An Introduction to Methods for the Solution of Ciphers

William F. Friedman

Publication No. 17

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918

ON THE FLEXIBILITY OF MIND NECESSARY IN CIPHER WORK

Deciphering is both a science and an art. It is a science because certain definite laws and principles have been established which pertain to it; it is also an art because of the large part played in it by imagination, skill, and experience. Yet it may be said that in no other science are the rules and principles so little followed and so often broken; and in no other art is the part played by reasoning and logic so great. In no other science, not even excepting the science of language itself, grammar, does that statement, "The exception proves the rule," apply so aptly. Indeed it may be said, and still be within the limits of the truth, that in deciphering, "The rule is the exception."

The reason for this is not hard to see. If one is dealing with a problem in physics, for example, a problem dealing with the temperature, pressure, and volume of a gas, the solution of the problem may be attained directly and with almost absolute accuracy, because the underlying laws are invariable and unchanging in their application. Because of this, the problem resolves itself into a problem in mathematics. From the very nature of mathematics, the results are absolutely predetermined. The data having been given, the solution is reached by a series of definite and unerring steps, subject to no modification whatever, because the results, being dependent on nothing but the data, are fixed from the start. Each step follows inevitably from the preceding. No imagination is at all necessary; no assumptions need be made, which may prove to be untenable and therefore must be rejected and replaced by others.

Contrast this situation, on the other hand, with that which confronts the decipherer at the very beginning of his attempts to solve a problem. Many times the cipher carries with it not even so much as an indication of the particular language in which it is written. Granted, however, that he knows the language, the foundations of any language are so unstable, so variable, and so uncertain, that no absolutely fixed laws can be made to hold. This does not refer to the innumerable variations in inflection, conjugation, etc., with which every language has to contend, but refers particularly to the very roots from which a language springs — the elementary sounds, the elementary syllables, and the words, phrases, and sentences. There is no rule, and there can be no rule, to determine the sequence of sounds, there can be no law which says that sound "ay," for example, must always be followed by sound "em," or any other sound. There can be no rule which determines how many letters shall compose a syllable, how many syllables shall constitute a word; nor what words shall follow any given word. Indeed, the characteristics which distinguish a good writer or speaker from a poor one, are exactly those which are concerned with the flexibility with which the former employs and manipulates the words, phrases, and sentences. A single idea may be expressed in a multiplicity of ways, all differing markedly from each other. Furthermore, the nature of the text as a whole varies. For example, scientific text differs materially from literary text or military text.

All such conditions affect the raw material with which the decipherer must work — the letters themselves. Therefore, only the most generalized rules can ever apply to deciphering operations; and there can be only a few guiding principles, which the decipherer should always be ready to modify. The most important generalizations, for instance, are those which have been derived from what are known as frequency tables, which will be discussed in detail later. Briefly, a frequence table is a systematized count of the individual letters which make up text passages in any language. For the present, let us simply consider three of the generalizations which follow from these frequency

tables for English. According to them, the single letter E, the pair of letters TH, and the group of letters THE are the most frequent. This does not mean that in every piece of text, no matter what length, E will be invariably the most frequent single letter, TH the most frequent pair of letters, or THE the most frequent group of three letters. But is in endeavoring to apply these generalized principles to the special conditions of the particular problem in hand, that the decipherer makes the assumptions upon which his work rests. If the special conditions of the problem approximate or conform closely to the generalized principles, the solution readily follows. But this is rarely the case, and he is forced to modify, not only his assumptions, but also his methods, and even to discard some of them. It is the facility and ease with which a decipherer is able to modify his methods and discard his assumptions, which differentiates the good decipherer from the poor one. *Deciphering is not a process for a "one-cylinder mind."*

Likewise the part played by imagination and intuition can hardly be overestimated. The knowledge of the circumstances surrounding the interception of a message, of the correspondents, etc., furnishes a wide field for the exercise of the intuitive powers; and a shrewd "guess" will often result in more progress than a whole day's painstaking labor. This faculty, so essential in deciphering, can be developed and trained. The exercise of the imaginative powers by attempting to assume whole words, given only two or three letters and their positions, will result in the stimulation of all the faculties concerned in the expression of ideas, will thus enlarge the decipherer's vocabulary, and otherwise arouse those qualities of mind which are peculiarly needed in cipher work.

Persistency is absolutely necessary for deciphering. Results are often secured only after seemingly endless experiment, and concentrated effort. It may be said that even after one has a thorough grasp of the underlying principles, patience and perseverance are the key-notes to success. *Yet, too long application soon results in mental exhaustion, and in such a condition little progress can be made. The decipherer will actually save time by ceasing from his labors and attacking the problem afresh later. A few minutes of work by a rested and clear mind is worth as many hours by a brain which is dull from fatigue.*

To summarize then, the qualities upon which success depends in deciphering are interrelated — reasoning from laws must be balanced with facility in modifying those laws; imagination must go hand in hand with discretion; and intuition can never wholly take the place of concentration and perseverance. *Finally, let it not be forgotten that many times the greatest ally the mind has is that indefinable, intangible something, which we would forever pursue if we could — luck.*

SOME SUGGESTIONS

Standardization of the details of operation in any work is essential if confusion and its consequent loss of time and labor are to be avoided. If a definite method of procedure is adopted and followed consistently, after a time it becomes a habit, and skill and accuracy in using it become second nature.

As a result of considerable experience, not only in the instruction of cipher operators, but also in the successful application of deciphering principles to unknown ciphers, the Department of Ciphers of Riverbank Laboratories has adopted a series of standard methods, close adherence to which, it is believed, will expedite the work materially.

1. PAPER

Do not crowd any work, but at the same time avoid wasting paper. Work sheets SHOULD NOT BE DESTROYED. They form a necessary part of the record pertaining to the solution of the problem. No work is too insignificant to discard, therefore it should be done well from the start. Cross-section paper, with squares $^1/_4$ inch in size, is indispensable.

2. PENCIL

A soft lead pencil should be used in order to permit of erasure. It will be found necessary to use the eraser quite as much as the pencil.

3. WRITING

The process of enciphering and deciphering is by no means a ONE-MAN-JOB. Handwriting will have to be read by others. It should be legible and clear. In ordinary writing, a doubtful letter is supplied, or an incorrect one is corrected, from the context; but in cipher writing a single error or questionable letter may throw the writer himself off the track, as well as those who may have to go over his work later. Script letters are rarely used in cipher work. All letters should be "printed"; that is, Roman capitals should be used exclusively.

The following forms of Roman capital letters, and Arabic numerals have been adopted as standard. In a very short time speed and nicety in their use may be achieved. Lower case, or small letters, should never be used in cipher work.

4. SLUGGING

This is the printer's term for the placing upon a piece of work a number which accompanies it until it is completely finished and disposed of in the files. Without it chaos inevitably results, as papers become disarranged, mixed, and lost very easily. Recovery of a lost paper, or the sorting out of mixed sheets is impossible unless a number is put in a conspicuous place upon each and every sheet. All problems, whether practice problems or real ciphers,

can and should bear their individual numbers. If every new sheet used on a particular problem is slugged before any other marks are made on it much trouble will be saved. The best place is the upper left-hand corner, using large size Arabic numerals of the style given in Section 3. Placing a heavy circle around it will help make it conspicuous.

5. ERRORS

Cipher messages pass through at least three different operations:

1. Encipherment
2. Transmission
3. Decipherment

In all of these operations the message passes through many hands; each operator concerned is liable to error; each error causes confusion. Due allowance should be made for errors in the work entered upon. An otherwise good assumption should never be rejected because in a single case an impossible combination results. Furthermore, time is wasted which is spent trying to correct an evident error which will in all probability straighten itself out later, when most of the message has been deciphered. All errors found in cipher text should be indicated in some manner. Thus:

XTVCB
THERE

A. Wrong letter.
If in a given alphabet cipher `V = R`, and the plain-text letter must be `E`, then write the correct letter, `E`, and underline it, or use a colored pencil.

12$\overline{33}$5 $\overline{5}\overline{2}$345
PNVID MOVCI
THEWR ITERS

B. Wrong alphabet.
If in a multiple alphabet problem "shifting" must be resorted to in order to produce the correct letters, indicate same by placing the numbers above the cipher letters showing which alphabet is necessary to produce the correct letter.

6. APPARATUS

The apparatus necessary for expeditious cipher work varies in amount. Such articles as typewriters, dictionaries, and maps are always indispensable. Rapidity in operations will be increased by devices which will eliminate as much hand work as possible. For this purpose wooden strips about 14 inches long, $\frac{1}{2}$ inch wide and $\frac{1}{4}$ inch thick, upon which paper may be mounted for the purpose of making sliding alphabets, will be found very useful. A rubber stamp containing the letters of the alphabet is also a convenience in the preparation of frequency tables, or, if the stamp is made with movable letters, straight or mixed alphabets may be made at will. A great amount of helpful apparatus is, of course desirable, the preparation of which is dependent only on the ingenuity and personal inclination of the operator.

7. COOPERATION

It will be found that a single operator working alone is able to accomplish very little. A group of two operators, working harmoniously as a unit, can accomplish more than four operators working singly. Different minds, centered on the same problem, will supplement and check each other; errors will be found quickly; interchange of ideas will bring results rapidly. In short, two minds, "with but a single thought," bring to bear upon a given subject

that concentration of effort and facility of treatment which is not possible for one mind alone.

8. WORD-EQUIVALENTS FOR LETTERS

When pronounced individually, the letters of the alphabet are so easily mistaken and confused, that in cipher work it is essential to use arbitrary words in "calling off" letters. The equivalents which have been adopted by the U.S. Army have been found to be very satisfactory and are given herewith:

A—Able	N—Nan
B—Boy	O—Opal
C—Cast	P—Pup
D—Dock	Q—Quack
E—Easy	R—Rush
F—Fox	S—Sail
G—George	T—Tare
H—Have	U—Unit
I—Item	V—Vice
J—Jig	W—Watch
K—King	X—X-ray
L—Love	Y—Yoke
M—Mike	Z—Zed

PRELIMINARY DEFINITIONS

Cryptology is that branch of knowledge which deals with the origin, development, and methods of all forms of secret communication.

Cryptography is that branch of cryptology which deals with the methods of secret writing.

A cipher, taken in a broad sense, is the name applied to any system of cryptography which involves the concealment (in a cryptographic sense) of the individual letters of a message.

The operation of thus concealing the letters of a message is called enciphering. The operation of translating or finding the secret meaning of such a message, whether done by means of the key or not, is called deciphering.

A code is the name applied to a specialized system of cryptography which involves the use of a book or a document, identical copies of which are in possession of the correspondents. Code books in general are of two kinds: (1) dictionaries, which consist merely of the most important words of a language arranged in alphabetical order, the words being accompanied by numbers usually in sequence; (2) repertoires, which consist not only of words, but also of phrases and sentences arranged in some arbitrary manner, and accompanied by arbitrary designations, either numbers, letters, or words. The latter type of code book is used at present much more frequently than the former.

The operations which apply to this system are called encoding and decoding.

When the code designations of the encoded words of a message are afterwards enciphered, the result is called enciphered code. For example: If the code word for the phrase "By order of the Commander-in-Chief" is `POBAL`, and if this code word is then enciphered on some system into the form `CITAX`, the latter word is then enciphered code.

OF THE HISTORY, USES, AND KINDS OF CIPHERS

Ciphers are as old as history — indeed history is full of instances of the conveyance of messages from one person to another by means of signs, symbols, gestures, and various contrivances. One of the stories related by a sixteenth century cryptographer[1] is of a cipher placed on the tomb of Semiramis, 1200 B.C. The cryptogram was deciphered some 700 years later —the decipherer's pains being rewarded with the salutation, "O, poor, miserable slave of deciphering that thou art; from this time on occupy thyself with more fruitful things than to spend time thus uselessly!"

The first military cipher device known to history was the Scytale, or round-ciphered staff, originated by the Lacedaemonians, and used extensively in Cicero's time. It has been asserted that Cicero himself wrote a treatise on ciphers, but no trace of this is found to exist. Cicero's servant, Tyro, is known to have recorded a number of ciphers which he asserted were used by his master. The generals of ancient times had endless methods of transferring information, such as shaving the head of a slave and writing thereon, then holding the slave until the hair grew, whereupon the messenger departed, to be shaved again when he had reached his destination, for the message to be read. Writing upon the back of the slave with a fluid, such as the juice of certain fruits, which became visible upon application of certain salts, was likewise a common practice. Thus the modern and highly-specialized invisible inks arose from the ancient use of fruit juices for the same purpose.

In the same way the modern straight alphabet ciphers can be traced directly to their forerunner, the cipher used by Julius Caesar: the use of B for A, C for B, D for C, and so forth. Other devices used in past centuries were the famous string cipher, the use of torches, musical notes, and many others too numerous to mention.

By the time printing had been put into use, ciphers had attracted so great a number of devotees, that throughout the sixteenth and seventeenth centuries there was an almost constant stream of books issued dealing with the various branches of cryptology — all under different and very impressive names, such as Steganology, Steganography, Polygraphy, Cryptomenytices, Scotography, and Synthemology or Semaeology. All of the works are interesting and curious, some of them contain valuable information. The first man to write of ciphers, and who is sometimes called "the father of ciphers," was Trithemius, abbot of Spanheim and Wuerzburg, whose book "Chronologica Mystica," a work of great magnitude, was published in 1516. All copies of this were later burned, because of the accusation that the book dealt with witchcraft. The manuscript remained in the monastery, however, and translations and reprints were made from this later. Gabriel de Collanges (Paris, 1561) and Gustavus Selenus (1624) were two writers who drew their material chiefly from Trithemius. Other well known writers on this subject in the sixteenth and seventeenth centuries, were John Baptist Porta (1561), Vigenère (1587), Bishop John Wilkins (1640), Falconer (1685) and innumerable others, all of more or less importance. In fact, in the latter part of the sixteenth century it was considered a necessary part of a man's education to become versed in ciphers.[2]

Since that time ciphers have increased in value and importance, scope and complexity. To those old writers of cipher, whose naiveté is so great a source of interest and even amusement to us today, the modern cipher which often uses scores of complex alphabets

[1] Blaise de Vigenère, in *Traicté des Chiffres*, Paris, 1587

[2] For a complete bibliography of works on cipher see Part II of Riverbank Publication No. 18, "Synoptic Tables for the Analysis of Ciphers." (In press.)

in the same message would seem as much like witchcraft as their simpler systems seemed to the people before them. Yet the complex systems of today are but a development of the older, simpler methods. Indeed, it may be said that almost every system of cipher known today can be traced to its forerunner of three centuries or longer ago.

At the present time ciphers and codes are used in almost every form of correspondence, both private and governmental. Commercial codes are as common as business itself. Newspaper correspondence is at times done in cipher. Criminals write and speak in cipher and code. Authorities have never been able to break up the "underground" means of communication in prisons by which "breaks" have been planned, and the "latest gossip" spread, without a spoken word.

Governmental ciphers may be spoken of as including diplomatic and military ciphers. Diplomatic ciphers are in use mostly by a few of the smaller nations. Although usually of good construction, on account of the carelessness of clerks whose almost total ignorance of ciphers in general makes consequent errors in judgement, these ciphers are often unsafe. To quote Bacon: "But in regards to the rawness and unskilfulness of the hands through which they pass, the greatest matters are many times carried in the weakest ciphers." The same is still true today.

Most of the large governments use enciphered code for diplomatic and naval communication, but inasmuch as it is the generally agreed upon assumption on the part of diplomatic and military officers that a new code book or a new cipher system is in possession of the enemy or of foreign governments at the moment of, or very soon after its inception, enciphered code becomes cipher only, so far as the decipherer is concerned.

The importance and value of military ciphers cannot be overestimated. Interception of such messages is no longer dependent upon the capture of messengers only. The use of radio, telegraph, buzzer, telephone, semaphore, heliograph, and klaxon systems of communication in the field all offer much greater opportunities for the interception of messages. All large governments must have a corps of decipherers to handle intercepted messages.

THE REQUIREMENTS OF A MILITARY CIPHER FOR FIELD USE

The requirements of a military cipher for field use have been laid down by Kerckhoffs,[1] but they are only such as a knowledge of deciphering would give.

1. *The system should be materially, if not mathematically, indecipherable*. Edgar Allan Poe has said: "Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve." This may or may not be true, but it is certainly true that no one has yet invented a mathematically indecipherable system which is practical. Hence, for our purposes we may consider no system in use today as indecipherable. The most that can be expected of a cipher adapted to field use is that it shall offer to the interceptor sufficient obstacles in the way of decipherment to enable the orders or directions contained therein to be executed. The highest degree of perfection as regards this requirement would be a cipher system, the details of the operation and the alphabets of which would be known to the enemy, but without the key a single message or even a series of messages would be absolutely indecipherable to the enemy for all time. Of course it is impossible to attain such a degree of perfection; so that we must modify this requirement by assuming the enemy in possession of everything pertaining to the cipher system, including the alphabets, but that a single message or even a series of messages should resist his efforts towards solution for a sufficient length of time to enable the orders or directions contained therein to be executed.

2. *It should cause no inconvenience if the apparatus and methods fall into the hands of the enemy*. A perfect cipher system would be one which would require nothing but pencil and paper. Apparatus is always subject to capture or derangement. Many cipher machines have been devised. But machines operate upon mechanical principles; it must be assumed, therefore, that if the enemy obtains possession of one of the machines he can find out the details of its operation. Furthermore, a seemingly complicated machine cipher may often be solved by the use of sliding strips of paper, even without a knowledge of the alphabets employed. But since it must be assumed that the enemy is in possession of the machine or the alphabets, since the systems employing machines possess no advantages, so far as secrecy is concerned, over systems not requiring them, and since they entail serious disadvantages, the use of machines is rather infrequent. The statement that many cipher machines have been invented, but very few are in use, quite covers this phase. Their only real advantage is that they usually are made in connection with a typewriter keyboard, so that speed in enciphering and deciphering is possible.

3. *The key should be such that it could be communicated and remembered without the necessity of written notes and should be changeable at the will of the correspondents*. These two requirements are of considerable importance. The capture of men with keys upon their persons, or the capture of positions housing the communication quarters is dangerous. Frequent change of key is about the most important safeguard to any field system; hence this should be made easy.

4. *The system should be applicable to telegraphic correspondence*. This is obvious today, where nearly all communication takes the form of Morse signals.

5. *The apparatus should be easily carried and a single person should be able to operate it*. This is certainly a requisite in the case of a field cipher.

6. *Finally, in view of the circumstances under which it must be used, the system*

---

[1] Kerckhoffs, A. *La Cryptographie Militaire*, Paris, 1883. Quoted by Hitt, *Manual for the solution of Military Ciphers*, 1916.

should be an easy one to operate, demanding neither mental strain nor knowledge of a long series of rules. This requirement is of the utmost importance. "It should be so simple that the thickest 'leftenant' in the army can use it," a British officer has said. The more simple, the less chance of errors in enciphering and deciphering.

Hitt says: "A brief consideration of these six conditions must lead to the conclusion that there is no perfect military cipher." Some of these requirements must be sacrificed in order to meet the most important ones.

In connection with the innumerable attemps on the part of the average person to devise new ciphers, it might be said, "There is nothing new under the sun." The information concerning ciphers that is possessed by the average layman is so meager that it has led an eminent cryptographer to say that a school boy might unknowingly invent a cipher which would resist the efforts of an expert for months, whereas only the actual solution of a cipher devised by a most capable business or professional man would convince the inventor that the claims of indecipherability for his system were unfounded. Edgar Allan Poe's experience in this country is of interest in this connection. (See Poe's Works, Vol. II, p. 490–505.)

Since we are dealing now with military ciphers only, we come at this point to the *kinds* of ciphers.

Ciphers in general may be divided into two great classes: (1) SUBSTITUTION and (2) TRANSPOSITION.

(1) Any message in which one or more letters, numerals, signs, or combinations of these three have been substituted in accordance with a definite system, usually some "key," for the original letters of the plain-text, constitutes a substitution cipher.

(2) Any message, the letters, words, or sentences of the original text of which have been rearranged according to some definite system, constitutes a transposition cipher.

In addition to these two main classes there is the Playfair cipher, which is a variety of substitution cipher, to be discussed later, and the combination of substitution and transposition ciphers, in which the original text is transformed first into a substitution cipher, after which the latter is transformed into a transposition cipher, or vice versa.

After the student has secured a thorough grasp upon the principles underlying the solution of the simpler varieties of substitution ciphers and has thus come to an understanding of the mechanics of a written language, he will be in a better position to comprehend the principles upon which the solution of transposition ciphers are based. We will therefore proceed at once to the methods of solving substitution ciphers.

OF THE FREQUENCY OF LETTERS AND ITS BEARING ON SUBSTITUTION CIPHERS

The following message is an ordinary passage of English text such as may be found in any periodical, newspaper, or book:

MESSAGE

"Men would be unlikely to render themselves liable to the penalties of the law if they knew that wherever they might flee their identity could not fail to be discovered. A sure means of identification would not only have the effect of deterring from crime in general but would evidently nullify all attempts of whatever kind at a substitution of persons. No impersonations of a pensioner, or a missing heir, or a business man could ever hope to be successful."

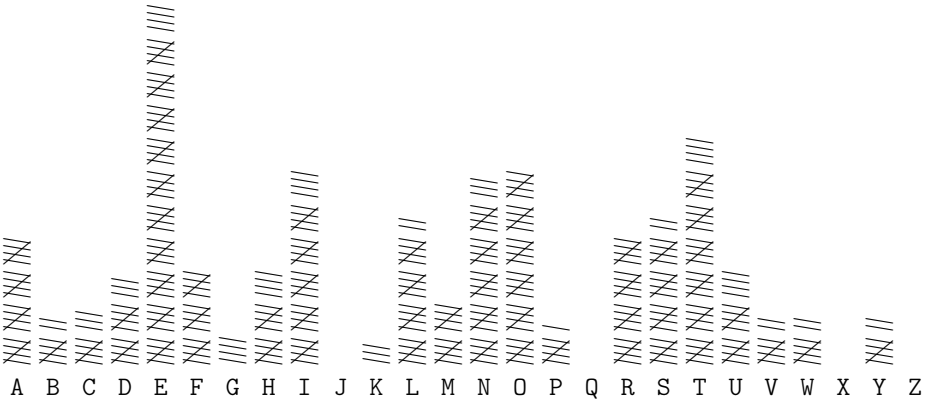


Fig. 1.

If the letters composing the words of this message (or of any message of similar nature and length) are distributed into what is known as a GRAPHIC FREQUENCY TABLE, shown in Fig. 1, which is nothing else than a short and systematic way of making a count of all the different letters in this message, it will be found that:

(1) The letters all vary greatly in the frequency of their use, some being used many more times than others. This results in the production of a series of "crests and troughs," the spatial relations and linear dimensions (frequencies) of which are definitely fixed. By their spatial relations is meant their positions with reference to each other only, i.e., the number of intervals separating any one crest or trough from another.

(2) Opposite the letter A, there is a crest, or a point of high frequency.

(3) Passing over three intervals after A, there is another crest, representing the letter E, which is the point of highest frequency and determines the biggest crest in the table.

(4) Passing over two intervals after E, there are two smaller crests, adjacent to each other, representing the letters H and I.

(5) Passing over four intervals after I, there are two more crests, adjacent to each other, representing N and O.

(6) Passing over two intervals after O, there is a sequence of three crests, representing R, S, and T.

(7) The order of frequency of the letters composing this piece of text is as follows: E, T, O, I, N, (S, L), (A, R), F, (H, U), D, M, C, (B, V, W, Y), P, G, K.

Fig. 2.

Now these characteristics approximate to a fair degree the characteristic or cardinal features of a normal frequency table[1] made from a total of 25,000 letters, which is shown in Fig. 2. The order of frequency of the letters composing this table is as follows: E, T, A, O, N, I, S, H, R, D, L, C, U, F, M, P, W, G, Y, B, V, K, X, Q, J, Z. The greater the number of letters in any particular portion of text, the more closely will the frequency table applying to it approximate the normal.

Now the relative positions and the frequency of the crests and troughs of the table shown in Fig. 2 would have been absolutely unchanged had the tabulation begun with, say R, instead of A, as the chart in Fig. 3 shows. Compare this chart with that in Fig. 2, noting the relative positions and length of the lines.

No matter with which letter of the alphabet the tabulation had been begun, these lines would have maintained their relative positions with respect to each other and the length of each line would have remained unchanged. In other words, the spatial arrangements and the relative frequencies of the crests and troughs are the results of certain *internal relations in the English alphabet*, as will be pointed out later. It should be clear, therefore, that the sequence of letters in the ordinary alphabet may be regarded as a continuous, cyclic arrangement of letters, and that no matter where the tabulation begins,

[1] See page **??**

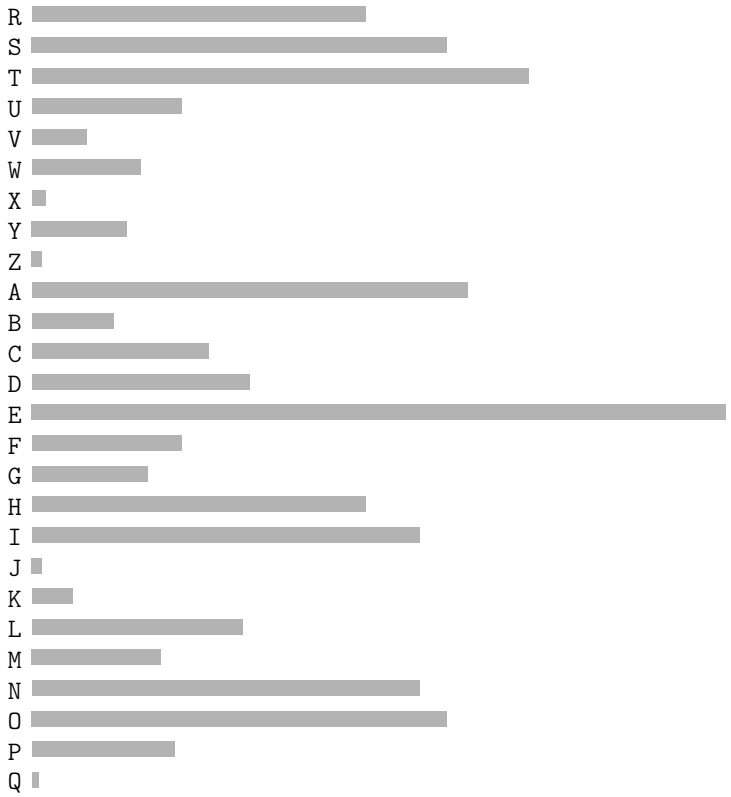


Fig. 3.

the spatial and frequency relations of the crests and troughs remain unchanged. Fig. 4 gives a clear idea of what is meant.

Now suppose the message given on page **??** is written by means of an alphabet which has been shifted, say nine spaces forward; that is, for the letter A, the letter J, which is the ninth from A, is written; instead of B, the letter K, which is the ninth letter from B, is written, etc., in accordance with the diagram of alphabets shown below:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
          ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Here is the message in a form which now constitutes a substitution cipher of the simplest kind:

MESSAGE[2]

```
VNWFX DUMKN DWURT NUHCX ANWMN ACQNV BNUEN BURJK
UNCXC QNYNW JUCRN BXOCQ NUJFR OCQNH TWNFC QJCFQ
NANEN ACQNH VRPQC OUNNC QNRAR MNWCR CHLXD UMWXC
OJRUC XKNMR BLXEN ANMJB DANVN JWBXO RMNWC RORLJ
CRXWF XDUMW XCXWU HQJEN CQNNO ONLCX OMNCN AARWP
OAXVL ARVNR WPNWN AJUKD CFXDU MNERM NWCUH WDUUR
```

[2] Cipher messages are usually sent in groups containing a definite number of letters or figures (usually five or ten) to each group, in order to prevent the would-be decipherer from securing clues from the indications of word lengths, which would be furnished . . .

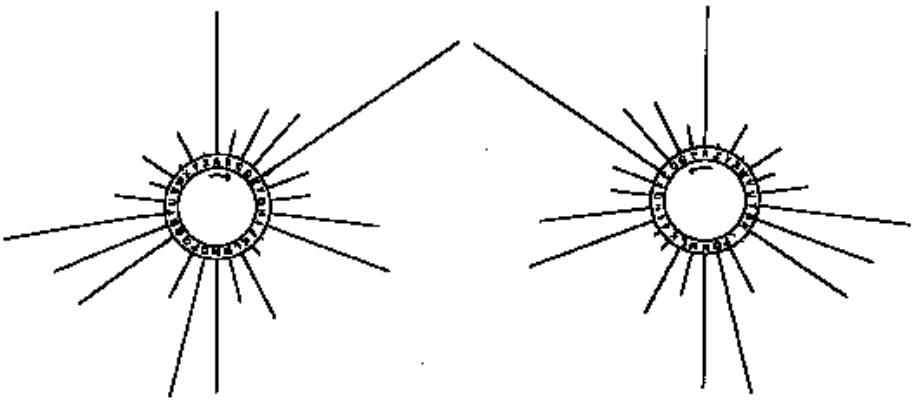


Fig. 4.

```
OHJUU JCCNV YCBXO FQJCN ENATR WMJCJ BDKBC RCDCR
XWXOY NABXW BWXRV YNABX WJCRX WBXOJ YNWBR XWNAX
AJVRB BRWPQ NRAXA JKDBR WNBBV JWLXD UMNEN AQXYN
CXKNB DLLNB BODU
```

If a graphic frequency table of this cipher message is now made, it will be found that crests and troughs are still present, and moreover, that their relative positions and frequencies have not been changed in the slightest particular, as comparison with Fig. 1 shows.

For example, the frequency of E in Fig. 1 was 54; at an interval of three spaces before E there is another crest representing A, the frequency of which is 20; on the other side of E, after an interval of two spaces, comes a sequence of two crests, H and I, with frequencies of 14 and 29 respectively. Compare these with their homologous crests and troughs in Fig. 5. The letter N marks the highest crest in the table. Its frequency is 54. Skipping four spaces before N there is another crest, with a frequency of 20; on the other side of N, skipping two intervals comes a sequence of two crests with frequencies of 14 and 29 respectively. In short, the spatial relations of the crests and the troughs in Fig. 5 seem to be exactly the same as those of the frequency table in Fig. 1 which applied to ordinary plain text. This would indicate, without a knowledge of how the enciphering was done, that cipher letter J represents plain-text letter A, K represents B, etc.; in other words, the cipher alphabet begins with J as A, and all the remaining letters follow as in the ordinary alphabet. If, therefore, opposite cipher letter J, the assumed plain-text equivalent A is written, followed by the remaining letters of the alphabet, not only does the whole sequence of assumed plain-text equivalents fit the requirements of the graphic table as regards frequency and spatial relations as found in a normal frequency table for English, but what is more important, if these values are substituted in the cipher text, the words of the plain text immediately appear. Thus:

```
VNWFX DUMKN DWURT NUHCX ANWMN A
MENWO ULDBE UNLIK ELYTO RENDE R
```

It becomes clear, therefore, that the fact that in this example, the cipher letter N represented plain-text letter E, cipher letter J represented plain-text letter A, etc., had absolutely no effect upon the spatial and frequency relations of the crests and troughs in

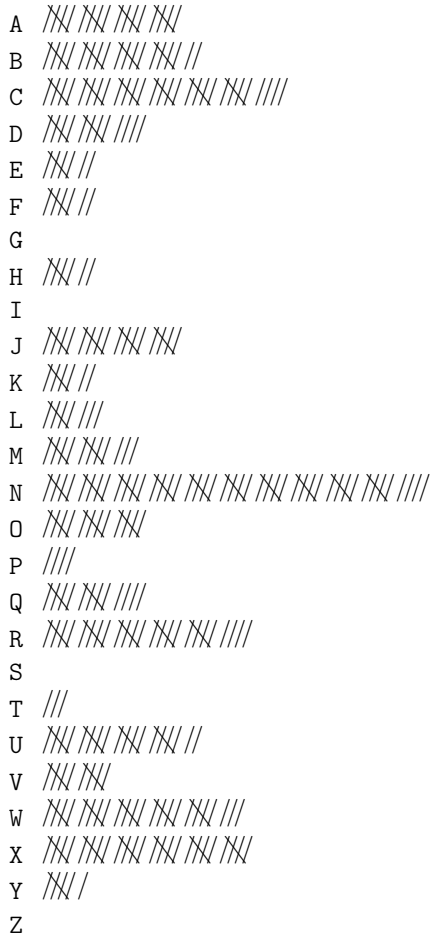


Fig. 5.

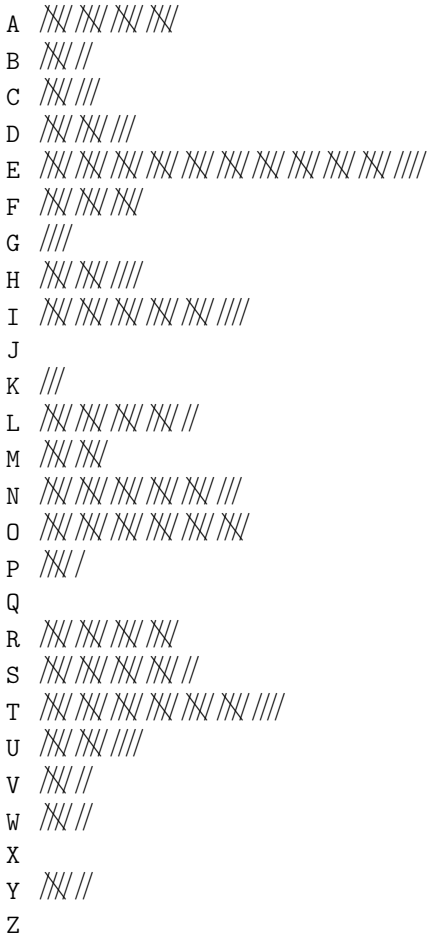


Fig. 1.

the graphic table. If A had been represented, for example, by R, B by S, C by T, D by U and E by V, etc., the spatial and frequency relations of the crests and troughs would have been exactly the same. The letter V in this case would have marked the highest crest in the table because it would have represented the plain-text letter E. This leads to the conclusion that the characteristic of being the most frequently used letter in the English language belongs to the letter E, not because of any special quality or peculiarity inherent in the letter E itself, but because *it is the symbol which has been adopted by convention to represent the most frequently used sound in the English language*; any other symbol which will convey the same idea, namely sound "ee," will serve just as well. This applies not only to the letter E but also to all the other letters in the language.

To explain: If we had been taught that the sounds represented by the symbols E, I and P were, instead, represented by the symbols $+, *$ and 8, respectively, the word PIE would be written $8*+$ and the latter would be perfectly intelligible to us. Or, if the sounds represented by our letters A, B, C, D, etc., were taught to us to be represented instead by the symbols V, K, L, X, etc., we would still read the latter as "ay," "bee," "cee," "dee," etc., and the combination LVK would be pronounced "CAB" and would convey the same idea

to us as the latter combination does now; for the combination of sounds indicated by CAB has been established by convention to represent a certain definite object, viz., a vehicle, or a means of transportation. The *spoken* words of a language, therefore, may be regarded as combinations resulting from the juxtaposition of definite sounds, which combinations ages of usage have fixed as the representatives of certain objects or ideas; and the *written* words of a language, therefore, may be regarded as combinations resulting from the juxtaposition of definite symbols, which ages of usage have fixed as the representatives of these definite sounds. For example, the juxtaposition of the symbols PIE "spells" to us — that is, calls to our minds — the sounds "pee," "i" and "ee." This combination of sounds, as the result of our previous experience, conveys to our minds, with various resultant sensations, a very definite object. Now if we should use the symbols immediately following these in the regular sequence of symbols in our alphabet, viz., QJF, the combination of sounds called for is perhaps not as easily pronounced but looks altogether strange, because, as we ordinarily say, there is no such word in the language — meaning that usage has not established that sequence of sounds as representing a thing or an idea in English. The necessity for the alphabet now becomes clear; for it becomes essential to fix definitely the sequence of symbols and the sequence of sounds so that when two individuals desire to communicate, that is, to convey to each other the combinations of sounds necessary for the production of intelligible words, they should understand what sounds are called for by the symbols indicated. It should be clear now why written language is absolutely dependent upon this basic principle — the alphabet — which is seen to be really double in nature, involving two separate but coinciding sequences, one of sounds and the other of symbols.

It would not be difficult to explain why the sequence of sounds in the English alphabet, for example, is as we have it today; why, in other words, sound "ay" is followed by sound "bee," etc. This sequence can be traced back through the various languages from which the English language is derived. But it would be difficult indeed to explain how or why the first real alphabet known, that is, one on a purely phonetic basis, came into existence. It is supposed to be a product of the Semitic race and of the Phoenicians. Its history is perhaps as old as language itself. It is also not difficult to explain why the symbol A is now used to represent the sound "ay" in English, because the evolution of the symbols can be traced back to the hieroglyphics of the Egyptians[3].

[3] "The letters in the English alphabet are derived from the corresponding forms in the Latin alphabet, the early forms of which in turn came from the Western Greek alphabet, and the Greek letters from the Phoenician. The origin of the Phoenician letters is not certainly known, though it is not improbable that they were suggested by signs used in Egypt. Although some of the Egyptian hieroglyphics had come to be used as letters, yet Egyptian writing was not strictly alphabetic. The use of an alphabet on a strictly phonetic basis is due to the Semitic race, and probably to the Phoenicians." — Webster's New International Dictionary.

THE KINDS OF ALPHABETS

The student is prepared now to understand the exact meaning of the definitions which follow:

1. An alphabet may be defined as a definitely fixed sequence of symbols representing a definitely fixed sequence of sounds.

2. The normal alphabet for any language is the ordinary alphabet in which the conventional sequence of the sounds used in the language is represented by the conventional sequence of the symbols used in that language; i.e., the two sequences which have been established after generations of use as normal or conventional, coincide. For example, in English the sounds "ay," "bee," "cee," "dee," etc., are represented by the symbols A, B, C, D, etc. To show that these sequences are conventional and arbitrary, it is only necessary to point out that languages vary as regards the order of the alphabet. For example, the Arabic alphabet proceeds thus: ا alif, ب ba, ت ta, ث tha, ج jim, or a, b, t, th, j, etc. Any sequence of letters which is written by means of a normal alphabet, and which results in the formation of a word or a series of words in that language constitutes what is known as plain-text.

The meaning of the expression use on page **??** in connection with the cardinal features of a frequency table of English normal or plain text, "internal relations in the English alphabet," should now be clear. The reasons why crests and troughs appear at all in the frequency tables are two: (1) certain sounds are used much more frequently than other sounds, and (2) each sound is always represented by one and only one symbol. The reason why the crests and troughs have definite spatial relations is that the intervals separating the component parts of an alphabet are definitely fixed; i.e., A comes first, E comes fifth, H comes eighth, etc.

3. A cipher alphabet is one in which either the sequence of sounds or the sequence of symbols or both sequences have been altered from the normal, or in which the normal coincidence of the sequences has been altered. Any sequence of letters which has been written by means of a cipher alphabet, and which represents a word or a series of words, constitutes what is known as cipher text.

4. A straight alphabet is one in which neither the normal sequence of symbols nor the normal sequence of sounds is altered, but in which only the normal coincidence of these two sequences is changed. The cipher message on page **??** is an example. Straight alphabets may be of two kinds, direct or reversed:

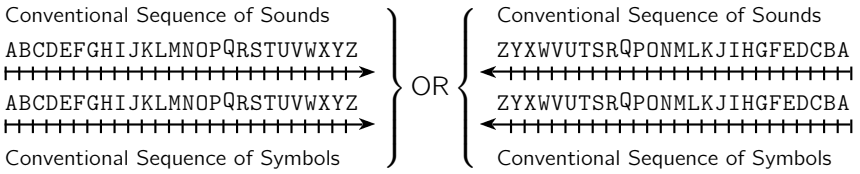
(a) In a direct alphabet the entire normal sequence of symbols, proceeding say from left to right may be shifted one, two, three . . . to twenty-five spaces to the right of the normal starting point of the entire normal sequence of sounds, proceeding likewise from left to right. In other words, when both sequences are normal and only the normal equivalence of the sequence is changed, a direct alphabet results. The cipher message on page **??** is an example of a direct alphabet cipher.

(b) In a reversed alphabet the entire normal sequence of symbols proceeding say from left to right is applied to the normal sequence of sounds proceeding from right to left; in other words, the normal sequence of symbols is applied to the reversed sequence of sounds, or vice versa, the reversed sequence of symbols is applied to the normal sequence of sounds. In both cases the results are the same.

The meaning of these definitions may be clearly illustrated in the accompanying Fig. 6. In each case the sequences are shown as going in two directions because it is immaterial whether the alphabet is written from left to right or vice versa. Some languages

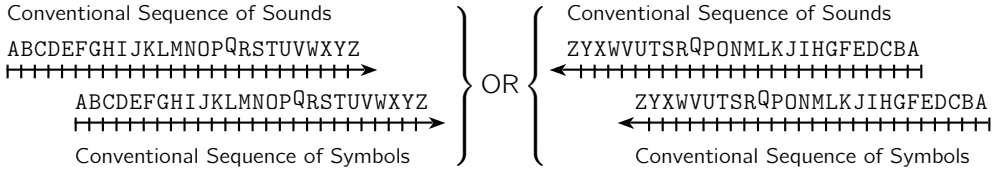
are written from right to left, as for example, Persian.

1 — Normal Alphabet



2 — Straight Alphabets

A — Direct



B — Reversed

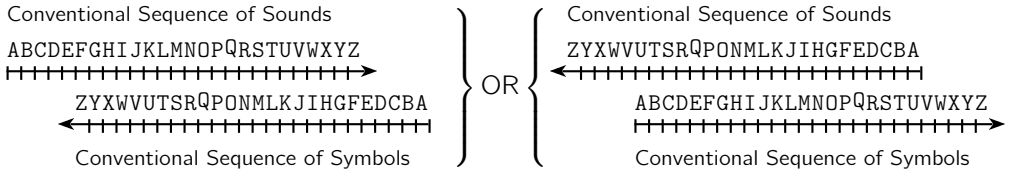


Fig. 6.

5. As regards the manner in which alphabets are mixed, they may be of three kinds:

(a) Key-word mixed alphabets, in which the sequence of letters is commenced by a key-word which is followed by the rest of the unused letters of the alphabet. Such a key-word should be long, and should break up the normal sequence as much as possible. Example: key-word Washington;

Plain-text — ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher — WASHINGTOBCDEFJKLMPQRUVXYZ

(b) Arbitrarily mixed alphabets, in which the sequence of letters is mixed according to some system previously agreed upon by the correspondents. Such a system, for example, may consist in the writing of the letters of a key-word mixed alphabet in a rectangle, the number of columns of which is determined by the number of different letters in the key-word, numbering the columns in accordance with the numerical sequence determined by that key-word and then writing out the alphabet by taking the columns in their numerical order. Thus:

Key-word — WASHINGTON

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

Plain-text — ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher — ACQGKYHEUIFVNJXOMSDRTLZWBP

(c) Random mixed alphabets, in which the sequence of symbols is determined by absolutely random assignments or by drawing out of a hat.

The chief advantage of the first two types of alphabets over the third type is that the former two may be communicated without the necessity of writing out the entire sequence, and can be reproduced from memory, whereas the latter one must be communicated by written notes and thus is dangerous. The chief disadvantage of the first two types is that given a few values, the entire alphabet may be reconstructed because of the clues furnished by the sequences which are usually unbroken, such as BCD, FGH, JKL, XYZ. In the case of the random mixed alphabet, the determination of a few letters gives no clue to the other because the sequence is absolutely hap-hazard and based upon no system whatever.

However, since the number of ways in which an arbitrarily mixed alphabet may be produced from a key-word are legion, as far as safety is concerned, one produced in this way is probably second in safety as compared with one produced by absolutely random assignments, or by drawing out of a hat.

6. As regards the internal nature of mixed alphabets, they may be of two kinds:

(a) Reciprocal alphabets, wherein if , for example, cipher letter X represents plain-text letter A, then cipher letter A represents plain-text letter X. Such an alphabet may be produced arbitrarily by random reciprocal assignments, or by sliding any alphabet against its reverse, in which case a series of twenty-six reciprocal alphabets is produced.

(b) Non-reciprocal alphabets, wherein the reciprocal relation does not hold true except as a matter of chance.

7. As regards their use, alphabets may be of two kinds:

(a) When a cipher alphabet is arranged for the sending of a message, it is called an enciphering alphabet. Example:

Plain text — ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher text — PKTXACNOVZBDEGHFIJLQMSUWRY

(b) When such an alphabet is arranged for the receiving or translating of a cipher message, it is called a deciphering alphabet. For the example given above the deciphering alphabet would be thus:

Plain text — ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher text — EKFLMPNOQRBSUGHATYVCWIXDZJ

SOLUTION OF STRAIGHT ALPHABET CIPHERS

Straight alphabet ciphers, it has been said, are of two kinds: direct and reversed. We shall first treat of direct alphabets.

(a) Single alphabet. Since there has been no change in either the sequence of symbols or the sequence of sounds in the cipher alphabet, the correct determination of the value of a single cipher letter in a message enciphered by means of a straight alphabet, whether direct or reversed, will result in the determination of the whole alphabet at once. Consequently, if a graphic frequency table of a straight alphabet substitution cipher is made, the spatial and frequency relations of the crests and troughs should at once disclose what letter represents E. Proceeding from this point, the values of the remaining cipher letters are assigned on the basis of a direct or a reversed alphabet, and if the spatial and frequency relations of the values thus found agree with the requirements of the normal graphic frequency table, the solution of the message is at hand. This process of applying the principles concerning the spatial and frequency relations of a normal graphic frequency table to a graphic frequency table of a cipher message, in order to arrive at the solution of the cipher, is spoken of as "fitting the graphic table to the normal."

MESSAGE

FXGPH NEWUX NGEBD XERMH KXGWX KMAXF LXEOX
LEBTU EXMHM AXIXG TEMBX LHYMA XETPB YMAXR
DGXPM ATMPA XKXOX KMAXR FBZAM YEXXM AXBKB
WXGMB MRVHN EWGHM YTBEM HUXWB LVHOX KXWTL
NKXFX TGLHY BWXGM BYBVT MBHGP HNEWG HMHGE
RATOX MAXXY YXVMH YWXMX KKBGZ YKHFV KBFXB
GZXGX KTEUN MPHNE WXOBW XGMER GNEEB YRTEE
TMMXF IMLHY PATMX OXKDB GWTMT LNULM BMNMB
HGHYI XKLHG LGHBF IXKLH GTMBH GLHYT IXGLB
HGXKH KTFBL LBGZA XBKHK TUNLB GXLLF TGVHN
EWXOX KAHIX MHUXL NVVXL LYNE

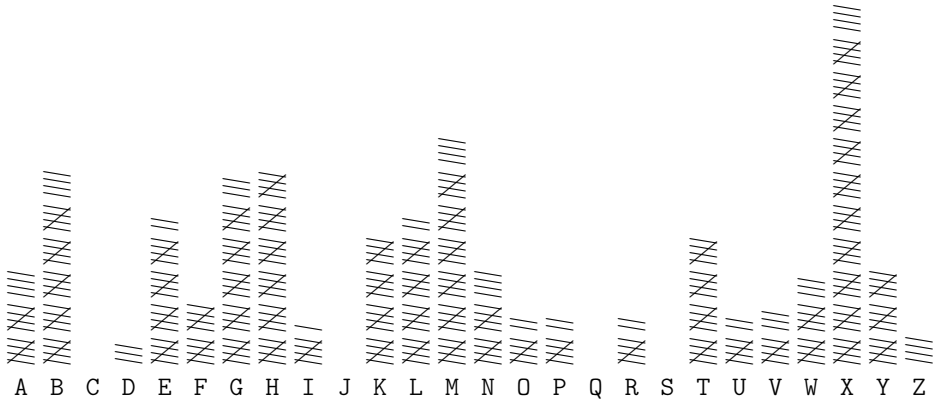


Fig. 7.

In the accompanying frequency table (Fig. 7) the letter X, which marks the highest crest in the table, is selected as the equivalent of plain-text letter E; wherefore, on the assumption of a direct alphabet sequence, cipher letter T equals A, cipher letter U equals

B, cipher letter V equals C, etc. The "fit" is excellent, the correct plain-text values are immediately assigned and substitution results in the solution of the message. The first two lines are as follows:

```
FXGPH NEWUX NGEBD XERMH KXGWX KMAXF LXEOX
MENWO ULDBE UNLIK ELYTO RENDE RTHEM SELVE

LEBTU EXMHM AXIXG TEMBX LHYMA XETPB YMAXR
SLIAB LETOT HEPEN ALTIE SOFTH ELAWI FTHEY
```

This method of deciphering is called "Solution by Frequency Table." There is, however, another method of deciphering such a message which does not necessitate the compilation of a frequency table.

After all, a straight alphabet cipher is only the result of shifting the sequence of symbols a certain number of spaces away from its normal coincidence with the sequence of sounds. If we could find, by means of two direct sequences, one representing symbols, the other sounds, the relative positions these two sequences were in, when the enciphering was being done, the solution of the cipher would be at hand immediately. The question then resolves itself into a search for these positions. We may therefore experiment with two direct sequences, starting with the setting of A on the sequence of symbols to equal B, on the sequence of sounds. We then apply the entire sequence of equivalents thus secured to the first two groups of our message. Thus:

```
Sequence of Sounds (= Plain text) — ABCDEFGHIJKLMNOPQRSTUVWXYZA
Sequence of Symbols (= Cipher text) —  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher letters — FXGPH NEWUX
Sounds indicated — GYHQI OFXVY
```

This series of letters does not "spell" any plain text, so that evidently the two sequences were not in the position indicated. We therefore move the sequence of symbols one more space to the right, and try again. Thus:

```
Sequence of Sounds (= Plain text) — ABCDEFGHIJKLMNOPQRSTUVWXYZAB
Sequence of Symbols (= Cipher text) —   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher letters — FXGPH NEWUX
Sounds indicated — HZIRJ PGYWZ
```

This series of letters also does not "spell" any plain text, so we therefore move the sequence of symbols one, then two, then three, four, five, six, seven spaces to the right until the series of sounds indicated spells out plain-text words. Thus:

```
Sequence of Sounds (= Plain text) — ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFG
Sequence of Symbols (= Cipher text) —         ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher letters — FXGPH NEWUX
Sounds indicated — MENWO ULDBE
```

We have thus discovered by successive experiments the positions of the two sequences in encipherment. Now let us analyze these experiments to see if a definite procedure would shorten the labor.

Cipher letters — FXGPH NEWUX
A = B — Results of 1st experiment — GYHQI OFXVY
A = C — Results of 2nd experiment — HZIRJ PGYWZ
A = D — Results of 3rd experiment — IAJSK QHZXA
A = E — Results of 4th experiment — JBKTL RIAYB
A = F — Results of 5th experiment — KCLUM SJBZC
A = G — Results of 6th experiment — LDMVN TKCAD
A = H — Results of 7th experiment — MENWO ULDBE

Note now that the net result of these seven separate experiments was simply the continuance of the direct alphabet begun by each cipher letter until the juxtaposition of a certain definite series of letters resulted in the spelling out of plain-text words. This certain series of letters was definite because the number of experiments coincided with the number of spaces the sequence of symbols had been shifted from the normal. If we take merely the two groups of cipher letters and continue beneath each letter the direct alphabet started by each letter, all the plain-text equivalents would appear on one horizontal line, which could then easily be selected from all the other horizontal lines because it is the only one which results in the formation of intelligible words. This process of continuing the direct alphabet sequence beneath a group of cipher letters is called "running down." Since each column considered separately consists of only the direct alphabet, it is clear that this "running down" process might be accomplished automatically by the use of the devices shown in Plate 1.[1] The Sliding Poly-Alphabet, A, consists of a series of twenty-six direct

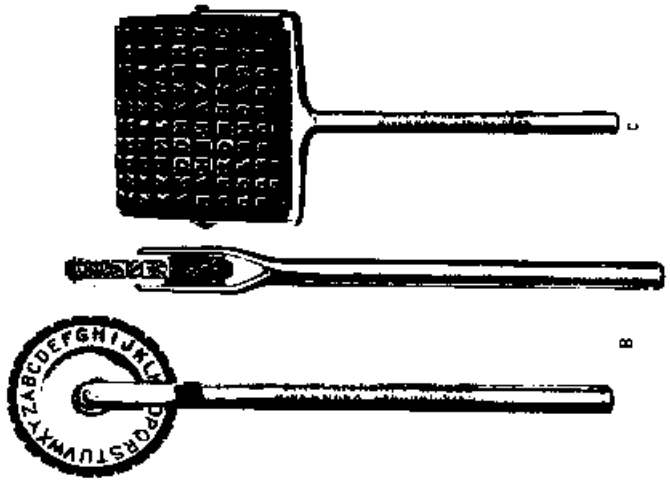


Plate 1

alphabets printed upon cardboard strips which are mounted upon celluloid; the strips are all movable, running either in grooves or on tracks, the two pieces of plate glass provided with set-screws at the corners holding the strips firmly, yet loosely enough so that they easily slide up and down. There is in addition a direct alphabet at the extreme left, and a reversed at the extreme right. The sliding strips bear upon their reverse sides other

[1] De kwaliteit van Plate 1 in de copie waarvan deze heruitgave is gemaakt, is onvoldoende voor een zinvolle reproductie van het "Sliding Alphabet", item A. De twee onderste figuren behoren bij alfabetroller B, de bovenste bij roller C.

alphabets, i.e., reversed, French or Spanish, etc. Now when a line of cipher is "set" at the top, that is, when the sliding strips are moved so that a given number (up to twenty-six) of cipher-text letters are brought into one horizontal line, the successive horizontal lines of equivalents, called *generatrices*, are indicated automatically, and thus a vast amount of writing is eliminated. In an alphabet containing twenty-six letters, there are twenty-five generatrices, the twenty-sixth generatrix becoming identical with the letters at the starting point. The second device, the Poly-Alphabet Wheel, B, the idea for which the Riverbank Laboratories is indebted to Lieutenant P.H. Burdick, produces the same results. It makes use of a revolving rubber stamp containing the letters of the direct alphabet equally spaced on the perimeter of the wheel. In order to "run down" a series of cipher letters it is only necessary to start each column with the cipher letter which is to be "run down." The letters all being equidistant from each other, the successive letters all appear upon horizontal lines, or in other words, the successive generatrices are printed. This method possesses some advantageous features which the other does not, the most important being, first, that the apparatus is much smaller and can be carried about easily; secondly, that once a group of cipher letters is "run down," the results are permanently indicated and may be referred to or re-examined at any future time; and thirdly, since the letters are all movable, they may be arranged in accordance with any mixed alphabet sequence.

The third device, the Poly-Alphabet Roller, C, makes use of a series of ten endless rubber belts containing the letters of the direct alphabet equally spaced. These belts fit snugly upon the drum, but may be moved with reference to each other so as to contain ten cipher letters in one line. The device is then inked and rolled upon a sheet of paper.

The various generatrices produced by any of these Poly-Alphabet devices are examined to see whether the letters of one such generatrix spell out any plain-text. If a sequence of plain-text words is found, then the solution of the cipher is attained. The key-letter is sought, that is, the cipher-equivalent or value of plain-text letter A is sought, and this determines the entire cipher alphabet, in a single direct alphabet substitution cipher. The key-letter may be found either by the use of two sliding direct alphabets, setting them so that plain-text M equals cipher F, and then noting what plain-text A equals; or by setting a reversed alphabet against the series of columns produced in the "running down" process so that A of the reversed alphabet is opposite the group of cipher letters which has been "run down." The key-letter will be found on the reversed alphabet directly opposite the plain-text equivalents of the group of cipher letters. This method of deciphering is called "Solution by Running Down" or "Solution by Means of a Poly-Alphabet." An actual example will make this clear. If these two groups of cipher letters are "set" at the top of the Poly-Alphabet, the following generatrices are produced:

```
 0. FXGPH NEWUX  0.        13. SKTCU ARJHK 13.
 1. GYHQI OFXYV 25.        14. TLUDV BSKIL 12.
 2. HZIRJ PGYWZ 24.        15. UMVEW CTLJM 11.
 3. IAJSK QHZXA 23.        16. VNWFX DUMKN 10.
 4. JBKTL RIAYB 22.        17. WOXGY EVNLO  9.
 5. KCLUM SJBZC 21.        18. XPYHZ FWOMP  8.
 6. LDMVN TKCAD 20.        19. YQZIA GXPNQ  7.
 7. MENWO ULDBE 19.        20. ZRAJB HYQOR  6.
 8. NFOXP VMECF 18.        21. ASBKC IZRPS  5.
 9. OGPYQ WNFDG 17.        22. BTCLD JASQT  4.
10. PHQZR XOGEH 16.        23. CUDME KBTRU  3.
11. QIRAS YPHFI 15.        24. DVENF LCUSV  2.
12. RJSBT ZQIGJ 14.        25. EWFOG MDVTW  1.
```

The decipherer has simply to examine the successive generatrices to find where the plain text appears. Such an examination takes but a few minutes, and this process should be applied to almost every new problem at the very outset — it may solve the problem, or may furnish valuable clues to the solution. Now note that the plain-text words in these two groups might have been secured by "running up" as well as by "running down," because of the continuous or cyclic nature of the alphabet. "Running up" may be regarded as reversing the process applied in enciphering, in order to get back to the line where the plain text is located; "running down" may be regarded as continuing the process applied in enciphering until one completes the cycle and thus arrives at the line where the plain text is located. This is simply stated for the purpose of pointing out the cyclic nature of the alphabet. By "running down" one must pass over an interval of seven letters in this case; by "running up" one must pass over an interval of nineteen letters. The sum of these two intervals is twenty-six, the total number of letters in the alphabet. In the case of any message, enciphered by means of a direct alphabet, the sum of the intervals necessary to pass over in the "running down" and the "running up" processes is twenty-six. The number of intervals in the "running down" process in any direct alphabet cipher is determined by the number of intervals the alphabets have been shifted in enciphering — or, in other words, by the key-letter. If successive words of a message were enciphered by different key-letters, or in other words, if a series of alphabets were used, it is apparent that the successive words would reappear on different generatrices. This leads to the consideration of the solution of the case where a series of direct alphabets is used.

(b) Series of Direct Alphabets.

In the example above, once the key-letter has been determined upon by the encipherer, he proceeds to encipher the whole message by means of that particular single direct alphabet. Now suppose the correspondents determine to use a key-word, and to encipher the successive words in the message by means of the different key-letters in the word. Thus, suppose the key-word BOSTON has been agreed upon; the first word of the message is enciphered by means of the direct alphabet in which sound A is represented by symbol B; the second word, by means of the direct alphabet in which sound A is represented by symbol O; the third word, by means of the direct alphabet in which sound A is represented by symbol S, etc., until six words have been enciphered. The seventh word then begins a repetition of the cycle. Thus not only might a key-word of many letters be used, but also a key-phrase might be used, at the will of the correspondents, or perhaps the running text of a book might be used. With the key-word SPRING, the message "Repeat the last order. Errors make it impossible to read," would be enciphered thus:

```
S      P   R    I     N      G    S  P          R  I
REPEAT THE LAST ORDER ERRORS MAKE IT IMPOSSIBLE TO READ
JWHWSL IWT CRJK WZLMZ REEBEF SGQK AL XBEDHHXQAT KF ZMIL
```

The message would then be sent in groups of five letters as usual.

Now notice that cipher letter W represents E in the first word, H in the second word, and O in the fourth. Cipher letter J represents R in the first word and S in the third. In fact, any given cipher letter may represent many different plain-text letters, depending upon the number of different key-letters used, and it follows that the frequency, on the basis of a single alphabet, of any given cipher letter in such a message would give no indication whatsoever as to the letter or letters for which it stands, as will be explained below.

The crest and trough appearance of a graphic frequency table of normal text, or

of a cipher message involving the use of only one direct alphabet, is due not only to the fact that there is a wide variation in the frequency with which the different sounds of the language are used, but also to the fact that in such a piece of text, or in such a message a single letter represents one and only one sound, or in other words that a given symbol always represents the same sound. But since in the case under discussion one cipher letter may represent a multiplicity of sounds (plain-text letters), and since the individual frequencies of the sounds represented varies greatly, it follows that the frequency table as a whole will not present the crest and trough appearance, but will appear "solid." It would be impossible to pick out the representative of E, or any other letter. However, if the "running down" process is applied to the cipher letters, the plain-text words will reappear on different generatrices, as stated above. This is because the alphabets used to encipher the successive words have been shifted a varying number of spaces in accordance with the different key-letters, and hence, when the "running down" process is applied, the number of intervals which must be passed over differs in the case of each word, and therefore the plain-text words must come out on different lines. The example above will serve as an illustration.

```
JWHWSLIWTCRJKWZLMZREEBEFSGQKALXBEDHHXQATKFZMIL
KXIXTMJXUDSKLXAMNASFFCFGTHRLBMYCFEIIYRBULGANJM
LYJYUNKYVETLMYBNOBTGGDGHUISMCNZDGFJJZSCVMHBOKN
MZKZVOLZWFUMNZCOPCUHHEHIVJTNDOAEHGKKATDWNICPLO
NALAWPMAXGVNOADPQDVIIFIJWKUOEPBFIHLLBUEXOJDQMP
OBMBXQNBYHWOPBEQREWJJGJKXLVPFQCGJIMMCVFYPKERNQ
PCNCYROCZIXPQCFRSFXKKHKLYMWQGRDHKJNNDWGZQLFSOR
QDODZSPDAJYQRDGSTGYLLILMZNXRHSEILKOOEXHARMGTPS
REPEATQEBKZRSEHTUHZMMJMNAOYSITFJMLPPFYIBSNHUQT A=S
      RFCLASTFIUVIANNKNOBPZT  GKNMQQGZJCTOIVRU A=R
      SGD    GJVWJBOOLOPCQAU  HLONRRHAKD  JWSV
      THE    HKWXKCPPMPQDRBV  IMPOSSIBLE  KXTW A=P
             ILXYLDQQNQRESCW              LYUX
             JMYZMERRORSFTDX              MZVY A=N
             KNZAN      GUEY              NAWZ
             LOABO      HVFZ              OBXA
             MPBCP      IWGA              PCYB
             NQCDQ      JXHB              QDZC
             ORDER      KYIC              READ A=I
                        LZJD
                        MAKE                   A=G
```

The key-letters are sought, as each word is deciphered, by the same methods as explained above. Simply setting two direct alphabets so that, for example, in the case of the first word, plain-text R was represented by cipher J, in which instance A was represented by cipher S. In the same way, P equals A in the second word, R equals A in the third, I equals A in the fourth, N equals A in the fifth, and G equals A in the sixth. Then the cycle repeats itself, until the whole message has been deciphered. In this case each word was enciphered by a different alphabet. This system may be varied by enciphering every group of five, ten or more letters by the various key-letters instead of each word, but the solution is attained by the same procedure, except that a little more study is necessary in order to pick out the entire words.

Reversed alphabet ciphers will now be considered.

(a) Single Alphabet.

EXAMPLE

XFWNV PYGIF PWYBZ FYLQV SFWGF SQCFX RFYOF
RYBJI YFQVQ CFUFW JYQBF RVEQC FYJNB EQCFL
ZWFNQ CJQNC FSFOF SQCFL XBDCQ EYFFQ CFBSB
GFWQB QLHVP YGWVQ EJBYQ VIFGB RHVOF SFGJR
PSFXF JWRVE BGFWQ BEBHJ QBVWN VPYGW VQVWY
LCJOF QCFFE EFHQV EGFQF SSBWD ESVXH SBXFB
WDFWF SJYIP QNVPY GFOBG FWQYL WPYYB ELJYY
JQQFX UQRVE NCJQF OFSZB WGJQJ RPIRQ BQPQB
VWVEU FSRVW RWVBX UFSRV WJQBV WRVEJ UFWRB
VWFSV SJXBR RBWDC FBSVS JIPRB WFRRX JWHVP
YGFOF SCVUF QVIFR PHHFR REPY

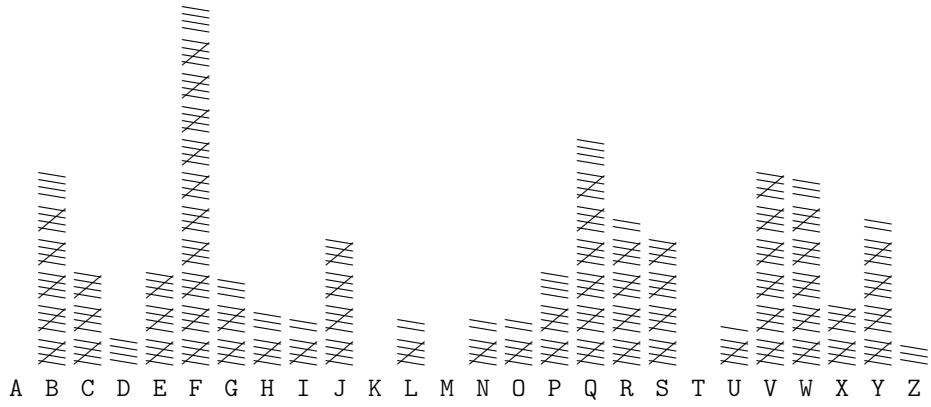


Fig. 8.

In the accompanying frequency table (Fig. 8), the letter F, which marks the highest crest in the table, is selected as the equivalent of plain-text letter E. Attempts made to "fit" this table to the normal, on the assumption of a direct alphabet, do not give good results, but on the assumption of a reversed alphabet, an excellent "fit" is obtained, the correct plain-text values may be assigned at once and substitution results in the solution of the message. Note that the relative positions of the crests and troughs have remained the same here as in the preceding encipherments of the same message. Only the direction of "reading" the series of crests and troughs has been reversed. The first two lines are as follows:

XFWNV PYGIF PWYBZ FYLQV SFWGF SQCFX
MENWO ULDBE UNLIK ELYTO RENDE RTHEM

RFYOF RYBJI YFQVQ CFUFW JYQBF RVEQC
SELVE SLIAB LETOT HEPEN ALTIE SOFTH

This is a "Solution by Frequency Table." But this message also may be solved by the "running down" process, or by the Poly-Alphabet. Suppose two alphabets, one direct, representing the sequence of sounds, the other reversed, representing the sequence of symbols, are now taken for experiment to try to find the relative positions these two

sequences were in when the enciphering was done, just as was done before. Setting A to Z in this position, the two sequences are as shown below:

Sequence of Sounds (= Plain text) — ABCDEFGHIJKLMNOPQRSTUVWXYZ
Sequence of Symbols (= Cipher text) — ZYXWVUTSRQPONMLKJIHGFEDCBA
Cipher letters — XFWNV
Sounds indicated — CUDME

This series of letters does not "spell" any plain text, so that evidently the two sequences were not in the position indicated. We therefore move the sequence of symbols one space to the right, and try again. Thus:

Sequence of Sounds (= Plain text) — ABCDEFGHIJKLMNOPQRSTUVWXYZA
Sequence of Symbols (= Cipher text) — ZYXWVUTSRQPONMLKJIHGFEDCBA
Cipher letters — XFWNV
Sounds indicated — DVENF

This series of letters also does not "spell" any plain text, so we therefore move the sequence of symbols one more, then two, three, etc., spaces to the right, each time noting whether the juxtaposition of the plain-text equivalents results in the spelling of a word. At the 11th experiment the results are as follows:

Cipher letters — XFWNV
Sounds indicated — MENWO

Now tabulate the results of these experiments:

	Cipher letters —	XFWNV
A = Z —	Results of 1st experiment —	CUDME
A = A —	Results of 2nd experiment —	DVENF
A = B —	Results of 3rd experiment —	EWFOG
A = C —	Results of 4th experiment —	FXGPH
A = D —	Results of 5th experiment —	GYHQI
A = E —	Results of 6th experiment —	HZIRJ
A = F —	Results of 7th experiment —	IAJSK
A = G —	Results of 8th experiment —	JBKTL
A = H —	Results of 9th experiment —	KCLUM
A = I —	Results of 10th experiment —	LDMVN
A = J —	Results of 11th experiment —	MENWO

Note now that the net result of the ten separate experiments *after the first experiment* was simply the continuance of the direct alphabet sequence started by the letters given by the very first experiment. In other words, after the first experiment, the process was exactly the same as explained on page **??**. In the latter case, the first experiment began with the continuing of the direct alphabetic sequence started by the cipher letters themselves; in this case, the first experiment began with the finding of the equivalents of the cipher letters when a reversed alphabet was set against a direct alphabet. In this case, A was set opposite Z; but had A been set opposite any other letter, and the same procedure followed, the final result would have been the same as is shown by the following, where Z is arbitrarily set opposite F:

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDE
ZYXWVUTSRQPONMLKJIHGFEDCBA

Cipher letters —	XFWNV
Equivalents on a reversed alphabet —	HZIRJ
	IAJSK
	JBKTL
	KCLUM
	LDMVN
	MENWO

This process of finding the equivalent is spoken of as "finding the reversed alphabet equivalent," or simply "finding the reversed equivalent." In order to solve such a message by means of the Poly-Alphabet, it is therefore necessary first to convert the cipher letters into their reversed equivalents, and then "set" these equivalents. The words of the message will then reappear on some generatrix below. The student should convince himself that "running down" without first finding the reversed alphabet equivalents for the cipher letters will not result in the production of the plain-text for the reason that in encipherment the two sequences, one of sounds, the other of symbols, were going in opposite directions, and therefore, "running down" by means of direct alphabet sequences could not possibly reproduce the plain-text.

(b) Series of reversed alphabets.

Just as the successive words of a message may be enciphered by means of a series of direct alphabets, according to the letters of a key-word, so they may be enciphered by means of a series of reversed alphabets. The reversed alphabet equivalents of the cipher letters would have to be found first, then when these are "run down" the successive words of the message would appear on different generatrixes.

SOLUTION OF SINGLE MIXED ALPHABET CIPHERS

It has been observed so far that in the case of straight alphabet ciphers the correct determination of one value in the message results in the solution of the whole cipher alphabet and the consequent decipherment of the message. The solution could be secured either by means of a frequency table, or by the "running down" process. The solution of mixed alphabet ciphers, however, is secured only by the frequency table method, and that only after considerably more experimentation than is the case with straight alphabet ciphers.

MESSAGE

IQMIN MKIWU TJBIE THTBT SKNTR RMKIJ
YTKKS IRYIM JIQYK DYJXQ KTKMI MMKIQ
MKJSZ IMISX QYJRM BISKB SZIQX YJSRT
KYCSJ ISUMD VYJOY ITSKM AZTCC MEUSJ
MFIMK BTHMU TMREB MJHTX MJMCS JITKL
ISXSD DYKET KLLMK MJYRI QYIBI YITSK
YKEMD VYJOT KLZKE MJQTB ETJMX ITSKB
IQMMK LTKMM JJMLT DMKIY KEIJY TKNTR
RCJMX MEMET HTBTS KVWYI RMYBI IQJMM
EYWB

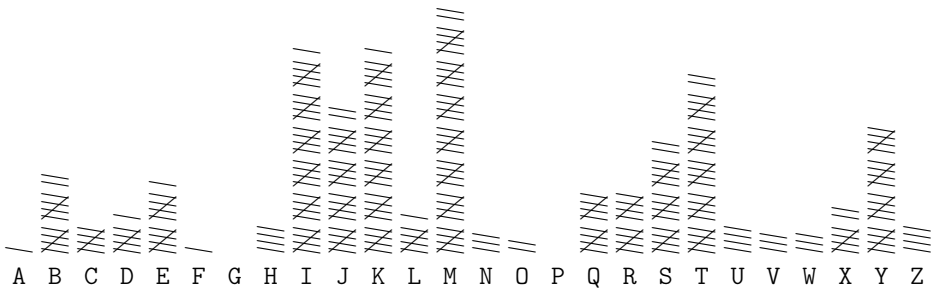


Fig. 9.

All attempts to solve this cipher by applying the Poly-Alphabet having failed, a graphic frequency table is made, and appears as shown in Fig. 9. *The fact that this frequency table shows marked crests and troughs and has proved not to be a straight alphabet cipher means that it is almost certainly a single mixed alphabet cipher*. The solution of such a cipher will be facilitated by the compilation of a special kind of table called a Frequency Table with Prefixes and Suffixes.

There are two kinds of frequency tables, as regards their form only.

(1) THE GRAPHIC FREQUENCY TABLE, which is to show only how many times any letter in a message occurs. It is made simply by placing a stroke opposite the tabulated list of the letters of the alphabet. The fifth occurence of a letter is made by a

diagonal stroke. This will add up the occurences automatically, and the table loses none of its graphic features thereby. Examples of such tables are seen on pages **??**, **??** and **??**.

(2) THE FREQUENCY TABLE WITH PREFIXES AND SUFFIXES, which can be made to show not only how many times any letter occurs, but will also show for each letter what letter precedes it and what letter follows it, each time that letter occurs — information which is necessary for the solution of most ciphers. (See Fig. 10.) The method which has been adopted is this: Write the alphabet in columnar fashion upon a sheet of cross-section paper, devoting one square to each letter. In the message which follows for solution IQMIN is the first group of cipher letters. In the upper half of the first square opposite I in our table a dash is placed to indicate that it has no prefix, being the first letter of the message. In the lower half of the same square the letter Q is written, which is the suffix of I. The next letter to be tabulated is Q. Its prefix, I, is placed in the upper half of the first square opposite letter Q in the table; its suffix M is placed in the lower half of the same square. The next letter to be tabulated is M. Its prefix, Q, is placed in the upper half of the first square opposite M in the table; its suffix, I, is placed in the lower half of the same square. The prefixes and the suffixes of the succeeding occurences of any letter are placed in corresponding positions in the succeeding squares, until the last letter of the message is tabulated. In the lower half of the square concerned, a dash is placed, indicating that it has no suffix. When all the letters have been tabulated in such a manner, the most important data — namely, the recurring groups and the number of their recurrences — may be obtained quickly, and should be placed in a condensed table on the same sheet. This condensed table will show the frequencies of the DIGRAPHS, TRIGRAPHS and POLYGRAPHS, which recur in the message.

(1) A digraph is a pair of letters. Just as certain letters are used more frequently than others in any language, so certain pairs of letters are used more frequently than other pairs of letters.

A digram is a two-letter word.

A frequently recurring digram is also a digraph; but a frequently recurring digraph does not necessarily have to be a digram. Examples: TH is a frequently recurring digraph, but not a digram; IN is a frequently recurring digraph and is also a frequently recurring digram.

(2) A trigraph is a group of three letters.

A trigram is a three-letter word. The statements made above concerning digraphs and digrams apply to trigraphs and trigrams.

(3) A polygraph is a group of more than three letters.

A polygram is a word of more than three letters. The distinctions as given above between digraph and digram apply here also.

In order to show how this data is secured, take the frequency of the letter Q in the accompanying table, Fig. 10. The upper halves of all the squares contain prefixes only, the lower halves, suffixes only. The letter I is indicated as a prefix to Q seven times. This means the digraph IQ occurs seven times. The letter M is indicated as a suffix to Q three times. This means that the digraph QM occurs three times. Now the letter M is indicated three times as a suffix of Q at the same time I is indicated as a prefix. In other words, the trigraph IQM occurs three times. In a similar manner the trigraph TSK is indicated as occurring five times. Now in order to list all the digraphs it is not necessary to find both the recurring prefixes and suffixes to a letter; either the tabulation of the prefixes, or the suffixes, is all that is necessary. For example, the table shows that opposite the letter Q, the letter I is indicated seven times as a prefix; opposite the letter I, the letter

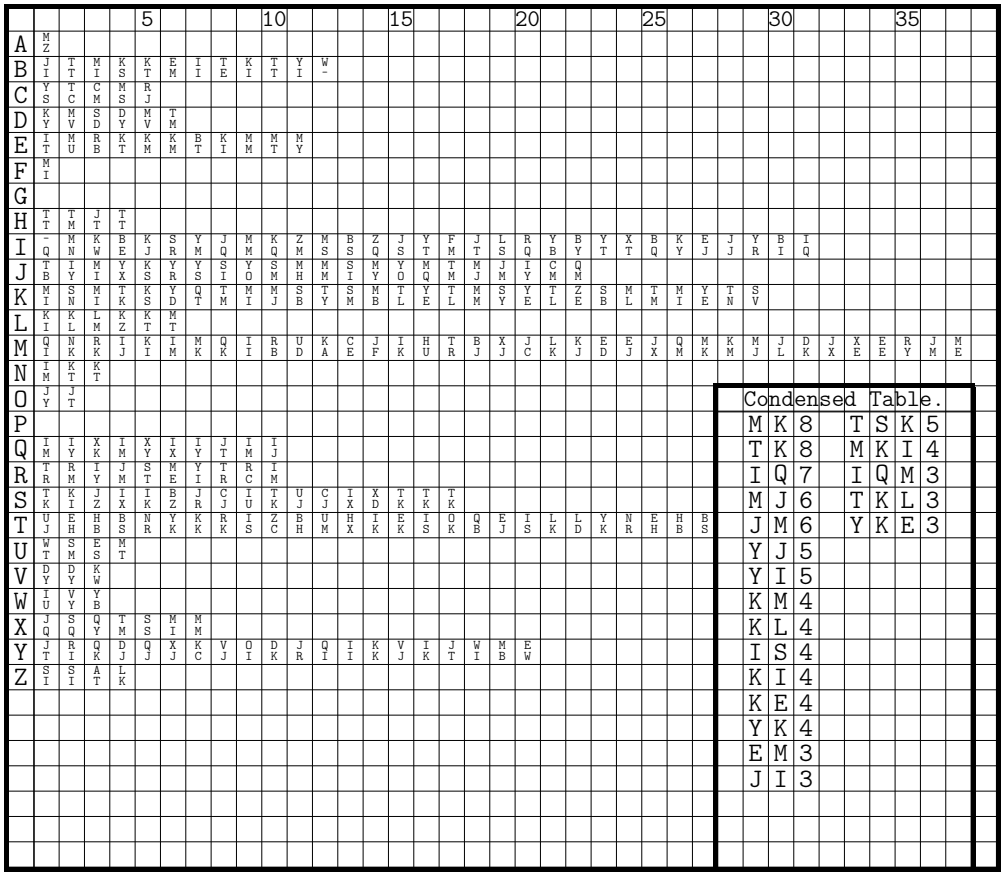


Fig. 10. Frequency Table with Prefixes and Suffixes

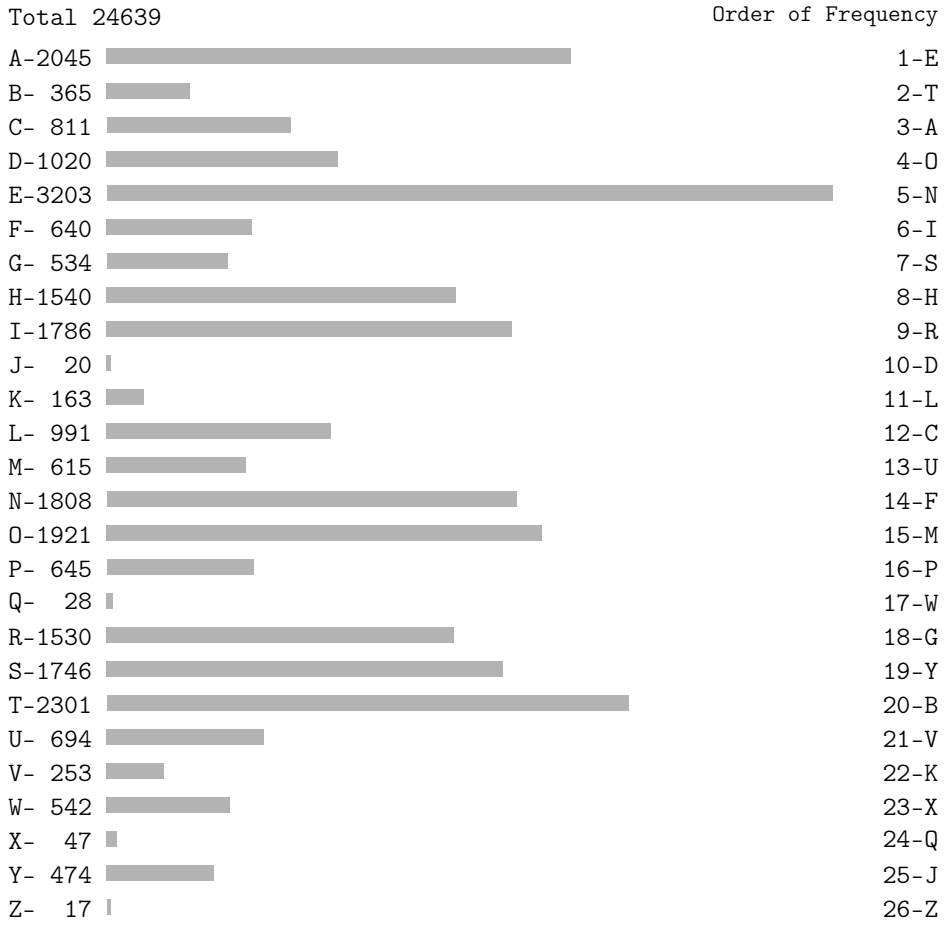
Q is indicated seven times as a suffix. In short, the frequency of the digraph IQ may be secured either from the letter Q, and considering only its prefixes, or from the letter I and considering only its suffixes. As long as the operator is consistent throughout in considering either prefixes only, or suffixes only, the final results will be the same. In the condensed table only recurrences of three or more need be indicated; for the information which may be obtained ordinarily from any less than three recurrences of digraphs or trigraphs is negligible.

Having compiled the data which applies to the particular case in hand, an attempt is to be made to fit the special conditions exhibited by this data to the generalized conditions for ordinary English text as exhibited in a frequency table compiled from a much greater number of letters. If these special conditions happen to approximate or conform closely to the generalized conditions, the normal conditions, in other words, the solution of the cipher will be attained directly. If they do not, considerable experimenting must be done before the solution will be reached. From a frequency table compiled from approximately 25,000 letters taken from various samples of ordinary English text, it has been found that the frequency of individual letters, digraphs and trigraphs is as given in Table I[1].

[1] Compiled 1918 at Riverbank Laboratories. The text was composite in character, passages from literary, scientific, military text, etc., being included.

TABLE I

Frequency Table for English Literary Text



Vowels 39.1%; Consonants LNRST, 34.0%; Consonants JKQXZ, 1.1%

From an inspection of the frequency table applying to this message, shown in Fig. 10, it is seen at once that cipher letter M represents E. Now it is a great advantage to be able to distinguish the cipher equivalents for vowels from those for consonants and the following method will be found useful. In English the vowels E, A, O, and I will usually be found among the first ten cipher letters of highest frequency. Write the ten highest frequency letters in a series and above and below each letter note graphically the number of times the cipher equivalent of E occurs as a prefix and a suffix respectively. Thus, for our message the series is as follows:

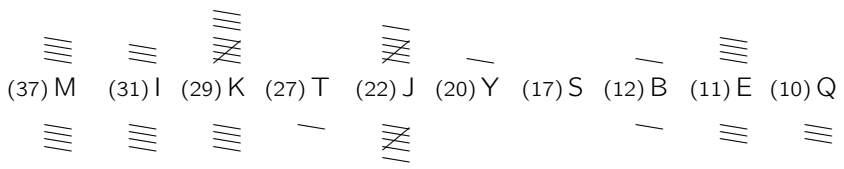


TABLE I *continued*

DIGRAPHS

TH - 748	ES - 370	HA - 272	IS - 231	HI - 209
HE - 694	ST - 327	AT - 265	EA - 225	LA - 205
IN - 465	EN - 312	NT - 259	IT - 223	NE - 182
ER - 420	ND - 305	OF - 257	OU - 218	AL - 181
RE - 412	ON - 298	OR - 238	AR - 216	LE - 169
AN - 403	ED - 278	AS - 237	NG - 215	EC - 163

TRIGRAPHS

THE - 522	HER - 97	HES - 71	VER - 58	WIT - 50
AND - 207	OFT - 77	TIO - 71	ITH - 57	DTH - 50
ING - 171	FTH - 76	ETH - 69	TTH - 57	SIN - 48
ERE - 116	ATI - 73	HIS - 66	ARE - 56	STH - 48
THA - 108	HAT - 73	INT - 65	NTH - 55	TER - 47
ENT - 98	EST - 71	WAS - 59	ALL - 53	REA - 46

Now any of the combinations of E with a high frequency consonant is much more frequent than any combination of E with another vowel. This fact forms the basis of the distinction. Thus, note that cipher letter I has plain-text letter E three times as a prefix and four times as a suffix; cipher letter I is therefore not a vowel. Cipher letter K has plain-text letter E as a prefix nine times and as a suffix five times; it also is therefore not a vowel. However cipher letter T is never preceded by plain-text letter E and is followed by it only once. This indicates that T is certainly a vowel. On this basis, the letters M, T, Y, S, and possibly B, may be taken to be vowels; while I, K, J, E, and Q, may be taken to be consonants.

Having thus determined the probable vowels and the probable consonants, we return to the frequency table and note what combinations are indicated with several of the high frequency letters. Cipher letter M has already been assumed to be E. Cipher letter I having been assumed to be a consonant, and being the second highest letter in frequency in the table, it would be logically assumed to be T. The condensed table shows that the trigraph IQM occurs three times, and might well be THE. The frequency table is consulted therefore to corroborate the assumption that Q represents H. It should show that Q is relatively low in frequency, and that it is often preceded by I, the letter which has been assumed to be T, since the digraph TH is among the most frequent in English. These conditions are complied with fully in our table, since Q is seen to occur ten times, seven times of which it is preceded by I; consequently, the assumption made stands corroborated, and these values are filled in throughout the message.

The results are as follows:

```
IQMIN MKIWU TJBIE THTBT SKNTR RMKIJ
THET  E T      T               E T

YTKKS IRYIM JIQYK DYJXQ KTKMI MMKIQ
      T  TE  TH       H    ET EE TH

MKJSZ IMISX QYJRM BISKB SZIQX YJSRT
E     TET   H   E  T      TH
```

```
KYCSJ ISUMD VYJOY ITSKM AZTCC MEUSJ
      T  E        T   E       E

MFIMK BTHMU TMREB MJHTX MJMCS JITKL
E TE     E   E    E     E E    T

ISXSD DYKET KLLMK MJYRI QYIBI YITSK
T             E  E   T H T T  T

YKEMD VYJOT KLZKE MJQTB ETJMX ITSKB
   E             E H      E  T

IQMMK LTKMM JJMLT DMKIY KEIJY TKNTR
THEE     EE   E    E T    T

RCJMX MEMET HTBTS KVWYI RMYBI IQJMM
   E  E E                E  T TH EE

EYWB
```

At once it is noted that within the message two sequences of letters look favorable. With the values already assumed they stand as follows:

```
MIMMKIQMKJ ------ IQYIBIYIT
 ETEE-THE-        TH-T-T-T-
```

The first of these suggest at once a word ending in TEEN or TEENTH. Hence K, which was one of the letters indicated as a consonant by the reasoning given on page **??** is assumed to represent N, and the assumption checked by the frequency table. Also Y, which was likewise assumed to be a vowel by the same reasoning, should evidently represent A, and the frequency table is consulted to see whether Y is high enough in frequency to represent A. The frequency table shows Y to be high and accordingly Y is substituted throughout by A as well as K by N. Now the trigraph YKE occurs three times and Y having been assumed to be A, and K to be N, YKE may well be AND. These values are also substituted throughout.

Now the digraphs ER and RE are among the most frequent in English. M has already been assumed to be E, so that it is necessary to search for a letter which, as a suffix with M, might respresent ER, and as a prefix with the same letter, might represent RE. In other words, a high frequency reversible combination is sought. Here are the combinations with M which present themselves for study:

```
MK - 8          JM - 6
MJ - 6          EM - 3
KM - 4
```

Of the letters which occur in combination with M, J is the only one to which a value has not already been given and J was indicated previously as being a high consonant. MJ, occurring six times, may well stand for ER; and so likewise JM, six times, for RE. The frequency table is consulted to see if J may represent R, and it is seen to be very good for that letter. Accordingly these values are substituted throughout the message. The results of all these substitutions are shown below:

```
IQMIN MKIWU TJBIE THTBT SKNTR RMKIJ
THET  ENT    R TD        N     E TR

YTKKS IRYIM JIQYK DYJXQ KTKMI MMKIQ
A NN  T ATE RTHAN  AR H N NET EENTH

MKJSZ IMISX QYJRM BISKB SZIQX YJSRT
ENR   TET   HAR E  T N    TH  AR

KYCSJ ISUMD VYJOY ITSKM AZTCC MEUSJ
NA  R T  E    R A T  NE       E   R

MFIMK BTHMU TMREB MJHTX MJMCS JITKL
E TEN    E   E D  ER    ERE   RT N

ISXSD DYKET KLLMK MJYRI QYIBI YITSK
T      AND  N  EN ERA T HAT T AT  N

YKEMD VYJOT KLZKE MJQTB ETJMX ITSKB
ANDE   AR   N  ND ERH   D RE  T  N

IQMMK LTKMM JJMLT DMKIY KEIJY TKNTR
THEEN   NEE RRE    ENTA NDTRA  N

RCJMX MEMET HTBTS KVWYI RMYBI IQJMM
  RE  EDED        N  AT  EA T THREE

EYWB
DA
```

This is about as far as the frequency of single letters, digraphs and trigraphs will carry the decipherer. Further progress must be made by assuming probable words from the skeletons of words shown by the working sheet. Incorrect assumptions soon manifest themselves as such because they will bring into juxtaposition, letters forming impossible combinations. The decipherer therefore should not bind himself rigidly to the rules and requirements of frequency of ordinary text; he should be ready at all times to free himself from any rules or requirements which lead him to no results.

The cipher letters of high frequency which still remain undecided are T and S, which have been indicated as vowels, and of the medium frequency letters, B and R. The representatives of the vowels O and I have yet to be found. The decipherer might experiment with these high frequency letters, trying the former pair out for O and I, and the latter pair for S and L, but another way is to examine the text carefully and try to assume a word. This combination is seen in the last two groups of the second line:

```
KTKMIMMKIQ
N-NETEENTH
```

The letter T, both in position here and in frequency, could well stand for I, giving in this place the word NINETEENTH. When the value of T is substituted throughout the message, the following sequence is noted:

```
YKETKLLMKMJYRIQYI
 ANDIN-ENERA-THAT
```

The repeated cipher letter L limits the assumptions for its plain-text equivalent very greatly and the words COMMANDING GENERAL are suggested at once.

A trial of this "guess" results in giving excellent combinations and no impossibilities anywhere. These new values are assigned throughout and the entire message may now

be deciphered with ease from the context. This is an illustration of what a good "guess" may lead to, based upon the conditions of the text.

The complete message is as follows: "The Twenty-first Division will entrain not later than March nineteenth enroute to Charleston, South Carolina, port of embarkation, equipped for extensive field service, reporting to commanding general that station and embarking under his directions. The engineer regiment and train will precede Division by at least three days."

In a short message where the ordinary frequency method has failed to lead to solution, because the approximation of the frequency of any letter to the normal frequency table is not close, a method which will often lead to results and which depends upon the assumption of a probable word in the plain-text, is as follows:

Given the cipher groups, IQMIN MKIWU TJBIE THTBT SKNTR, if it is suspected that the message contains a word relative to troop movement, the word DIVISION may be assumed. The requirements of this word are these:

The first letter is medium in frequency.

The second letter is high in frequency and coincides with the fourth and sixth letters.

The third letter is very low in frequency.

The fifth letter is high in frequency.

The seventh letter is high in frequency, as is the eighth, and these should combine in a digraph which is medium in frequency.

One begins, therefore, by attempting to locate this word, looking first for a place where three identical letters are separated by one interval between the first and second, and the second and third appearances. The only possibility is THTBT. When the values derived from this assumption are substituted throughout, the results are as follows:

```
IQMIN MKIWU TJBIE THTBT SKNTR
      N-- I-S-D IVISI ON-I-
```

The combination -I-S-DIVISION suggests FIRST. These assumptions are all substituted throughout, and if no impossible combinations result, are assumed to be correct. Further assumptions are then made, and the process continued as in the preceding method. Such a method as this is to be used only as a last resort, when frequency methods have failed after repeated attempts toward solution.

Cases are encountered in which a single cipher letter stands for two different plain-text letters; but because of the possibilities for error and misinterpretation, such double values usually involve a high frequency letter coupled with one of low frequency, so that the context would determine which of the two is correct. Such cases give no trouble to the decipherer because the high frequency letters, digraphs, and trigraphs are still prominent. The alternate values soon disclose themselves in the process of decipherment and cause no further difficulties.

The method shown here for solving a simple single mixed alphabet cipher is applicable to all cases where only one alphabet is concerned, whether that alphabet involves the use of letters, signs, figures, or combinations of these three symbols. In most of the cases where more than one alphabet is involved, if the cipher can be reduced to single alphabet terms, that is, if the message can be rearranged so that its constituent parts may be examined on the basis of single alphabets, the solution can nearly always be reached with little difficulty.