z  A  G  P
```

The new value $\frac{H}{B}$ when traced through yields K_c. Referring to the cryptogram and applying the K basic cipher-text sequence (table 9) to the text, the first coincidence is found in locus Uh, where $D_c = F_p$.

The following equations result:

GENOA (1st part) — Since D_c, key HNNOU, $= F_p$, then
D_c, key LNNOU, $= C_p$ . . . . (1)
But C_p, key LNOOT, $= A_c$, hence

GENOA (2d part) — C_p, key LNOOU, $= V_c$ . . . (2)

These two equations are now used to give an additional placement in MCAL3.

Referring to the strips, the following is the new result:

```
                    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS3-----            . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                                        ↓
         ┌ . . .    N O P Q R S T U V W  X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M  . . .
AL3----- ┤
         └ . . .    . . . . . . . . . .  .  .  .  .  .  .  .  .  .  R  B  .  .  .  .  .  . . .
         ┌ . . .    O P Q R S T U V W X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M  N  . . .
AL4----- ┤
         └ . . .    B L K D S X M C P Z  G  U  Y  E  R  T  I  Q  F  N  J  O  H  V  A  W  . . .
         ┌ . . .    U V W X Y Z A B C D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  . . .
AL5----- ┤
         └ . . .    P G T B Z O H R Y M  S  L  A  J  I  W  C  K  U  Q  F  N  V  X  E  D  . . .
RFS-----            T Y O E U M X D F J  Q  V  K  W  B  N  S  H  C  I  L  R  Z  A  G  P

                    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
BS3-----            . . . . . . . . . .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                                                                        ↓
         ┌ . . .    O P Q R S T U V W X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M  N  . . .
AL3----- ┤
         └ . . .    . . . . . . . . . .  .  .  .  .  .  .  .  .  R  B  .  .  .  .  .  .  . . .
         ┌ . . .    O P Q R S T U V W X  Y  Z  A  B  C  D  E  F  G  H  I  J  K  L  M  N  . . .
AL4----- ┤
         └ . . .    B L K D S X M C P Z  G  U  Y  E  R  T  I  Q  F  N  J  O  H  V  A  W  . . .
         ┌ . . .    U V W X Y Z A B C D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  . . .
AL5----- ┤
         └ . . .    P G T B Z O H R Y M  S  L  A  J  I  W  C  K  U  Q  F  N  V  X  E  D  . . .
RFS-----            T Y O E U M X D F J  Q  V  K  W  B  N  S  H  C  I  L  R  Z  A  G  P  . . .
                                         ↑
```

This process is continued until the entire sequence in MCAL3 is established, yielding the following:

```
AL3----  { 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
         { T S K P L D R B E I Z G J O C F W N V X U A Y H Q M
```

70. **Procedure in reconstruction of AL2.**—Having at hand AL1, 3, 4, and 5, it is now a very simple matter to establish AL2. Any deciphered message will do, and the process is thought to be sufficiently obvious to warrant its being passed over with a brief mention. By tracing through any plain-text letter, from LFS, through AL1, and the resultant cipher letter backward from RFS, through AL5, 4, and 3, the continuation point of the circuit, established in AL2 by the circuit from AL1 forward and from AL3 backward, becomes fixed. The entire AL2 is as follows:

```
AL2----  { 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
         { O R L W V J F P X M H Y G T K N C Z S U E A D I Q B
```

71. **Results of complete reconstruction.**—It is obvious that when all five cipher alphabets have been reconstructed, the translation of any cryptogram enciphered by means of the same horizontal permutation of the cipher wheels as that employed for the 10 test messages is no longer a process involving analysis, but merely one involving decipherment by manual operation

56973—34——7

of sliding strips. But suppose a different horizontal permutation is brought into play? What then?

The analysis of such messages would not be difficult. First, tables of basic cipher-text and basic plain-text sequences would be established for each one of the cipher alphabets. There would thus be five of each kind. Given a cryptogram enciphered by means of a new horizontal permutation each of the five tables of basic cipher-text sequences would be applied to the text. That table which yielded the best distribution upon the basis of single alphabet substitution for each horizontal line of text in the dispatch would immediately show which of the five cipher wheels was acting as CW5. Having determined that, a similar process with respect to the columns of the dispatch would soon show which cipher wheel was acting as CW1.

Having identified the cipher wheels acting as CW1 and 5, respectively, by applying the process elucidated in section XII, "Solution without preliminary analysis of any line of text", the message would soon yield. This would then show the positions of the other three cipher wheels, and thus any other message in the same horizontal permutation could be read by reference to the strips.

These strips would be modified in minor particulars if some or all of the cipher wheels were inserted in an "upside down" position. Each of the 10 tables of basic sequences would have to be tried to determine which cipher wheel was acting as CW5; the same applies to the case of CW1.

Section XIV

REVERSE ENCIPHERMENT

72. **Introductory statement.**—When a dispatch has been enciphered with the machine set to the normal or DIRECT position, the decipherment is effected merely by setting the machine to the REVERSE position and depressing the keyboard keys corresponding to the cipher letters. The appropriate lamps of the lightboard, corresponding to the plain-text letters are illuminated. It may be well to demonstrate how this is accomplished electrically.

73. **Study of electrical circuits in encipherment and decipherment.**—The accompanying sketch (fig. 3) is intended to show how the enciphering-deciphering reciprocity is effected. The diagram applies to only one pair of letters, viz, $A_p = Y_c$, when the effective key setting of the cipher wheels is AAAAA. When the machine is set to DIRECT and key A is depressed a circuit is established as follows: From positive of battery 1, along conductors 2, 3, through closed key A, conductor 4 to movable contact 5, which, when the machine is set to DIRECT, is in juxtaposition with fixed contact 6. Thence the current continues along conductor 7 to a contact 8 in LFS, through the cipher wheels to a contact 9 in RFS, along conductor 10 to contact 11. Another movable contact 12, touches fixed contact 11 when the machine is set to DIRECT, and the current continues along conductor 13, through lamp Y, conductors 14 and 15 to negative of battery. Lamp Y is lighted. Thus $A_p = Y_c$. There are 26 such sets of connections, one for each letter of the keyboard.

Now when the encipher-decipher set screw is turned to REVERSE what happens is that the whole set of 52 movable contacts such as those shown at 5, 16, 12, and 17 are shifted to the left so as to make contact with another set of fixed contacts, 26, 23, 31, and 20. Now suppose key Y is depressed. The following circuit is established. From positive of battery 1, through conductors 2 and 18, closed key Y, conductor 19, movable contact 17, which is now against the left fixed contact 20, conductor 21, fixed contact 11 (the connection between fixed contact 11 and movable contact 12 being broken), conductor 10, contact 9, through the cipher wheels (these being at the proper position for deciphering), contact 8, conductor 7, fixed contact 6 (the connection between movable contact 5 and fixed contact 6 being broken), conductor 22, fixed contact 23, movable contact 16 (which is now against fixed contact 23), conductor 24, lamp A, conductors 25 and 15 to negative of battery. Lamp A is lighted. Thus $Y_c = A_p$. It will be noted that when set to DIRECT the direction taken by the current is shown as being from left to right through the cipher wheels; when set to REVERSE, it is from right to left. (Of course if the connections at the battery are reversed, the directions taken by the current through the cipher wheels will be opposite to those shown, but the directions for the DIRECT and REVERSE settings will still be opposite to each other.) This change in direction is brought about by a reversal in the points of entry and exit provided by the conductors for the current, effected by the shifting of the contacts 5, 16, 12, and 17. The change in the direction of progress of the current through the cipher wheels is of no significance so far as the results of encipherment or decipherment are concerned, for after all, the direction has no effect upon the cipher resultants. It is really only the circuit established that counts, and whether the current flows through that circuit in one direction, or the opposite, the result as expressed in the form of a cipher letter or a plain-text letter, is the same regardless of the direction of the current.

74. **Comparison of results of the two methods of using the machine.**—When set to DIRECT the cipher resultants for the same plain-text letter for 26 depressions are different solely because

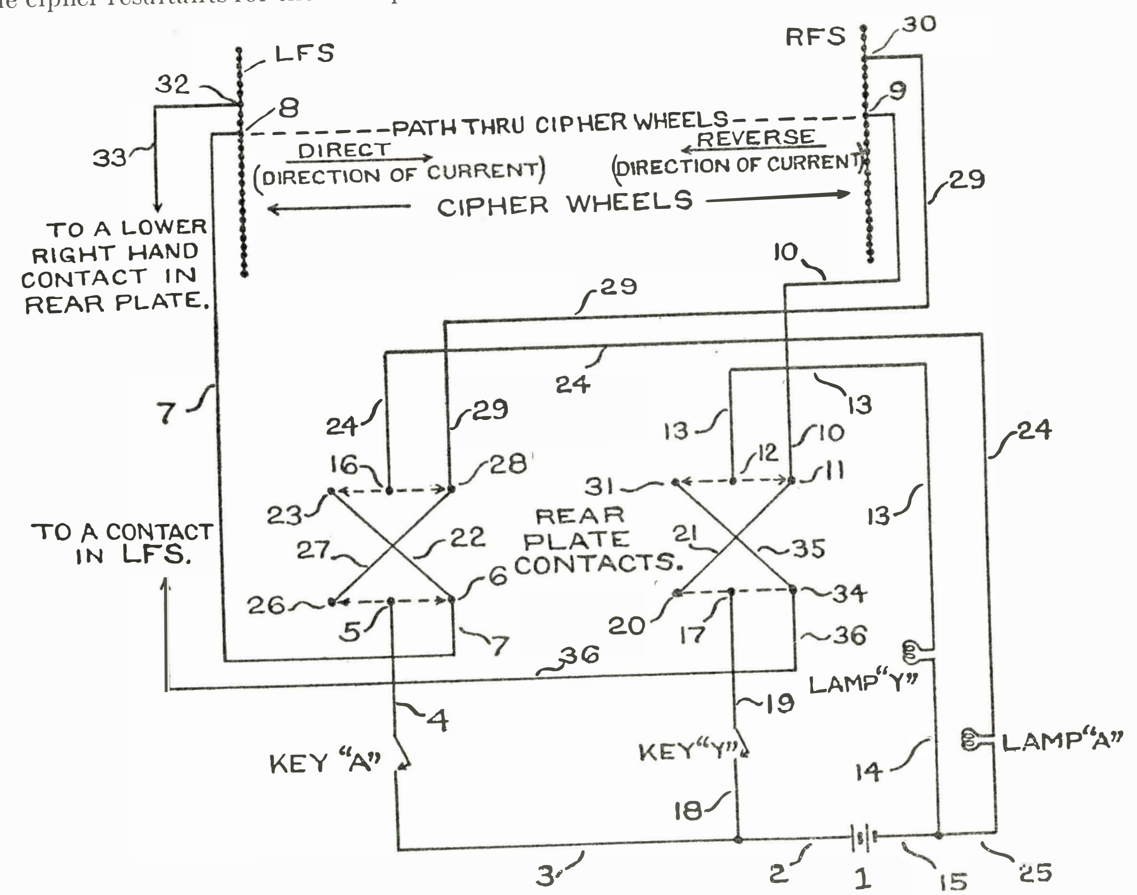


Fig. 3

of the displacements of CW5. The path taken by the current from the closed key to a contact in LFS, and thence through CW1, 2, 3, and 4, is exactly the same for all 26 depressions. The path only changes at the very end of the journey. Now suppose the machine is set to REVERSE and a message is *enciphered*. It will be seen, on reference to the sketch of the circuits, that depression of key A will establish a wholly different circuit from that previously noted when the machine is set to DIRECT. With movable contact 5 against fixed contact 26, the current flows from positive of battery 1 along conductors 2 and 3, closed key A, conductor 4, contacts 5 and 26, conductor 27 to contact 28. Movable contact 16 being against fixed contact 23, the connection between contacts 28 and 16 is broken and the current continues along conductor

29 to contact 30 in RFS. Thus a wholly different path is provided for the current into the cipher wheels than was the case with the machine set to DIRECT, and the cipher resultant will be different from that produced at the DIRECT setting. The current may emerge at contact 32 in LFS, thence along conductor 33 to the lower right hand fixed contact of some set of fixed contacts other than those shown. And while successive depressions of key A will constantly bring the current to contact 30 in RFS, the cipher resultants will all be different due to two causes: Firstly, to the successive displacements of CW5, and secondly, to the effects of this displacement upon the subsequent path taken by the current through the rest of the cipher wheels. In contrast to the case in direct operation, here the path changes at the beginning of the journey of the electric current through the cipher wheels, whereas in the direct method it changes at the end of the passage through the first four cipher wheels.

Now with CW1, 2, 3, and 4 undergoing no displacement, it is apparent that for every position of CW5 there is but one path through CW5, 4, 3, 2, and 1 for a current initiated by a given key. That is, there can be but 26 paths for each plain-text letter through the five wheels, or 676 paths for the entire keyboard (CW2, 3, and 4 undergoing no displacement). Then when CW1 becomes displaced another set of 676 paths is set up. But, when messages are arranged in lines of 26 letters (as described before), the different equivalents of the same plain-text letter falling in the same column are due solely to the displacements of CW1 so long as CW2, 3, and 4 undergo no displacement. It will be remembered that in the direct method of operation the different equivalents of the same plain-text letter in the same vertical column are also due to the displacements of CW1, but the details of the cause of the difference are not the same in both cases.

75. **Results of foregoing observations.**—It should be clear that if the machine has been used to encipher a set of dispatches with the normal DIRECT setting, and these dispatches have been solved by cryptanalysis along the lines indicated in the preceding sections, the solution of another set of dispatches enciphered with the REVERSE setting should offer very little difficulties. It has been shown how the table of basic cipher-text sequences and the table of basic plain-text sequences can be reconstructed from an analysis of the former text (DIRECT operation). Having these two tables the analysis of text enciphered by the REVERSE method, with the same horizontal permutation of the cipher wheels, is very much facilitated. The method is strictly analogous to that described in the preceding section, with modifications necessitated by the difference in the applicability of the tables of basic cipher-text and plain-text sequences. For in the direct method the cipher letters finally emerge from the RFS, and have been spoken of as belonging to the table of basic cipher-text sequences; in the reverse method, the cipher letters emerge from the LFS, and must therefore be considered as belonging to the table of basic plain-text sequences *applicable to the direct method*. In order, however, to avoid a complete reversal of terminology, no change will be made in the names designating the two tables, and it will be understood that in the reverse method the plain-text letters come from the table of basic cipher-text sequences *of the direct method*, and that the cipher letters come from the table of basic plain-text sequences *of the direct method*. As before, the letters composing the text are distributed into 26 classes. Identification of 2 or 3 classes is made by recourse to principles of frequency and repetition. Then identification of the remaining classes is made by filling in the skeletons of words suggested.

76. **Solution of illustrative example.**—An example will serve to make the process clear. The illustrative alphabets employed in the first few pages of this paper (p. 10) will be used, in

connection with which the table of basic cipher-text sequences applicable was shown as table 1, page 19. The table of basic plain-text sequences for CW1 is as follows:

TABLE 14.—TABLE OF BASIC PLAIN-TEXT SEQUENCES FOR CW1 OF ILLUSTRATIVE ALPHABETS (P. 10)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	D	G	Z	T	K	X	F	A	S	B	Y	R	P	L	W	U	Q	N	E	M	H	J	O	C	V	I
B	J	E	U	S	N	W	A	P	X	V	I	Z	L	F	D	M	G	R	K	Q	Y	O	H	B	C	T
C	U	H	O	P	Q	V	Z	K	R	C	J	B	A	M	X	G	F	E	W	T	N	I	Y	S	L	D
D	T	N	J	M	C	A	K	S	F	L	R	U	W	G	Q	O	B	V	E	P	I	H	Z	X	D	Y
E	B	V	P	J	D	C	L	Y	E	R	T	H	X	O	M	K	S	W	Z	Q	F	N	U	I	A	G
F	L	T	S	G	M	D	N	H	C	E	O	W	Z	X	P	J	A	U	F	R	B	V	Y	Q	I	K
G	C	W	R	K	Z	M	T	U	P	L	D	N	V	Q	E	A	Y	B	O	I	J	S	X	G	F	H
H	E	J	M	H	P	B	C	Q	D	S	Z	T	K	O	F	I	N	X	G	V	L	Y	A	U	W	R
I	Y	A	T	F	W	L	X	I	Z	J	G	C	R	B	S	P	E	H	Q	N	D	V	M	K	O	U
J	A	U	X	O	J	M	E	B	G	H	S	I	N	W	C	V	T	Z	L	Y	Q	F	D	R	K	P
K	F	M	D	H	E	I	U	G	A	K	Q	V	B	C	R	T	X	S	J	O	Z	P	L	N	Y	W
L	N	Z	F	A	H	U	P	X	M	O	E	C	Y	T	B	L	D	K	I	W	S	G	V	J	R	Q
M	S	O	L	E	R	N	Y	F	G	M	U	J	Q	V	T	X	W	I	D	A	K	Z	P	H	B	C
N	I	S	Y	D	V	R	G	Z	W	U	L	Q	E	H	A	F	C	O	B	K	P	M	J	N	T	X
O	R	I	Q	X	B	H	S	J	Y	W	N	K	O	E	V	Z	D	L	A	F	G	C	T	P	U	M
P	W	R	V	C	A	G	H	M	T	Z	B	S	D	P	O	E	U	Y	X	J	K	Q	I	L	N	F
Q	H	Q	K	N	X	Y	I	V	B	A	C	G	F	R	L	D	O	M	P	S	E	U	W	Z	T	J
R	M	K	I	L	Y	E	W	O	N	P	A	D	G	J	H	Z	R	T	C	U	V	X	B	F	Q	S
S	V	R	N	Q	T	S	B	C	K	F	P	O	J	U	Z	Y	I	A	H	G	X	W	E	D	M	L
T	G	L	W	B	X	P	O	R	V	Q	F	Y	U	I	J	H	K	D	M	C	A	E	N	T	S	Z
U	X	C	E	U	O	Q	R	W	L	D	V	F	I	Y	K	B	Z	P	N	H	T	A	G	M	J	S
V	P	F	A	Y	G	J	B	T	I	N	X	E	M	K	U	W	H	Q	S	D	R	L	C	O	Z	V
W	Z	P	H	W	I	O	M	E	Q	G	F	L	S	D	Y	R	V	J	U	B	C	T	K	A	X	N
X	Q	X	B	V	U	Z	D	L	O	T	H	P	I	N	W	S	J	C	R	E	M	K	F	Y	G	A
Y	O	B	A	R	S	T	J	P	U	I	K	M	C	Z	G	N	L	F	Y	X	W	D	Q	V	H	E
Z	U	D	G	Z	F	K	Q	N	H	Y	W	X	T	A	I	C	M	J	V	L	O	R	S	E	P	B

Now allocate the letters of the text of the dispatch shown below to their basic plain-text sequences. For example, beginning with the first letter, N, in locus *Um*, and referring to the table above, it will be found that the letter N, in line *m* of table 14, falls in column 6. The next letter of the dispatch, P, is found in column 23, line *m* of the table, and so on. The first letter of the second line of the dispatch, H, locus *An*, falls in class 14, because H occurs in column 14, line *n* of the table. The process is continued until all the letters have been allocated into their respective classes. The results for only the first two lines of the dispatch are shown herewith as an example of the process.

Keyword: SMITH

CW5..	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
m																					N	P	R	E	T	M
																					6	23	5	4	15	10
n	H	B	N	R	Q	B	M	W	A	J	O	Q	U	Y	R	D	C	S	L	T	V	V	K	A	E	D
	14	19	24	6	12	19	22	9	15	23	18	12	10	3	6	4	17	2	11	25	5	5	20	15	13	21
o	F	Q	U	S	K	M	D	G	Y	W	I	K	W	Q	C	N	P	N	J	R	H	Q	N	C	H	W
p	G	I	X	O	Z	V	J	B	L	R	V	D	J	G	Z	C	B	C	K	E	M	A	P	U	V	Y
q	A	L	C	O	U	I	P	R	W	O	Z	E	E	M	N	N	U	D	G	A	W	D	J	V	K	G
r	S	B	U	Y	A	X	C	R	H	B	L	G	K	Y	E	W	C	H	L	P	E	W	U	N	J	Z
s	E	K	D	J	B	N	T	M	P	O	D	J	Z	T	F	H	S	L	Q	F	D	L	W	R	H	F
t	P	Y	Y	K	O	K	K	D	F	Q	Y	J	A	Z	G	B	O	Y	R	E	Y	X	X	X	R	F
u	Y	G	N	R	X	I	H	R	P	I	B	I	W	Z	F	F	K	U	L	U	K	X	X	A	Q	A
v	D	U	X	H	L	B	S	K	C	H	O	R	R	D	N	O	N	Y	R	J	Q	S	P	O	N	X
w	W	P	A	C	Q	V	W	N	A	K	F	V	N	Y	F	F	U	Y	N	O	O	A	D	V	D	R
x	N	P	Q	J	D	R	H	A	Z	P	R	R	A	B	F	J	R	H	L	O	T	F	T	V	T	L
y	E	J	Z	W	N	Q	G	F	N	I	P															

Now it is obvious that there exists between members of the same category the same relationship here as was found to be the case in the study made of the dispatch solved in section XII. In the latter case it was observed that the determination of the value of a member of any class led directly to the determination of the value of any other member of the same class, through the intermediacy of the table of basic plain-text sequences. In this case the letters of the cryptogram having been distributed into classes according to their location in the table of basic plain-text sequences it follows that the relationship between members of the same class can be found by reference to the table of basic cipher-text sequences. For example, let us assume that the first letter of the dispatch is M_p. Since the locus of this letter is *Um*, on referring to the table of basic cipher-text sequences, table 1, page 19, the letter M is sought in column *U*. It is found in line 14 of table 1. The class in which N_c was placed is 6. There are two representatives of class 6 in line *n* of the dispatch, viz, in locus *Dn* and locus *On*. Refer now to line 14 of table 1 and find the letters in columns *D* and *O*. They are N and F, respectively. This means that if $N_c = M_p$ in locus *Um*, then R_c in locus *Dn* equals N_p and R_c in locus *On* equals F_p. Similarly the values of the rest of the members of class 6 for the whole dispatch are found by reference to table 1. It is only necessary that the correct value of one member be assumed. It was shown in section XII how the correct, or most probably correct value can be selected by weighted frequency determinations. The same method is, of course, here also applicable. When the values of 3 or 4 categories are determined by this process as indicated above the skeletons of words soon manifest themselves. It is thought that further demonstration of the process of solution is unnecessary.

77. **Solution when tables of basic sequences are not known.**—In the foregoing case it was assumed that messages enciphered upon the reverse method of encipherment were intercepted after messages enciphered upon the direct method had been solved, so that both tables of basic

sequences were already known to the cryptanalyst. The question, of course, arises: What if the reverse method were the first that had been employed? Can the dispatches be solved?

The answers to these questions also assume a two-fold form, based upon two cases. First, when the LFS and RFS are known, and second, when these sequences are unknown.

78. **Solution when LFS and RFS are known.**—In the direct method of encipherment it was shown that each horizontal line of 26 letters could be reduced to elements constituting a unique single-mixed-alphabet substitution cipher. In the reverse method of encipherment, it should be clear from what has gone before, that each vertical column of 26 letters can also be reduced to elements constituting a unique single-mixed-alphabet substitution cipher. The mathematical basis for the reconstruction of AL5 in the former case is also applicable to the latter case only it is AL1 that is to be reconstructed first and not AL5. In the former case by virtue of a knowledge of the RFS, all the letters of the cryptogram can be converted into their $NCAL5_c$ equivalents. A statistical analysis of these equivalents enables one to reconstruct AL5; this then leads to a reconstruction of the table of basic cipher-text sequences; the last process enables one to resolve the letters of the horizontal lines of text into single-alphabet distributions. It follows, therefore, that in the case of reverse encipherment all the letters of the cryptogram can be converted into their $NCAL1_c$ equivalents (since AL1 is the one concerned in producing different cipher resultants for similar letters in the same column) by a knowledge of the LFS. A statistical analysis of these equivalents should lead to the reconstruction of AL1, this to a reconstruction of the table of basic plain-text sequences, and then the letters of columns can be resolved into single alphabet distributions. Experiments with dispatches have shown that there are no difficulties in the method and it is thought unnecessary to go further into detail. The solution of the single alphabet columns will be discussed later.

79. **Solution when no sequences are known.**—In the absence of a knowledge of the LFS and RFS, the analysis is, of course, much more difficult, and a large volume of text is necessary, but it is by no means impractical of achievement. The mathematical theory of repetition and nonrepetition necessary to the reconstruction of basic sequences as developed in section V applies here to the columns of dispatches instead of the horizontal lines. If only two basic plain-text sequences can be reconstructed, the entire table can then be derived by appropriate modification of the principles elucidated in section VII.

80. **Illustration of reconstruction of a basic plain-text sequence.**—In order to test the applicability and truth of the hypotheses outlined in the preceding paragraph, a series of 50 dispatches in a known set of alphabets was prepared. In this series there were found 23 messages in which the key setting for CW1 was such that the successive members of a pair of lines were enciphered with the key settings O–P for CW1. These 23 pairs of lines were subjected to a careful frequency analysis. For example, every time L_c occurred in the O line, the letter directly beneath it in the P line was tabulated. The result was as follows:

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
|||				||		|	||	|	|		|	|			|				||	|||			||	||||/	|

The letter L was found to occur 26 times in line O, and the letter Y was found to occur most often beneath L in the P line. Refer now to the table of basic plain-text sequences (table 14), and specifically to the O line. Find L, and it will be seen that Y stands directly beneath it.

By taking the sequence LY as correct, and studying P–Q horizontal lines, to find what letter most often occurs in the Q line beneath Y in the P line, it would be found to be M, providing a sufficient amount of text were available. It is stated here that the LY sequence was selected for demonstration because it conformed to the results expected on the hypothesis, but there is

no doubt whatever that given a larger volume of text, say 100 messages, the tabulations would all conform strictly to the requirements of the theory.

When two sequences have been reconstructed by the mathematical analysis, juxtaposition of them would enable one to reconstruct the LFS, and MCAL1, and then the entire table could be reconstructed. It is thought unnecessary to make this demonstration in view of its similarity with that concerned in the reconstruction of the RFS, MCAL5, and the table of basic cipher-text sequences.

81. **Solution of columnar single-mixed alphabets.**—In the direct method of encipherment the solution of a horizontal line of cipher text is not particularly difficult because the repetitions, having been indicated, form parts of words reading horizontally. In the reverse method, however, although the words here too read horizontally, the repetitions can only be indicated in columns and therefore words are more difficult to build up. It becomes essential that the cryptanalyst work upon a whole message instead of concentrating his attention upon one or two lines. But the case here is essentially the same as that which confronts the cryptanalyst when he attempts to solve a cryptogram involving 26 mixed alphabets, with lines of superimposed text. It becomes necessary that he have a considerable number of such lines of superimposed text before solution can be attained quickly, the greater the number of lines the easier the solution. In this case, the largest number of superimposed lines that can be obtained from one dispatch is 26, because CW3 becomes displaced after 26 lines of text have been enciphered. But, given the complete key settings for a large number of dispatches, it becomes possible to superimpose lines from different dispatches, so long as the settings of cipher wheels 2, 3, and 4 are the same for all the superimposed lines. The cipher equivalents due to the displacement of CW1 can all be reduced to a common basis through the reconstructed table of basic plain-text sequences, and thus there will be at hand a number of superimposed lines of text in the same horizontal series of 26 different mixed alphabets.

If all messages emanating from one station were enciphered by the same setting of CW2 and 4, as was proposed by the manufacturers, the problem of finding a sufficient amount of text for superimposition becomes simpler, for then the messages from that station can show only 26 different settings as regards CW2, 3, and 4. For example, in a set of 50 dispatches enciphered upon this scheme there turned out to be 10 messages which, in part, were in the same setting of CW2, 3, and 4. These 10 messages yielded approximately 65 lines of superimposed text. There would be no difficulty at all in solving them upon the basis of simple frequency, after they had all been reduced to common terms, by means of the table of basic plain-text sequences.

82. **Steps thereafter.**—After solution by superimposition has been achieved, the reconstruction of the table of cipher-text sequences would be a simple matter, and would follow the lines already indicated. Then would come a reconstruction of the various cipher alphabets by application of the principles elucidated in the preceding section, and the cryptanalyst would then be in a position to solve all dispatches directly by means of the sliding alphabets.

SECTION XV

MISCELLANEOUS

83. **Cause of repetitions in the basic sequences.**—It has been stated (see pp. 30, 32) that repetition of at least one letter in each basic cipher-text sequence is an unavoidable phenomenon in this machine. It will now be shown why this is the case.

It may be stated that whenever the interval between two letters in MAL5 is the same as the interval between these two letters in the normal alphabet, that is, NAL5, then a repetition of one letter in each basic sequence is produced. Thus, for example, AL5 of the illustrative alphabets is as follows:

```
NAL5....  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
MAL5....  F R I S Y A D P L J U X Z G K O B T W C V M H E Q N
                                          -  . . . . . -
```

Consider the pair of letters B.....H in MAL5. The interval between them coincides with the interval separating them in NAL5. Therefore, whatever cipher letter is produced for θ_p when B of NAL5 is the entering point for the enciphering current, θ_p if again enciphered at six letters removed from its first occurrence must involve H of NAL5, and thus the same cipher letter will be produced for the second θ_p as for the first. Note the following diagrams:

```
                                           ↓
NAL5.  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 G H I J K L . . .
                         ┌─────────────────────┘
MAL5.  P L J U X Z G K O B T W C V M H E Q N F R I S Y A D P L J U X . . .
                         ↓
RFS...           T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
───────────────────────────────────────────────────────────────────────────
                                           ↓
NAL5.  N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R . . .
                         ┌─────────────────────┘
MAL5.  G K O B T W C V M H E Q N F R I S Y A D P L J U X Z G K O B T . . .
                         ↓
RFS...           T Y O E U M X D F J Q V K W B N S H C I L R Z A G P
```

Refer now to the first basic sequence of table 1, page 19, which reads as follows:

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

Note the repetition of X in this sequence, at an interval six. In the same table it will be found that there is a repetition in all the sequences and that the interval between the repeated letters is always six, though the letter that is repeated is different in each sequence. The constancy in the interval is due to the fact that it is always this same pair of letters, B.....H, in MAL5 that is involved in producing the repetition.

Now if there were two cases in which the same phenomenon with respect to the interval between a pair of letters in MAL5 occurred, there would be two repetitions in each of the basic sequences; if there were three, there would be three cases, and so on. If MAL5 coincided with the normal alphabet, each basic sequence would consist of but one letter repeated 26 times. Thus, the use of such an alphabet in CW5 would result in producing cryptograms completely monoalphabetic in constitution.

It is obvious, therefore, that a certain amount of care must be exercised in establishing the mixed alphabet in CW5. Normal alphabet intervals between its letters must be avoided so far as possible.

The question raises itself: Can a mixed alphabet be constructed such that the interval between no two of its letters will coincide with their interval in the normal alphabet? The answer must be in the negative in every case in which the alphabet is one composed of an even number of elements, such as ours is. Why this is the case cannot be demonstrated here, for it would require a discussion involving the Theory of Numbers, a subject beyond the scope of this paper. Suffice it to say that the best that can possibly be done in this case is to reduce the number of repetitions in each basic sequence to but one, the minimum possible number. This is of interest only in a purely theoretical way, for the occurrence of several cases of repetition in each basic sequence would not materially weaken the system.[1] It is evident that much care was taken in establishing the mixed alphabets of the test messages, for if examination be made it will be found that in no alphabet is there more than one case where the interval between two letters coincide with their interval in the normal alphabet.

84. **Recovery of cipher alphabets from a small amount of deciphered text.**—It was not long after the author had written the explanation given in paragraph 34, section VII, page 38, relative to the possibility of reconstructing AL5 from a few lines of cipher text and their equivalent plain-text, when he was afforded an excellent opportunity of testing his theories, in the form of an actual example. Private Benjamin R. Brigman, then on duty in the Code and Cipher Compilation Section of this office had, previous to his entry into the military service, been in communication with the Hebern Electric Code Co. That firm, wishing to demonstrate the security of their machine sent him a cryptogram and indicated the key. So sure were they of the secrecy of the dispatch that they felt it unnecessary to break up the cipher text into regular groups of five letters, as is usual in practice, but left the dispatch in its original word lengths, and even stated that the text was a poem in English. They challenged Brigman to solve the message.

The following is the cryptogram as submitted to Brigman:

Key: GORDON-Z, write ELEANOR

Setting of wheels: 5-4-3-2-1, with #4 and #5 inverted.

```
KB  BTR  EKSMO  DG  TNS  GDNX  AAT  XCN  ICA
IDUSEA  AJEF  HI  RGZ  TKCD  FP  AQWDJ  YD  MON
ZK  DA  JGE  ONW  HXTCHQC  WOSG  WTMCP  BN  RF
GUUKHEJ  II  XHR  WARHVH  FQ  QIKCW  HGBQLY
PWVHHROT  SMHLME  PHGEEPNFY
```

[1] In an alphabet consisting of any odd number of elements, mixed alphabets can be constructed so that in no case will there be two letters whose interval in the mixed alphabet corresponds to their interval in the normal alphabet. For a mathematical discussion of this point see A. Sinkov, *The existence of alphabets having no interval repetitions*, Technical Paper of the Signal Intelligence Section, 1934.

He fitted the following poem to the text, word for word, by their lengths, after a long search through various books of quotations:

```
KB   BTR   EKSMO   DG   TNS   GDNX   AAT   XCN   ICA
IN   THE   PHOTO   OF   HER   HERO   SHE   CAN   SEE

IDUSEA   AJEF   HI   RGZ   TKCD   FP   AQWDJ   YD   MON
THINGS   THAT   DO   NOT   SHOW   SO   CLEAR   TO   YOU

ZK   DA   JGE   ONW   HXTCHQC   WOSG   WTMCP   BN   RF
OR   ME   FOR   HER   OUTLOOK   EVER   SEEMS   TO   BE

GUUKHEJ   II   XHR   WARHVH   FQ   QIKCW   HGBQLY
COLORED   BY   HER   DREAMS   IN   WHICH   GOLDEN

PWVHHROT   SMHLME   PHGEEPNFY
SUNSHINE   GLEAMS   ENDLESSLY
```

There could not be the slightest element of doubt but that the clear text shown was correct, for the chances of finding two different pieces of clear text that would exactly fit the cipher text word-lengths, group for group, are exceedingly remote. But Brigman could not "prove" the correctness of the clear text by a cryptographic analysis. Soon after his entrance upon his duties in this section he submitted the matter to the writer, who realized the surprisingly good opportunity afforded by such a test. It may be stated that the results were entirely successful. Both Alphabets 1 and 5 were completely reconstructed, as was an equivalent Alphabet 2–3–4, and the Table of Basic Cipher-text Sequences.

85. **Procedure followed in tests.**—The first thing to do was to determine whether the DIRECT or the REVERSE method of encipherment had been employed. If the former, then the test was to find the cases in which the two cipher equivalents of one pair of identical letters in one line of text coincided with the two cipher equivalents for another pair of identical letters in the same columns but in a different line. The key indicated was, of course, of no use in the analysis, because it was evident that the key actually employed was the cipher resultant of depressing the letters of the name ELEANOR upon the keyboard, with the original setting GORDON–Z. Now it has been noted in previous work that it is most convenient to arrange the text so that the initial letter of each line gives the initial points of the various basic cipher-text sequences, in other words, so that the letter O of RAW is the key letter for the beginning of each line. In this case it becomes almost essential to do this, and provision must be made for it. The dispatch was accordingly written out in the manner shown below.

Note that each line after the first contains 52 letters so arranged that the key letter of AL5, as well as of RAW, whatever they be, can be made to apply to any column and the rest of the text be properly aligned on that basis. For example, suppose that the first letter had been enciphered with AL5 at A. Then a vertical line drawn between the Z and A columns would

properly align the rest of the text in lines of 26 letters; if the first letter had been enciphered at B, the line would be drawn between the Y and Z columns, and so on.

```
    ABCDEFGHIJKLMNOPQRSTUVWXYZA′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 {                           INTHEPHOTOOFHERHEROSHECANS
  {                           KBBTREKSMODGTNSGDNXAATXCNI
b { NTHEPHOTOOFHERHEROSHECANSEETHINGSTHATDONOTSHOWSOCLE
  { BBTREKSMODGTNSGDNXAATXCNICAIDUSEAAJEFHIRGZTKCDFPAQW
c { ETHINGSTHATDONOTSHOWSOCLEARTOYOUORMEFORHEROUTLOOKEV
  { AIDUSEAAJEFHIRGZTKCDFPAQWDJYDMONZKDAJGEONWHXTCHQCWO
d { RTOYOUORMEFORHEROUTLOOKEVERSEEMSTOBECOLOREDBYHERDRE
  { JYDMONZKDAJGEONWHXTCHQCWOSGWTMCPBNRFGUUKHEJIIXHRWAR
e { RSEEMSTOBECOLOREDBYHERDREAMSINWHICHGOLDENSUNSHINEGL
  { GWTMCPBNRFGUUKHEJIIXHRWARHVHFQQIKCWHGBQLYPWVHHROTSM
f { MSINWHICHGOLDENSUNSHINEGLEAMSENDLESSLY
  { VHFQQIKCWHGBQLYPWVHHROTSMHLMEPHGEEPNFY
g { AMSENDLESSLY
  { LMEPHGEEPNFY
```

Now note the following two cases:

In locus *Ob*, $H_p = G_c$ and in locus *C′b*, $H_p = D_c$
In locus *Oc*, $O_p = G_c$ and in locus *C′c*, $O_p = D_c$

Here there are two cases such as are necessary to be found, if the DIRECT method had been employed. The reasoning behind this is as follows:

When the direct method is used, identical letters in the same line of text are enciphered by members of the same basic cipher-text sequence. Therefore, if by chance, the same basic cipher-text sequence is again employed, and if there happens to be another case of two identical letters in another line of text, and in the same columns as the letters of the first pair, and the cipher equivalents of the second case coincide with those of the first case, then it follows that the direct method had been used. If, on the other hand, the reverse method had been used, then such cases would be impossible to be produced (this follows from the mechanico-electrical relations described in the previous analysis). Hence, it seems certain that having found such a case as that noted above, the direct method was the one employed.

The same basic test can now be used to determine where the vertical line mentioned above should be drawn, to show the key setting of CW5. Where should this line be drawn in this case? It is certain that it cannot be between columns O and C′, for then the relationship shown between the pairs $H_p = G_c$ and $H_p = D_c$ would be impossible. Therefore, the limits of the position of the line are already defined by this much: It must fall somewhere between columns C and O, or between C′ and N′.

A search was then made for (1) additional cases of the nature discussed above, or (2) a case in which the requirements as to the relation between plain-text letters and cipher equivalents are not complied with. Note the following:

In locus *Ud*, $O_p = H_c$ and in locus *N′d*, $O_p = K_c$
In locus *Ue*, $E_p = H_c$ and in locus *N′e*, $E_p = L_c$

Since the cipher letters in column U are the same (H_c) and those in column N′ are different (K_c and L_c), with the same pairs of plain-text letters involved (O and E), it follows that the vertical line must lie somewhere between columns U and N′. It has already been shown that the line cannot fall anywhere between columns O and C′ (from the preceding case) and therefore it follows that the position of the line is somewhere between columns C′ and N′.

There are no cases of repetition to be found between columns C′ and N′ and we must therefore be content with the delimitation found thus far for the vertical line.

The next step was to try to reconstruct as much of any basic sequence as possible, from the indicated repetitions of plain-text letters and their equivalent cipher letters in each line.

The writer reasoned that it was extremely likely that the LFS and RFS in the machine used to encipher this poem were the same as those in the machines submitted for examination, because, as it has already been stated (see footnote to p. 53) it seemed that the manufacturers had in mind a fixed and standard wiring for the rear plate. At any rate, it was worth the chance to make a trial.

By experimenting with a sliding strip for AL5, and the known RFS, in a short time the following AL5 was reconstructed from the partial basic cipher-text sequences resulting from a study of the text:

AL5----	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
	F	I	Z	D	T	M	P	G	A	V	U	B	H	Q	W	L	R	C	J	X	S	O	Y	K	E	N

It is not thought necessary to give the details of that work. Suffice it to say that lacking a knowledge of exactly where the vertical line should go a certain amount of experimentation was necessary before a complete MAL5 sequence could be established which would satisfy all the requirements of the text, viz, that the application of the AL5 upon RFS should yield the cipher letters shown in the cryptographic text for identical letters of the plain text. In so completing the work it was found that the vertical line must be placed between columns F′ and G′ (p. 105), and that the text should be arranged as shown below. Let the reader verify that this is the case, and also verify MAL5.

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

After MAL5 was reconstructed the entire table of basic cipher-text sequences was easily reconstructed. Following this AL1 was reconstructed by reference to the text. It was found to be as follows:

AL1----	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
	E	H	L	N	S	V	Z	C	F	K	M	Q	U	Y	D	J	P	R	W	A	G	I	O	T	B	X

Then an equivalent AL2, 3, and 4 was reconstructed, as follows:

Equivalent 2-3-4-----	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
	Y	Q	W	T	B	U	M	X	K	R	D	L	I	Z	G	E	S	F	P	V	O	N	H	C	A	J

(These are not the "converted alphabets", but the real ones; that is, in using them, a letter of the normal component is traced to the same letter in the mixed component.)

Test the following set of strips on the text, with the initial points as shown in the diagram:

LFS----	B	S	X	R	Z	T	K	D	N	G	C	H	M	V	O	L	Y	Q	E	U	P	W	J	A	I	F
AL1----	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
	E	H	L	N	S	V	Z	C	F	K	M	Q	U	Y	D	J	P	R	W	A	G	I	O	T	B	X
AL2-3-4----	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	R	D	L	I	Z	G	E	S	F	P	V	O	N	H	C	A	J	Y	Q	W	T	B	U	M	X	K
AL5----	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	X	S	O	Y	K	E	N	F	I	Z	D	T	M	P	G	A	V	U	B	H	Q	W	L	R	C	J
RFS----	T	Y	O	E	U	M	X	D	F	J	Q	V	K	W	B	N	S	H	C	I	L	R	Z	A	G	P

It is clear that by using these strips the correctness of the clear text has been established to an absolute degree. One error in encipherment (or copying ?) was found. The letter H_p of the word SUNSHINE was incorrectly designated by the letter H_c; it should have been Y_c.

It is obvious that the analyst is now in a position to solve all other messages written by means of the same cipher wheels in the same horizontal permutation. This shows how far-reaching the effects of finding even a short message with its decipherment would be in actual practice.

86. **Analysis by superimposition.**—The method of analysis of cryptograms by recourse to the principles of superimposition are, of course, among the most fundamental processes in cryptanalysis, and are resorted to only when all other methods fail. In this superimposition, letters which have been enciphered by the same secondary alphabets are brought together within the same column, and the column is then analyzed on the basis of pure frequency. When a sufficient number of letters is included in such columns, solution can always be achieved, no matter what method of encipherment has been employed, or how complex.

In the case of this machine, when the key words for dispatches are known, the principles of superimposition can be applied to this cryptographic system. It is possible, of course, to use the machine in conjunction with a code book for indicating the key words, in which case enemy cryptanalysts might have no clues as to the key word for each dispatch, providing that the code system adopted really affords the kind of secrecy necessary for the purpose. But the necessity for using a code book would constitute such a very serious disadvantage that for practical reasons it would be most advisable to dispense with such use and take chances on what information the enemy could obtain from a knowledge of the key words.

It is obvious from what has gone before, that every one of the secondary alphabets of this machine can be given a number, and that every letter of every message can be allocated to the secondary alphabet to which it belongs. If a sufficient amount of text is available, it can easily happen that 50 or more dispatches can be superimposed, thus yielding columns of 50 or more letters which then constitute the elements of single alphabet substitution ciphers. Solution of such columns is possible by recourse to the simple principles of frequency. It is unnecessary to indicate how the allocation can be made, for it will be obvious to anyone who has a thorough comprehension of the mechanics of the system of cipher-wheel movement. If every station has a different setting as regards CW2 and 4, then the traffic of the most important station may easily yield a sufficient number of dispatches for superimposition, since in this case only 17,576 secondary alphabets are involved. If the same cipher wheels and the same horizontal permutation are used for a number of days, then there would be no question about the availability of a sufficient amount of text for superimposition and solution.

APPENDIX

56973—34——8

DISPATCH NO. 1

Key: AGRAM. (Effective key: AGRBN)

LAW	CW1	CW3	CW5	RAW	
				RAW..	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
				CW5...	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
A	G	R	B	N	J
					P
B	H	R	C	O	N U T X H V Z S L U M L Z X H X H O H Y B R C L M S
					R E S I D E N T O F T H E U N I T E D S T A T E S I
C	I	R	C	O	U F C D S U F M O V K C N K Y N N G A U W Y L I Q Z
					N V I T A T I O N T O D I S C U S S P A C I F I C O
D	J	R	C	O	U T L W B Y D G O W K H R X T C J C S V G J J F Y V
					C E A N P O L I C I E S C O M E S L I K E A B O M B
E	K	R	C	O	J S R C E Z U Q K D O Y T X V T V C A S N Q P G E C
					T O J A P A N W H O W A S P R E P A R E D T O C O N
F	L	R	C	O	A R U C W L D D C U Q D X F L C B K D B E C H X D G
					S I D E R R E D U C T I O N A R M A M E N T S B U T
G	M	R	C	O	V A Y E E U Z H W R W V V P V D V M G E N J W V U U
					R E S E N T S D I S C U S S I O N A S I A T I C P R
H	N	R	C	O	E N M O Q J P U M V K G W Q C Z W K R I I X M J A C
					O B L E M S A S U N W A R R A N T E D I N T E R F E
I	O	R	C	O	L N S W E A M I A U U V W V B L E M B O S P X F R R
					R E N C E G R E A T E S T B L O W T O P R I D E A N
J	P	R	C	O	S G O W C J L V M H Y A J E Z G F Y B U D A Z L O Q
					D P R E J U D I C E I S I N V I T A T I O N T O C H
K	Q	R	C	O	U M T Z T O V T B D K W H A C H Y N Y O B N P I H R
					I N A T O P A R T I C I P A T E F O L L O W I N G J
L	R	R	C	O	T K S X F G W M N L N G O H Y M K H P G W I E B E L
					A P A N S F A I L U R E T O R E N E W B R I T I S H
M	S	R	C	O	A B L Z C J U C L J X S O U D L W U T A F I A R T U
					A L L I A N C E B R I N G S R E A L I Z A T I O N O
					↓ OTSDP
N	T	R	C	O	S N G X A Z B O H G W P Y G Z R V
					F N A T I O N S I S O L A T I O N

DISPATCH NO. 2

Key: COBAN. (Effective key: DPBBO)

```
                        RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
LAW CW1 CW3 CW5 RAW     CW5... 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

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


DISPATCH NO. 3

Key: BLOIS. (Effective key: BLOJT)

```
                        RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
                        CW5... 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
LAW CW1 CW3 CW5 RAW

B L O J T------{           P Z X X O Z W T S R S F F B X K H Y X B Y
               {           C O M P L E T E G E R M A N F I R E C O N
C M O E O------{ J N I R N L I F K V O R A R B V Z U G V A C C N B T
               { T R O L S Y S T E M A V A I L A B L E T O U N I T E
D N O E O------{ Y L P C W T O L Q D V H A Z Z G Z P G J P F E R M Q
               { D S T A T E S F O R D I R E C T S A L E S Y S T E M
E O O E O------{ U D P K F K Q E M D S O D L M O K R T D U V C A N L
               { E M P L O Y S A L T E R N A T I N G C U R R E N T A
F P O E O------{ Z Q B O R W I U P F H Q O O G X M T M I J M V U B Z
               { N D H A S A C C U R A C Y T O T W O M I N U T E S O
G Q O E O------{ G A H P N G Q R J F T L S I P N L W C K I E T H I K
               { F A R C S T O P G E R M A N S H A V E P E R F E C T
H R O E O------{ O S E R O I B J O P H X S V X G L Y U F Y A E L G K
               { E D A P P A R A T U S A L O N G L I N E S N O W B E
I S O E O------{ O L A L F V E F H R N Z D X I X Z K V B G I Q P M L
               { I N G D E V E L O P E D B Y G E N E R A L E L E C T
J T O E O------{ R Y H A Q H Q U G Q X O U K C M*P A Q U R N Z E A C
               { R I C C O M P A N Y S T O P J A P A N E S E A B O U
K U O E O------{ X N T X I C L R S Z O A A P H B I K S D C H R Y R S
               { T T O C O N C L U D E N E G O T I A T I O N S F O R
L V O E O------{ W W D Y C Q S K K U B J I Q W Q F J H N U K Z U S D
               { P U R C H A S E O F S A M E S T O P G E N E R A L D
M W O E O------{ R I B N W M S C S F M N H Q D U P P U Q L U†U R A H
               { E S C R I P T I O N I N A C C O R D A N C E W I T H
                  |↓ OXPFP
N X O E O------{ X|N G Q E D J M R W X X K R Y S V
               { M|Y R E P O R T N U M B E R O N E
```

* Underlined portion should be ZX.

† Underlined portion should be PUEDZRK.

These were errors in encipherment.

DISPATCH NO. 4

Key: AGANA. (Effective key: AGAOC[1])

```
                     RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
                     CW5..  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
LAW CW1 CW3 CW5 RAW
A  G  A  O  C ......{                               F S R U X M M F Y E P A
                    {                               N A V A L C O U N C I L
B  H  A  A  O ......{ J I U K X J S Q S G Z I R K S R Y L L R D Y C O V Z
                    { N O W I N S E S S I O N T O K Y O T O D E T E R M I
C  I  A  A  O ......{ O E E K A P N Z R Q B P O S S E P Q D X G D L T N A
                    { N E D E M A N D S A T P A C I F I C C O N F E R E N
D  J  A  A  O ......{ O P R R N F O B Z F L C K G M K C L M X L L J H V V
                    { C E P R A C T I C A L L Y A L L A G R E E R A T I O
E  K  A  A  O ......{ O H U D H V O G A K D I C S C B E Y X M P Y T R D K
                    { O F J A P A N E S E V E S S E L S T O U N I T E D S
F  L  A  A  O ......{ K V J D W D O A L J Z C Q N M W T Y U O D Y Z C O E
                    { T A T E S N A V A L V E S S E L S M U S T B E S E V
G  M  A  A  O ......{ S N W T S F Y C G P X V R V J C E Y Y V L G W P I P
                    { E N T E N T H S O R T W O S H I P S T O T H R E E S
H  N  A  A  O ......{ Y R M K Z O M C L G P C S O Z S C C A N P N X Y W Y
                    { T O P D E C I D E D T O P U T I N R E S E R V E F O
I  O  A  A  O ......{ K S K J H L L Z F N Z Q Y S B Z O L T I X M R U J U
                    { U R P R E D R E A D N A U G H T S S E V E N A R M O
J  P  A  A  O ......{ Z A M P K Q A D B R B C O R P U G J I H K A J K L K
                    { R E D C R U I S E R S F I V E C R U I S E R S A L L
K  Q  A  A  O ......{ M G S P E G R E S I F A I X Z Q F I W M A D U C F M
                    { O L D S T O P N A V A L D E L E G A T E S W I L L B
L  R  A  A  O ......{ I V D A E S I E U O Z S O B H M Q N W N D U R G O L
                    { E V I C E A D M I R A L K A T O C A P T A I N S Y A
M  S  A  A  O ......{ B G R U B H C V I Q U A U N G W
                    { M A N A S H I A N D N A G A N O
```

[1] The key as given was in error. It should have read AGANB instead of AGANA.

DISPATCH NO. 5

Key: CUNEO. (Effective key: CUNFP)

```
                     RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
LAW CW1 CW3 CW5 RAW  CW5..  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
C  U  N  F  P ......{   H K W Z A R R P B Q B I V Y S M P D M Q M V U D C
                    {   S M I T H S T A T E S C A S E S C O N T A I N I N
D  V  N  E  O ......{ E M Z X D P I D L I A W W U B Q M E Z P I X I S N H
                    { G C O N T R A B A N D W E R E P O I N T E D O U T T
E  W  N  E  O ......{ R I Q O W Y I N R C X Y M X H J Z C R H A T H S B Z
                    { O H I M B Y M A J O R R S S N I V E L Y W H O S T A
F  X  N  E  O ......{ P M L K V O U Z R S A U G O H L T K O U Z J E C X L
                    { T E D T H A T T H E Y C O N T A I N E D H O U S E H
G  Y  N  E  O ......{ S K D H W B I L E S K S W G Z G P R U I Q L H J J P
                    { O L D G O O D S O F H I S S T O P H E R E Q U E S T
H  Z  N  E  O ......{ M K D Q E U D K M I G E O J L R Z D K N N P N Y X Y
                    { E D S M I T H T O L O O K O U T F O R T H E M S T O
I  A  N  E  O ......{ H N M S S Y W Q D W D K V O B B G L U E B W M Z X D
                    { P S M I T H S A I D H E S A W S I M I L A R B O X E
J  B  N  E  O ......{ W K S A V U E A S U L C O G R Q L Z W U K I K T J Z
                    { S I N C O U R S E O F C O N S T R U C T I O N I N B
K  C  N  E  O ......{ P O W I I X H L J B H F K B W V G G L A G G Y I C Y
                    { A C K Y A R D O F S N I V E L Y S Q U A R T E R S A
L  D  N  E  O ......{ V C J A B X N D I W C C E M H G K Q Q D C B I G R I
                    { N D S A W A S I M I L A R B O X W I T H O N E C O R
M  E  N  E  O ......{ A Z E H O F O R Z F F J O N F I V S M O Q W T Z I S
                    { N E R O P E N A T P O L I C I A B A R R A C K S I N
                         ↓ OFOFP
N  F  N  E  O ......{ W|Z L I E U E Y Z P B Q E Z I Q G O P L V W B T I X
                    { T|H I S B O X H E R E C O G N I Z E D A C A S E M A
P  G  O  E  O ......{ H Q B X R Z S I V Z M C S P Z
                    { R K E D H A I G A N D H A I G
```

NOTE.—Underlined portions were incorrectly enciphered.

DISPATCH NO. 6

Key: DOVER. (Effective key: DOVFS)

```
                   RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
LAW CW1 CW3 CW5 RAW CW5... 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
                   CW1
D O V F S------{          L P I O U E Z K S J B X C A F E U K S D W H
               {          W U S F O R C E O F T W E N T Y F I V E T H
E P V B O------{ R Y S N W A N I P U J M Z A H O U Y V U V O E C N B
               { O U S A N D M E N E X E C U T I N G N O R T H E R N
F Q V B O------{ S M P N L Q A P T A G G V H R M Z V B N Z I I X P B
               { E N C I R C L I N G M O V E M E N T C H A N G S P O
G R V B O------{ O L Y X B S S M B W L H V X V S P Z I K O G O O C C
               { S I T I O N V I C I N I T Y O F R I V E R B E C A M
H S V B O------{ F E K X M R A L N V R S K A E S D S M T G R X S Y P
               { E U N T E N A B L E C H A N G S A R M Y I S W I T H
I T V B O------{ S M G S G Z B V D E N W Z S I V J E S V W Y J R G X
               { D R A W I N G I N T O M A N C H U R I A F O R R E O
J U V B O------{ E P I X V E J E B H I F G S V P X X G A Z C Q C Z S
               { R G A N I Z A T I O N W H E R E W U I N A L L P R O
K V V B O------{ F R I V W W D G V A H G H Q L V L M V B U S W X Y Z
               { B A B I L I T Y W I L L N O T F O L L O W F O R F E
L W V B O------{ I N W W T N K V B Z U Y R T P M R W P I C V Q Z P D
               { A R O F C O M P L I C A T I O N S W I T H J A P A N
M X V B O------{ N X C E W Y R M H D W N P Z L W C C N X W T L V K G
               { D U R I N G W H O L E C A M P A I G N W U W A R N E
                   ↓ OYWCP
N Y V B O------{ L|F E N T M E G L C U M E V K H Z Y N A H D S T J L
               { D|A L L A M E R I C A N C I T I Z E N S T O L E A V
P Z W B O------{ D H J B N I Q W N W A T I T L S J F U A R Y N W L E
               { E I M M E D I A T E L Y A N D S H O W E D G R E A T
Q A W B O------{ F K O S P S C F A Z W S N T Q Y B X Q M G G V A N
               { P E R S O N A L B R A V E R Y R E M A R K A B L E
```

NOTE.—Underlined portion was incorrectly enciphered.

DISPATCH NO. 7

Key: GENOA. (Effective key: GENPB)

```
                   RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
LAW CW1 CW3 CW5 RAW CW5... 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
G E N P B------{                           B Y P F M L W Q Y S D Z U
               {                           G E R M A N C O N T R A C
H F N C O------{ W X Q G M G X N K T R V K V T T B Y T P V D Z T N N
               { T S F O R Y E A R C O N T E M P L A T E S F O R C U
I G N C O------{ N R O T L D H S W W G M I P B Z Z C G P G P R V T B
               { T T I N G U P B R I T I S H W A R S H I P S A S F O
J H N C O------{ M B Y B U Q Q O U R Q D M D B N E Q D S B H Y C Z J
               { L L O W S A P P R O X I M A T E L Y F O R T Y T H O
K I N C O------{ X S J R L I G G D J D V A T H Y W R U W X L B Y Y I
               { D I C F J E A M M F S Q M R S A Z D Y A W G R H N C
L J N C O------{ L J Y V T N D B Q T Z W H X D Q C C G M O U R Y X W
               { L U D I N G S I G H T S U P P O S E D F O U R L A R
M K N C O------{ C T B J P N R M F F O V L Z Q D V B Z Q A T O C Q Z
               { G E C R U I S E R S T H R E E S M A L L C R U I S E
                   ↓ OLODP
N L N C O------{ E|W D K L W H H P V W A U T U N K A E I S J T B Z P
               { R|S F O U R T E E N I N T R O D U C E D A N D T H R
P M O C O------{ I L L V M K Q B O Y X J M H U K F H B G X S A H Z O
               { E E M O N I T O R S S T O P T H E S E V E S S E L S
Q N O C O------{ O I Q N M G M O G Y B W U H Y F K O T S P L I B O F
               { H A V E B E E N P U R C H A S E D O U T R I G H T A
R O O C O------{ E W K D Y A D X Z S N X L J Q W O S K U R L E O G L
               { C P B L T Z C Z Z C Z B T X U D T K D V A Q E L O R
S P O C O------{ S V Z W W G O Y Q C W J S A D P S O Q U Y H D S U R
               { T S T W O B A T T L E S H I P S O F D A N T O N C L
T Q O C O------{ S E N X T M F T Q Y L O S W U M J L P V A Q K T
               { A S S P U R C H A S E D F O R S C R A P P I N G
```

Note.—Underlined portions were incorrectly enciphered.

DISPATCH NO. 8

Key: HAGUE. (Effective key: HAGVF)

```
LAW CW1 CW3 CW5 RAW   RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
                      CW5... 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

H A G V F ......{                                      S Y Y G S T X V P
                {                                      H A V E A B S O L

I B G E O ......{ M A G V Q J T A R Q R M F L A H W T Z L B H T V D R
                { U T E L Y R E L I A B L E I N F O R M A T I O N T H

J C G E O ......{ O H H B H P D Q N T K Q Q H S F J M C F O J A A M K
                { A T G E R M A N G O V E R A R T M G H A Z E A Q Y A

K D G E O ......{ W Y S X V B I W O A J Z G Z E J A D C K W Z K R I I
                { W A R D E D C O N T R A C T T O F I R M F O R D E S

L E G E O ......{ T I N O V U O Z P Y L H T Y S R P W G L R V Y F G B
                { T R U C T I O N O F W A R S H I P S H E D F R I E D

M F G E O ......{ A I H P U C B R K O Z U G C C H W Z D I X G R B A P
                { R I C H S H A F F N I N T E R A L L I E D A E R O N

                   ↓ OGHFP
N G G E O ......{ Z|G C U N V K U A T D Y X V E K N W Y X R V P D W K
                { A|U T I C A L C O M M I S S I O N N O T I F I E D Y

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

Q I H E O ......{ Z I F O D O F Z I F T E L V M U D C B V P O P T N O
                { R K O F D E S T R U C T I O N M U S T C O M M E N C

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

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

T L H E O ......{ V R Q G B S N J H B S P X Q V S U M H K W Y I B C Y
                { M I S S I O N I S E X E R T I N G P R E S S U R E O

U M H E O ......{ H O W F V F J N N A U J F L S C O
                { N G E R M A N G O V E R N M E N T
```

NOTE.—Underlined portion represents error in encipherment.

DISPATCH NO. 9

Key: MONTE. (Effective key: MONUF)

```
LAW CW1 CW3 CW5 RAW   RAW..  O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
                      CW5... 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

M O N U F ......{                                      H D R Y Y Z Y T O
                {                                      Z E P P L I N C O

                   ↓ OPOEP
N P N D O ......{ U|J J S L S W C R N U L S A E X T G W P Z Y V G I V
                { M|P A N Y A C C E P T A L L G E N E R A L C O M P R

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

Q R O D O ......{ O V D U Q Z T H H S Y G E G K O A Q F Z H X R P M H
                { X I O U S T O P R O C E E D A S S O O N A S P O S S

R S O D O ......{ Y Z T J L I U N X X U J A I V S S T F X T Z L J V U
                { I B L E T I M E T O E X E C U T E O N E Y E A R B U

S T O D O ......{ V E Y Y G O D Z L N M L V K U O F R X H V K I H P F
                { T T H E Y P R O P O S E S E V E R A L M O D I F I C

T U O D O ......{ L N C E L F Q F S Q Z S W H L E H D T G S B U H E T
                { A T I O N S W H I C H D E P A R T M E N T S H O U L

U V O D O ......{ U Z A C A M H V P D J Z K I F A J G V O R H X O D J
                { D C O N S I D E R A N D W H I C H A R E I N M A I L

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

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

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

Y Z O D O ......{ C U Z Q W D V W Q X Z E N E Q E S H C E C L U H P S
                { O M P A N Y C A N P R O C E E D F U R T H E R I N T

Z A O D O ......{ H E X G E K O E
                { H E M A T T E R
```

DISPATCH NO. 10

Key: NEPAL. (Effective key: OEQBM)

LAW	CW1	CW3	CW5	RAW	
				RAW	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
				CW5	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
O	E	Q	B	M	Z N / A R
P	F	Q	D	O	S I I B X A R U N D E G X D Z M M Q X Y A Y T F G B / M Y G E N E R A L S T A F F C I R C U L A T I N G J
Q	G	Q	D	O	E U Z W C L G R B M Q K T C C G H V P T F A B X D H / A P A N E S E P R O P A G A N D A H E R E A N D C H
R	H	Q	D	O	H U D X Z S P N O L Y V C T R E C G J S E A J L W T / I N A S T O P U N I T E D S T A T E S M I L I T A R
S	I	Q	D	O	P M L J B R Y O M C V T N P Q P Y D M N T S C P U F / Y A N D E C O N O M I C A L M E N A C E S T O P H E
T	J	Q	D	O	E X V M N P X Q Y I I R F X Z Z G K G Z T C Y D V W / R I N T E R F E R E N C E C H I N A A N D S I B E R
U	K	Q	D	O	Q I A F M V D U F C L Q J A G C Z A B B D K T I U E / I A C O M P E L S J A P A N T O B U I L D A N M A X
V	L	Q	D	O	J Y W P O T P F G W L B X M M B D J V L F Q F Q W T / N T A I N N A V Y B E Y O N D M E A N S S T O P W I
W	M	Q	D	O	P X D J K B X C N I F S C M G S T G B T O R E M T E / L L I N G T O M A K E S O M E R E D U C T I O N B U
X	N	Q	D	O	K L H C C U P D Q X C P T F O B L M V Y Z R I R M V / T M U S T R E T A I N N A V A L S U P R E M A C Y O
Y	O	Q	D	O	H D G G H V T F W Q R Q F H K H N L X Q J I T N C S / F W E S T E R N H E M I S P H E R E P R E V E N T A
Z	P	Q	D	O	G S N S E J Q W R B I U K V G T O U E T B W P L C J / M E R I C A F R O M E V E R I N T E R F E R I N G I
A	Q	Q	D	O	Y C X Q T B P J D M U S I R O K Y M A D O B V U P Z / N T H E I R D O I N G S I N T H I S P A R T O F T H
B	R	Q	D	O	M B K H V B / E W O R L D

Note.—Error in underlined portion.

TABLE 15.—TABULATION OF $\overset{1}{\theta}_1 \overset{4}{\theta}_2$ PAIRS IN TEST MESSAGES

	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	4	9	2	3	5	4	6	8	7	8	1	6	4	4	5	3	3	7	1	8	5	4	5	5	6	7	A
B	9	2	11	4	7	7	8	3	6	5	4	8	6	7	5	7	2	9	8	3	2	4	6	3	10	7	B
C	2	8	2	7	3	4	5	5	1	4	1	6	6	7	3	4	7	10	6	4	4	5	3	5	7	7	C
D	5	2	5	4	8	5	5	1	5	2	7	6	2	3	6	6	1	3	6	16	9	4	3	8	9	6	D
E	4	4	3	5	7	1	9	4	2	7	2	9	3	3	9	7	8	2	5	7	6	8	4	1	4	3	E
F	5	6	5	4	5	7	7	5	5	7	8	4	2	4	4	2	5	8	4	3	3	3	4	7	5	10	F
G	1	9	7	4	5	3	7	3	6	4	5	4	3	1	6	8	5	3	7	5	3	1	5	5	6	9	G
H	4	1	5	2	3	6	3	10	8	4	8	4	3	4	3	4	7	4	4	7	2	5	7	6	8	7	H
I	8	3	3	5	3	5	4	4	10	4	7	2	5	1	6	2	0	8	6	7	9	8	2	3	6	9	I
J	6	6	12	6	2	4	2	5	0	4	7	3	4	6	1	5	6	5	6	8	3	2	5	5	2	6	J
K	6	3	3	5	3	9	7	6	3	8	5	5	4	8	4	2	2	8	3	4	6	0	3	8	3	5	K
L	4	4	1	5	2	3	4	6	8	0	2	5	4	1	4	6	3	5	7	3	11	6	10	8	8	7	L
M	5	2	4	6	7	4	3	3	7	4	2	2	2	3	3	6	5	3	3	4	6	4	6	1	3	2	M
N	4	2	6	7	8	3	2	5	5	2	2	3	2	3	5	5	1	10	10	7	2	2	3	8	6	1	N
O	3	5	8	6	4	9	1	5	2	5	5	5	3	3	9	0	11	3	4	4	5	6	3	6	8	4	O
P	0	6	2	6	2	12	4	4	8	3	5	3	3	7	4	4	4	9	3	7	5	6	2	2	5	5	P
Q	3	6	3	0	5	1	3	7	3	4	3	7	5	5	9	4	2	3	8	1	7	8	8	4	7	3	Q
R	7	10	2	3	7	3	7	5	5	8	8	4	3	5	9	2	3	7	6	6	5	8	2	6	8	6	R
S	8	6	10	6	7	5	8	5	4	3	4	6	8	3	4	6	2	3	8	9	5	3	4	6	6	7	S
T	6	12	3	6	6	2	8	4	4	7	7	4	4	2	7	8	6	8	8	4	10	7	9	3	9	5	T
U	7	7	4	13	7	5	2	5	2	5	7	5	4	9	3	2	5	4	5	5	4	6	2	10	3	7	U
V	3	6	7	7	6	6	5	6	4	3	6	1	7	7	3	6	7	9	5	5	1	7	5	7	2	2	V
W	9	7	4	4	2	4	4	3	2	6	4	6	3	4	4	1	3	4	6	6	8	4	7	10	3	4	W
X	5	9	6	3	2	5	6	5	3	11	4	4	4	7	2	10	6	3	7	5	9	4	5	7	5	6	X
Y	10	6	2	6	4	4	5	5	13	4	8	15	8	5	3	5	7	6	2	12	4	8	5	4	5	3	Y
Z	6	8	7	9	4	13	5	3	5	4	2	3	3	5	3	5	9	6	6	2	5	6	6	3	10	4	Z
	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	

Column headings: $\overset{4}{\theta}_2$; row headings: $\overset{1}{\theta}_1$.

TABLE 16.—TABULATION OF $\overset{1}{\theta_1}\ \overset{6}{\theta_2}$ PAIRS IN TEST MESSAGES

$\overset{1}{\theta_1}$ \ $\overset{6}{\theta_2}$	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	5	6	6	4	4	4	4	4	7	3	10	2	4	5	0	7	2	5	1	5	6	6	4	6	5	8
B	8	4	5	6	2	7	2	4	7	3	3	6	2	5	3	3	9	10	5	3	2	3	8	6	10	4
C	3	12	6	8	1	6	1	3	1	4	6	5	5	3	5	6	3	5	2	4	4	3	4	4	5	3
D	1	3	4	4	1	8	5	5	7	7	5	6	0	3	5	5	8	3	6	3	3	6	5	8	6	9
E	1	9	5	2	1	5	3	2	3	6	6	5	2	4	5	4	3	7	5	4	6	4	6	6	5	5
F	7	3	5	7	6	1	4	9	4	4	3	3	5	4	3	8	6	5	1	8	7	1	1	5	4	5
G	4	7	6	3	4	4	8	4	5	5	5	4	5	4	6	2	5	5	4	4	6	5	3	3	9	5
H	6	9	2	6	4	7	3	2	2	4	7	9	4	2	6	1	7	4	6	2	1	4	4	3	7	4
I	5	4	4	6	3	5	5	4	2	6	4	6	1	2	5	1	3	5	4	8	3	3	2	7	11	6
J	2	6	2	2	6	5	5	3	4	2	4	7	4	3	4	3	1	2	6	6	7	10	7	1	4	3
K	5	4	6	3	6	6	3	5	4	4	5	1	6	7	6	5	3	3	4	2	2	9	3	3	3	4
L	7	4	3	7	10	6	1	6	0	3	3	4	8	2	5	4	5	4	5	8	2	5	4	4	6	4
M	4	5	3	3	5	1	8	3	5	1	2	2	2	5	4	3	3	4	2	3	7	5	2	2	5	5
N	3	3	3	5	2	2	2	7	6	1	3	7	5	1	4	7	4	4	1	3	4	4	3	7	3	5
O	4	4	8	6	1	2	8	5	3	3	5	3	3	4	1	1	3	3	10	7	4	3	6	6	8	7
P	7	2	5	5	3	4	3	4	5	4	6	2	1	6	1	3	2	5	7	2	4	3	5	4	7	7
Q	2	1	4	4	8	3	3	8	3	7	1	5	3	3	1	5	4	4	5	7	10	1	4	4	5	4
R	4	3	3	3	5	3	5	3	8	10	1	5	5	7	4	3	7	5	8	10	2	7	5	10	6	5
S	4	6	6	5	5	3	6	6	6	2	4	9	9	1	5	3	4	6	4	6	8	7	7	5	4	1
T	10	8	5	6	4	6	3	5	4	4	5	1	4	8	7	3	3	8	5	5	7	4	5	8	4	10
U	5	3	5	5	4	4	5	2	4	8	1	3	5	1	5	6	4	4	4	7	6	7	5	13	4	4
V	5	4	2	5	4	7	7	4	1	7	7	5	0	7	4	4	2	8	9	4	6	3	2	2	8	3
W	4	4	3	5	4	7	8	0	11	3	0	4	3	3	6	4	6	9	5	8	2	2	5	4	5	2
X	4	9	4	3	7	5	6	5	4	4	3	4	1	5	9	4	7	3	7	7	7	7	4	2	1	7
Y	8	3	4	8	8	6	9	6	8	6	1	7	5	1	10	7	4	7	6	11	4	5	3	4	2	5
Z	3	5	5	3	6	3	6	9	4	1	7	4	7	6	5	4	5	5	6	8	2	3	9	3	9	6

TABLE 17.—TABULATION OF $\overset{1}{\theta_1}\ \overset{7}{\theta_2}$ PAIRS IN TEST MESSAGES

$\overset{1}{\theta_1}$ \ $\overset{7}{\theta_2}$	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	9	2	2	2	3	7	4	8	3	6	6	6	4	2	3	3	4	7	7	5	11	4	2	4	5	2
B	4	5	3	1	6	2	3	3	7	5	2	5	12	2	5	7	5	5	4	7	7	5	3	7	9	6
C	3	5	5	5	2	2	5	3	8	3	5	5	4	5	1	4	3	2	3	5	3	9	5	4	6	8
D	7	8	0	8	4	3	2	3	4	6	3	8	5	3	15	4	4	6	6	3	1	1	2	5	4	8
E	3	4	2	3	6	2	1	5	3	2	4	1	5	7	3	4	4	6	4	7	3	3	4	7	12	7
F	6	2	4	6	1	3	7	3	6	5	3	5	7	2	4	9	3	4	4	1	5	6	5	7	5	5
G	4	4	6	5	1	3	10	4	4	2	2	3	1	2	4	6	6	8	4	5	6	7	2	6	11	5
H	8	7	4	6	3	5	4	6	1	7	3	2	2	1	0	6	2	6	10	12	2	8	5	0	4	4
I	4	2	7	1	3	10	6	4	7	3	5	7	3	1	3	5	2	5	5	6	6	3	5	2	2	5
J	2	4	6	3	5	4	5	3	6	4	4	1	4	5	6	6	7	4	2	2	4	5	3	2	5	6
K	1	4	4	5	5	5	5	5	2	2	4	5	2	3	3	2	6	5	3	6	4	4	6	6	5	5
L	7	6	6	2	2	7	1	2	3	6	4	1	4	7	4	4	5	7	10	5	7	1	3	5	5	4
M	4	4	2	6	4	3	1	4	6	3	3	1	3	7	3	2	3	4	3	3	2	3	7	6	3	3
N	2	7	4	4	1	2	7	3	1	5	8	1	6	1	1	2	4	6	9	1	6	2	4	6	2	4
O	7	6	1	8	6	6	4	3	4	2	3	8	1	3	6	3	7	4	5	5	1	7	5	3	5	4
P	3	2	5	3	7	9	4	9	8	2	4	6	3	3	8	3	3	2	2	2	5	2	0	6	3	5
Q	3	1	7	7	5	6	1	5	6	1	12	4	4	4	2	3	2	3	3	2	4	4	0	5	6	6
R	3	6	2	7	4	6	6	6	1	9	2	4	2	8	7	4	9	3	6	13	6	4	4	5	5	4
S	5	6	13	3	2	8	4	5	4	5	3	7	1	3	3	4	2	7	2	8	5	3	8	4	9	6
T	2	8	8	5	5	6	4	5	7	5	5	3	4	0	6	4	6	7	7	3	10	5	6	5	11	5
U	6	10	5	5	4	4	8	5	4	5	3	5	4	1	3	3	6	7	3	8	2	6	6	6	1	5
V	9	4	2	2	5	3	7	2	5	4	4	8	5	5	3	3	1	5	5	12	5	2	4	4	5	4
W	5	2	5	5	6	5	8	2	6	3	3	4	3	11	3	3	2	2	4	4	3	8	6	4	3	3
X	5	14	4	6	6	2	7	4	2	2	5	4	0	4	9	3	2	6	4	6	4	4	7	10	6	5
Y	8	1	1	7	7	7	5	9	7	6	4	8	3	6	6	3	4	5	5	6	6	4	7	5	4	9
Z	3	2	7	6	7	3	3	3	3	6	5	5	4	4	9	5	6	4	9	7	1	8	5	7	7	2

TABLE 18.—TABULATION OF $\overset{1}{\theta}_1\ \overset{10}{\theta}_2$ PAIRS IN TEST MESSAGES

$\overset{1}{\theta}_1$ \ $\overset{10}{\theta}_2$	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	5	3	5	5	9	8	6	5	1	2	5	5	2	3	3	8	4	5	4	3	3	8	6	5	3	4
B	9	5	6	4	8	6	3	5	6	4	7	4	6	7	1	7	4	5	3	3	0	2	4	7	5	5
C	4	4	2	4	5	7	1	4	5	6	7	3	3	4	4	5	3	6	4	7	2	4	3	4	6	2
D	4	8	3	3	4	6	4	4	2	2	2	7	3	1	5	8	7	5	3	8	1	2	7	5	11	4
E	5	3	1	5	5	3	4	5	2	4	2	4	2	1	8	3	2	6	6	9	7	6	3	7	6	4
F	4	6	4	3	4	9	5	5	2	4	3	4	3	6	4	8	5	4	5	7	6	2	3	6	3	6
G	5	3	4	1	6	5	6	2	4	3	4	3	5	3	6	1	6	8	11	4	3	5	6	7	6	3
H	3	6	4	7	2	4	5	4	3	6	7	5	4	5	0	4	4	4	4	7	3	5	2	5	7	3
I	5	5	2	3	4	2	5	8	5	4	4	2	2	4	3	2	1	8	2	5	6	5	5	7	6	5
J	3	5	4	4	2	3	6	5	8	5	1	4	4	3	3	1	5	7	2	3	3	10	1	6	5	3
K	5	4	3	5	5	6	2	3	2	5	2	6	3	0	6	4	6	3	7	6	2	5	3	3	6	5
L	8	8	6	4	3	8	7	3	5	2	5	4	6	3	3	2	1	6	3	0	2	5	15	4	2	3
M	2	3	1	2	3	3	5	5	4	1	4	3	5	5	3	0	2	5	5	5	9	3	3	4	2	5
N	4	5	2	6	2	3	5	4	6	4	1	5	2	8	4	1	4	4	3	6	1	2	4	4	3	7
O	5	5	4	5	6	2	6	3	11	4	3	7	4	4	2	4	3	2	6	3	5	4	4	3	5	6
P	1	10	5	2	4	6	1	6	4	6	3	2	6	3	6	1	4	3	2	8	3	6	3	3	5	3
Q	2	3	3	5	9	6	6	4	8	3	4	3	1	5	2	2	6	3	6	6	3	4	5	7	1	5
R	4	3	10	7	3	2	8	5	6	1	5	4	5	8	5	7	2	6	9	4	4	5	4	6	7	4
S	3	6	7	11	4	0	6	5	3	5	6	4	7	4	4	2	7	6	2	4	6	3	2	7	9	5
T	2	2	7	4	4	4	4	1	6	7	3	7	3	5	7	8	6	6	5	6	10	10	6	4	7	5
U	3	4	6	4	3	4	6	3	4	4	2	3	2	2	7	3	4	4	6	7	8	9	4	5	9	6
V	7	8	4	6	3	5	4	4	7	3	5	6	2	2	6	4	1	4	5	7	1	1	4	4	7	7
W	13	6	3	5	1	5	1	4	1	3	6	7	8	1	5	4	2	4	4	4	6	2	3	5	6	4
X	4	3	4	6	4	3	4	4	3	7	5	2	6	1	4	7	6	8	7	5	7	4	7	4	5	7
Y	3	3	7	3	7	5	5	6	5	2	12	5	3	1	4	5	6	5	9	8	11	1	5	3	4	9
Z	6	2	5	5	2	5	7	4	4	9	2	5	0	5	10	6	5	5	4	4	6	4	4	5	4	9

TABLE 19.—TABULATION OF $\overset{1}{\theta}_1\ \overset{13}{\theta}_2$ PAIRS IN TEST MESSAGES

$\overset{1}{\theta}_1$ \ $\overset{13}{\theta}_2$	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	5	6	3	5	6	4	7	4	9	6	6	5	4	3	6	3	1	5	10	1	5	4	3	3	4	1
B	6	3	2	2	6	3	3	5	6	6	8	6	2	7	6	3	2	3	7	5	3	9	6	7	5	6
C	3	2	7	5	7	5	9	3	5	1	8	2	1	3	5	3	2	4	2	6	4	5	6	2	4	5
D	3	6	5	3	2	6	2	4	3	2	7	11	5	2	6	6	2	6	6	5	4	4	6	4	2	5
E	6	5	6	4	3	7	3	10	4	3	5	3	3	1	4	3	6	5	10	3	3	2	4	2	5	6
F	2	5	4	6	8	5	5	5	4	4	3	3	2	5	4	3	3	7	8	4	6	5	4	5	8	4
G	6	2	3	6	5	7	3	5	5	8	4	3	3	3	5	2	4	7	4	10	2	4	8	5	5	5
H	4	6	5	4	3	6	3	2	4	6	4	2	6	6	4	6	3	4	1	7	9	3	4	3	4	8
I	5	7	4	6	2	4	9	4	3	3	5	10	6	3	1	4	3	3	4	6	1	5	4	4	7	1
J	6	3	5	8	5	4	5	2	6	3	1	2	4	3	5	3	8	3	3	3	2	4	1	5	7	6
K	1	7	6	4	4	3	6	3	3	0	1	1	1	6	8	6	2	5	4	10	7	7	1	6	7	5
L	5	3	2	7	4	4	4	4	4	3	3	5	4	3	4	3	4	6	5	8	3	2	4	12	6	3
M	0	6	5	3	3	1	5	3	2	6	2	5	4	4	2	5	1	6	3	3	5	5	3	3	3	5
N	5	2	4	4	0	4	5	5	6	5	4	4	3	7	3	0	1	4	5	3	5	3	4	5	5	3
O	6	4	1	3	6	7	1	5	4	2	12	6	3	2	5	3	3	5	2	4	7	2	1	7	8	7
P	7	8	6	3	2	3	6	8	4	5	5	2	0	3	1	6	7	4	6	3	4	4	3	4	1	7
Q	5	7	1	7	4	6	3	2	7	7	2	1	4	2	4	2	7	9	3	4	4	3	2	4	6	4
R	2	4	7	5	4	3	7	4	3	8	3	6	4	4	10	6	9	2	5	6	3	4	7	6	7	2
S	6	3	5	4	6	2	4	4	4	6	6	9	4	0	2	3	4	4	7	9	6	13	8	3	6	4
T	3	2	4	6	9	6	6	6	10	1	0	4	7	5	9	8	3	7	4	7	5	9	6	10	3	5
U	5	7	2	3	5	6	5	7	3	3	2	3	4	2	4	7	8	8	4	6	3	3	2	6	3	10
V	3	5	6	5	5	5	6	2	3	3	0	5	5	1	5	1	7	7	5	9	7	1	3	3	9	8
W	4	2	5	3	3	4	6	4	5	3	5	6	5	4	1	7	3	6	6	3	6	4	6	3	6	5
X	7	7	5	3	2	4	3	4	2	4	3	3	10	6	7	4	5	6	5	8	4	2	5	8	6	5
Y	6	8	7	6	2	7	6	5	6	6	6	4	4	10	2	5	8	8	7	4	6	6	5	8	5	1
Z	7	8	7	5	6	6	2	5	3	4	4	6	2	6	4	4	5	2	2	9	9	5	4	5	11	6

56973—34——9