CHAPTER VIII

Substitution Types

Substitution cipher presupposes the selection of a set of symbols which can represent the letters or words of messages. As to what these symbols may be, there is practically no limit; we meet substitution in our every-day life: the dots and dashes of the Morse alphabet, the pot-hooks of shorthand, the combinations of Braille, and so on; and we hear of its use in the sign-language of Indians and Gipsies, or in the drum-language of the African jungle. These, of course, are not cipher, yet in each case the plain language has been replaced with symbols. Considering the use of symbols for cipher purposes, there are doubtless many among us who played, as children, with the alphabet of the " Masonic " cipher, based upon a design like the one used for ticktacktoe. Lord Bacon's alphabet has already been mentioned. The use of printers' symbols, and similar characters, can be seen in the works of Edgar Allan Poe. Charles I of England is said to have used a cipher alphabet in which letters were represented by a series of dots, placed in certain positions with reference to the line of writing. An endless number of queer symbols is met with in fiction, such as the use of the little dancing men by Sir Arthur Conan Doyle. Cipher alphabets of the nature mentioned do not produce ciphers in any way different from those produced by substitution with letters and numbers; as a matter of fact, the decryptor who must deal with a cryptogram made up of arbitrary signs usually begins the work by making a substitution of his own, replacing each unfamiliar symbol with some one letter (or number). We will confine our discussion, then, to those characters which are transmissible by Morse.

Substitution ciphers may be classified under four major types, each having its subdivisions and variations, and its intercombinations with other types:

1. *Simple substitution* (also called *monoalphabetic substitution*) makes use of only one cipher alphabet.

2. *Multiple-alphabet substitution* (also called *double-key substitution, polyalphabetic substitution,* etc.) makes use of several different cipher alphabets according to some agreed plan.

The term " multisubstitutional " is sometimes applied to the multiple alphabet cipher, but more correctly refers to a certain form of the simple substitution cipher, in which the single alphabet is so designed as to provide optional substitutes for all or part of the letters.

3. *Polygram substitution* provides a scheme by means of which groups of letters are replaced integrally with other groups, which may be of letters or of numbers.

4. *Fractional substitution,* which requires a certain type of cipher alphabet, breaks up the substitutes for single letters, and subjects these fractions to further encipherment. More often than not, the result is a combination cipher, rather than a purely substitutional one.

CHAPTER IX

Simple Substitution — Fundamentals

Simple substitution is ordinarily defined as a cipher in which each letter of the alphabet has one fixed substitute, and each cryptogram-symbol represents one fixed original. When this cipher is used for puzzle purposes, as we find it in our newspapers and popular magazines, the substitutes (which are invariably letters of the alphabet) may be chosen at random, and the cryptograms must follow certain arbitrary rulings which are designed to make them " fair ": Word-divisions and punctuation must follow religiously those of the original text; a certain minimum of length must be provided; no letter may act as its own substitute; foreign words are not permissible; and so on. Aside from the observance of such rules, however, no holds are barred; the constructor of such a cryptogram, totally unconcerned with the meaning of his plaintext (except that it must have one), sometimes gives his chief attention to distorting the normal language characteristics in an effort to baffle the analyst, and often will carefully search his dictionary for words like *yclept, crwth, syzygy, pterodactyl, ichthyomancy,* not infrequently producing a plaintext which is almost as incomprehensible as its corresponding cryptogram. Our study here will be confined to the simple substitution cipher as applied to normal English text.

When a substitution key (a pair of alphabets) is being used for cipher purposes, the letters which make up the cipher alphabet cannot be chosen at random; the key must be of such a nature that any one of the several correspondents, desiring to make use of it, will have it at his disposal. Word-divisions are usually concealed, or, occasionally, falsified. Punctuation, if used at all, must don the apparel worn by the rest of the text; no limitations can be placed on length, and no word whatever can be barred, where the intention is that of conveying actual messages; and it is not at all uncommon to find that one or more letters are serving as their own substitutes.

In discussing keys, we will make some arbitrary rulings of our own, but only in the interests of clarity. We will assume, for all cases, that the two necessary alphabets are always written horizontally, as several are shown in Fig. 59; that wherever the two complete alphabets appear, the upper of the pair is always the one in which plaintext letters must be found, so that the lower one is always the cipher alphabet. Thus, whenever the two alphabets are written out in full, the substitute for any given plaintext letter will be the letter standing immediately below it; and the original of any cipher letter will be the letter standing just above it. Wherever it seems advisable to show a distinction, the cipher letters will be expressed as capitals and the plaintext letters will appear in lower case.

Among the oldest cipher alphabets ever used for practical purposes are those of the type called " Caesar," one such alphabet having been used by Julius Caesar, and another by Octavius. As may be seen at (a) of Fig. 59, this type of cipher alphabet is no more than a simple *shifting* of the normal alphabet to a new point of beginning. Using this particular example, the word " Caesar " will be enciphered as *F D H V D U;* or, if the word *R Y H U* is found in a cryptogram, it deciphers as " over."

At (b) of the same figure, we have a pair of *inverse* normal alphabets. Here, it is not necessary to specify that one of the pair is a plaintext alphabet and the other

a cipher alphabet; whenever a plaintext alphabet is merely reversed and allowed to serve as its own cipher alphabet, the encipherment becomes *reciprocal;* that is, whenever *Z* is the substitute for *A*, then *A* will also be the substitute for *Z*, and so for other letters. Thus, we need not write down more than half of the key shown at (b); and, in any other case of reciprocal alphabets, only enough of it to make sure that we have all 26 of the letters; after that, we may find them where we please, both for encipherment and for decipherment. Simple reciprocal alphabets are also ancient. The one just mentioned, and also the one shown at (c), are both said to have been used in parts of the Bible. The two inverse alphabets of (b) may, of course, be *shifted* with reference to each other; that is, one or the other may be caused to begin at any desired letter, just as is done with the ordinary alphabet in deriving one of the " Caesars." It is also possible, as indicated at (d), to divide the

Figure 59

Some Simple Substitution Keys

(a)

A shifted, or "Caesar," alphabet:

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

(b)

A pair of inverse alphabets:

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

Other examples of the RECIPROCAL alphabet:

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

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

normal alphabet into its two halves, and shift one of the halves; in this case the encipherment would be reciprocal whether or not the shifted portion runs in reverse order. At (e) and (f), we have mixed (or interverted) alphabets which, though crude, are more in line with modern practice than those which precede them, since both of these are based on the key-word CULPEPER.

The usual plan for deriving cipher alphabets from key-words is as follows: First, all repeated occurrences of any same letter, such as the second *P* and the second *E* of the word CULPEPER, are discarded. The unrepeated letters of the key-word, as *C U L P E R*, are placed at the beginning of the cipher alphabet, and the rest of the 26 letters are made to follow these, usually in their normal alphabetical order. If an adequate key-word be chosen, for instance the word UNCOPYRIGHTABLE, a well-mixed alphabet results; but, in order to have a cipher alphabet which is truly incoherent, and hard for the decryptor to reconstruct, we may write this already-mixed alphabet into block form and subject it to a transposition of some kind. Several examples of this may be examined in Fig. 60. In example (a), the repeated letters of the key-word have merely been discarded, while example (b) retains these two positions in order to produce more and shorter columns, with three different lengths. In both cases, the columns of the block have been taken out by descending verticals to form cipher alphabets (a) and (b), but the transposition may follow any desired route or other process. Example (c) suggests further uses for key-words. Still another process (not shown) consists in writing the key-numbers above a block, exactly as in example (c), and allowing them to govern the *lengths of rows.* In the writing-in of the alphabet, normal or mixed, the first row of letters is made

to end under key-number 1, the second row under key-number 2, and so on, so that the completed block contains rows of different lengths; it may then be taken off by columns, or otherwise. Numerous other devices exist, but it should be plain from the foregoing that we have an unlimited field in which to derive well-scrambled cipher alphabets, so that there is no need whatever for forming one at random and later being unable to set it up again.

Figure 60

Some Methods for Forming a Keyword-Mixed Alphabet

Keyword: CULPEPER

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

*)(An OHAVER Method).

(a)

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

(b)

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

(c)

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

For the *encipherment* of substitution cryptograms, the plaintext is first written out in full with enough space between its lines to allow for the later insertion of cryptogram-letters. The correct substitute for each letter is then written below it, after which, these substitutes are nearly always marked off into five-letter groups, and the groups are taken off on another sheet to form the finished cryptogram. It is sometimes recommended that plaintext and cipher letters be written in two different colors, so as to avoid any risk of taking off portions of plaintext along with a cryptogram.

Figure 61

"Running Down the Alphabet"

```
Cryptogram:  Y B P R O B Q L...
             Z C Q S P C R M...
             A D R T Q D S N...
Plaintext:   B E S U R E T O...
```

For *decipherment*, the plan is the same, except that the cryptogram is written first, and the two alphabets of the key exchange their functions. Often, when the cipher alphabet in use is so incoherent that its letters are not quickly found, the decipherer will prepare for himself a special *decipherment key*, in which he places the letters of his cipher alphabet in straight alphabetical order, and allows the plaintext alphabet to grow mixed.

In taking up the *decryptment* of simple substitution, we may dispose summarily of the Caesar alphabets by pointing to Fig. 61. If we suspect that one of these has been used, we may verify the suspicion by taking some ten-or-fifteen-letter segment of the cryptogram, and, with each of its letters as a beginning, extend the ten or

fifteen alphabets, a few letters at a time, until we come to the line which is purely plaintext. This process is popularly known as " running down the alphabet," and whenever it results in a row of plaintext, we may quickly determine the amount of " shift," set up the cipher alphabet, and start deciphering.

The same thing is true of a pair of *inverse normal alphabets* which have merely been *shifted with reference to each other*. But in this case, the cryptogram (or that segment of it which is being investigated), *must first be enciphered in the same kind of alphabet*. To explain this, suppose that our cryptogram fragment is *B Y K I L V J O*. If we encipher this with the pair of inverse alphabets which was shown at (b) of Fig. 59, we obtain a new cryptogram fragment *Y B P R O B Q L*. This new fragment is now a " Caesar," and we may " run it down the alphabet " until we find its plaintext. This particular fragment was done with a pair of inverse normal alphabets in which the lower one began at *C*, instead of at *Z*. Most decryptors, in dealing with any kind of substitution, will make these two tests before trying anything else. When the guess proves correct, a great deal of paper work can be saved.

Concerning decryptment in the case of the less simple alphabets, the true vulnerability of simple substitution can be seen when the word " battalion," enciphered in alphabet (f) of our Fig. 59, becomes *T S B B S M Z E P*. Since each letter of the alphabet may have only one substitute, the pattern of *-atta-* shows up clearly in its enciphered version *-SBBS-*. The decryptor knows instantly what kind of pattern it represents, since the letters *S* and *B* can have only one original each. The frequency with which these two letters have been used in his cryptogram will tell him approximately what their two originals ought to be, and, by making a few trials, he loses little time in arriving at a solution. As a matter of fact, a simple monoliteral substitution, given fewer than a hundred letters of text and no information whatever as to source or subject-matter, can be decrypted purely through the frequencies and other characteristics of its letters; and if, in addition, the original word-divisions have been preserved, we have the lengths and patterns of these words, plus the knowledge that individual letters have their favorite positions in words.

The " Crypt " with word-divisions. — Not infrequently, the cryptogram which retains its word-divisions can be read at sight, without putting pencil to paper, and this regardless of how short it may be. Again, even though based on normal text, it will prove more troublesome; and thus, in dealing with this type of simple substitution, we attack each individual example according to what appears at first glance to be its greatest weakness. The cryptogram shown in Fig. 62, for instance, would be attacked through its many *short words*, probably the simplest of the available methods. The words in question are those numbered 3 (*RD*), 4 (*MD*), 9 (*QYR*), 11 (*RKV*), 13 (*DF*), and 15 (*DN*). Among the two-letter words, it is noticeable that every one of these includes a letter *D*, used indiscriminately as the initial or final letter. We do not need to know much of cryptanalysis to guess that this letter represents the *o* found in such words as *to, no, do, go, of, on, or*. A comparison of the two three-letter words shows that these, also, have a common letter, *R*, which ends one of these words and begins the other. Of all words in English, the commonest is *the*. If *RKV* be assumed as *the*, then *RD*, already thought to contain *o*, will check as *to*, another extremely common word.

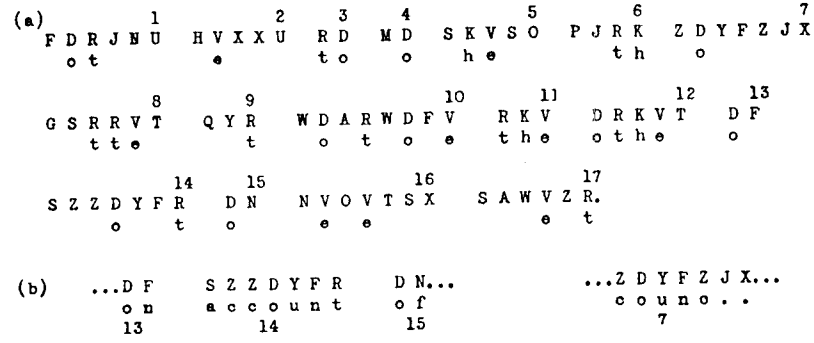
Thus we are able to begin work by *tentatively assuming* that the four cryptogram letters *R, K, V*, and *D*, are the substitutes, respectively, for plaintext letters *t, h, e*, and *o*. These assumptions are tested by actually making the necessary substitutions directly on the cryptogram, as seen at (a) of Fig. 62. And we may be sure that they are correct when we see the 12th word clearly outlined as *other*. This word gives a new substitution: cipher letter *T* evidently represents *r*, occurring in three

different words; the actual making of this substitution will cause the 8th word to show a very common ending: *-tter*.

If we now consider the other three-letter word, the 9th of the cryptogram, we see that *QYR* cannot represent any one of the common words *not, got, out, yet*, since the substitutes for *o* and *e* have already been determined. It may, however, represent the common word *but*, especially if we care to investigate the frequency in the cryptogram of its first letter, *Q*. This letter has been used only once; and its assumed original, *b*, is normally of very low frequency, and, in addition, is known to have a fondness for initial positions. The assumption of this word as *but* gives us the substitute for *u*, which appears to be *Y*.

Figure 62

Making Substitutions



In addition to the points mentioned, it is not unusual to find that short words, by their very positions with reference to some longer word, will identify a whole sequence, as might happen with the sequence shown at (b) of the same figure. Good examples of this are: *as well as, as soon as, in order to*, and so on. In this particular case of (b), we began with only the identified *o*, and immediately were able to identify *t;* this alone should serve for spotting the whole sequence *on account of*, taking into consideration the doubled *c*. Notice what the identification of the word *account* will do toward identifying the 7th word.

Among methods which do not seem indicated in the given example, there is a very fertile field for research in the examination of *terminal sequences*. When two or more of the affixes *-tion, -ing, in-*, and *con-* are present in the same text, as they practically always are, they will serve to identify one another, and may, in addition, be cross-compared with many of the short words, as *in, on, no, not, into, upon, can*. The prefix *sub-* may serve to identify the word *but*. There is a whole group *-ment, -ence, -ance, -ency, -ancy;* another group *pre-, re-, -er, de-, -ed*, etc.; or a good comparison in *be-, -able, -ible*, etc.

Still a third road to solution, especially popular with those who solve the " aristocrats," is found in *pattern words*, that is, words having one or more letters repeated. The puzzler, examining a dictionary, prepares lists for his permanent use, one list for each " pattern "; such a list, for instance, would contain PATTERN, FALLING and all other words in which the third and fourth letters are the same and all others different, another would contain all words having the pattern STATE, DEFER, ROBOT, still another all words of the pattern BANANA, ROCOCO, and so on. The solver, having thus armed himself in advance, begins work by searching his cryptogram for words having repeated cipher letters, and attempts to identify these

from the proper lists. He may provide himself, also, with non-pattern lists, on which words have given lengths but contain no repeated letters; and with "transposal lists" containing pairs of words (as NIGHT and THING) which use the same letters but not in the same order. It is true that such lists are troublesome to prepare, but they are extremely effective; they will break the most resistant of the "aristocrats" or the shortest example of legitimate cipher.

No matter how resistant the cryptogram, all that is really needed is an *entry*, the identification of one word, or of three or four letters. The experienced solver knows well that persistence will find this entry, and trusts largely to instinct and perseverance; the beginner, however, may feel at a loss for a "system," and, if so, may, perhaps, be able to find suggestions for one in the next few paragraphs.

Figure 63

A Favorite Form of Frequency Count Combined With CONTACT Data

A	D S R W	2/4
B		
C		
D	F R M Z W W V T Z R R M S Y A F R F Y N	10/11
E		
F	* Y D D Y D Z V S R	5/6
G	X S	1/2
(Etc.)		

Concerning the numbers: A has a frequency of 2, and a variety-count of 4. D has a frequency of 10, and a variety-count of only 11. (Yet D, with so little variety of contact is a vowel!)

First of all, in any substitution problem, there should be a counting of the letters in the cryptogram in order to find out their frequencies. This is called a *frequency count*, and is usually accomplished as follows: The decryptor first lays out the normal alphabet — either horizontally or vertically. He then begins with the first letter of his cryptogram, taking letters one by one just as he finds them, and for each time that he finds a letter in his cryptogram, he places a tally mark beside that same letter as found in his prepared alphabet. The result of such a count, taken on the foregoing cryptogram, will be shown further on, when the same cryptogram appears again without its word-divisions.

If the problem seems likely to prove really difficult, there should also be a *contact count;* that is, a list showing every letter, together with the two which have flanked it right and left each time it was used. Such a count is partly shown in Fig. 63. This, like the frequency count, may be prepared either vertically or horizontally; and, just as in making ready for the frequency count, an alphabet may be laid out in advance ready to receive the contact letters, taken from the cryptogram as they happen to be found. Specifically: The letter *F* comes first in the cryptogram; it has no left-hand contact, but is contacted on the right by *D*. We find the *F* of the prepared alphabet, and place beside it its contacts: *-*D*. The second letter of the cryptogram is *D*, flanked by *F* and *R*. We find the *D* of the prepared alphabet, and place beside it its contacts: *F-R;* and so on to the end of the cryptogram. Some solvers do not prepare an alphabet in advance, but simply put down the main letters as they happen to come across them in the cryptogram. It should be added, too, that the few contacts included in Fig. 63 were taken from the *undivided* cryptogram. When word-divisions exist, and are known to be the correct ones, a great many solvers do not include any contacts which involve two different words. Here, for instance, the second appearance of *D* is shown with contacts *R-M*. These solvers, knowing that this *D* stands at the end of a word, will leave the *M*-contact blank: *R-**

It will be noticed from the figure that the contact-count is, in itself, a frequency

count; it shows that *A* has been used twice (frequency 2), that *B* and *C* have not been used at all, that *D* has a frequency of 10, and so on. We may also make it a *variety-count*, by noting down beside each letter the number of *different* letters present among its contacts. Ordinarily, the vowels have more variety in their contacts than do the consonants, and take part in more reversals. The uses of contact data will be examined more closely later on.

Now, giving our attention to English frequencies: No matter what frequency table we examine, we always find that the letter *E* tops the list, with a frequency of over 12%. Except in telegraphic text, the letter *T* always has the second frequency, near 10%. After that, the frequency tables will disagree as to whether *A* or *O* should have the third frequency, or whether *I* should come before *N*, or *S* before *R;* but always the same nine letters, *E T A O N I R S H*, will constitute the *high-frequency group* of letters. These particular letters will make up about 70% of any English text, and it is almost impossible to prepare one, no matter how short, without using them in about that proportion, though in the shorter texts, *L* and *D* will sometimes creep up into the high-frequency class, taking the place of *H*. Following the high-frequency group, we find a group of letters which are always of *moderate frequency;* and a third group made up of *low-frequency* letters. Since the frequency tables themselves are not duplicates throughout, we could not expect, even having a 10,000-letter cryptogram, to make substitutions by simply following the frequency table and be absolutely sure of coming out with the correct solution, though we might very nearly do so, and might, to some extent, succeed in doing this with a cryptogram of 2,000 letters. The "aristocrats," however, are arbitrarily confined to lengths which run between 75 and 100 letters. Even without manipulation, a text of this length will not always show *E* as a frequent letter, and may, for some reason, show *Z* or *X* with a fairly high frequency.

However, the "class distinctions" among the letters are always, to some extent, dependable. High-frequency letters, moderate-frequency letters, and low-frequency letters, all tend to be very exclusive. They will exchange frequencies with letters of their own class, but all three classes are disinclined to welcome outsiders. The vowels, also, as we have seen, have their fraternity; if the frequency of *E* is lowered, some other vowel, even *U* and *Y*, will insist upon making up the difference, rather than yield this privilege to a consonant.

The high-frequency group, as mentioned, includes the nine letters *E T A O N I R S H*. Even in this exclusive circle, there are cliques — not ironclad, but clearly noticeable:

Class I. The letters *T O S* appear frequently *both as initial letters and as final letters* in their own words, with terminal *O* confined largely to short words. All three of these are very freely doubled.

Class II. The letters *A I H* appear frequently as *initial letters,* but far less frequently as finals, especially *A I*. Not one of these is readily doubled.

Class III. The letters *E N R* appear frequently as *final letters,* but far less frequently as initials. The letter *E* is very freely doubled; the other two not so often.

The following further observation might be made: When one of these letters changes its class, the least likely exchange is one occurring between classes *II* and *III*.

Now let us return to the foregoing cryptogram and consider the application of this information. A frequency count taken on this cryptogram will show that when its letters are rearranged according to their frequencies, they divide automatically

into three rather clearly-defined groups, much like those of the normal frequency table. There are eight letters which outrank the rest, and these, named in the order of decreasing frequencies, are: *R, D, V, S, F, Z, K, X*. Presumably, then, most of these are substitutes for letters of the class *E T A O N I R S H*.

If an examination now be made of the terminal letters in the cryptogram, it will be found that, of the eight considered, the letters *R D F* have appeared at least once in both positions. These we may label class (a), as being good material for the originals *t, o, s*. It is found that the letters *S Z* have appeared at least once as initials, but not at all as finals. These we may label class (b), that is, good material for the originals *a, i, h*, except for a point which will be mentioned in a moment. The remaining three letters, *V K X* are found at least once as finals, but not at all as initials; these we will call class (c), good material for the originals *e, n, r*. Thus, we are enabled to begin our work by noting down the following possibilities:

(a) *R D F* might represent (*I*) — *T O S*. (Compare the facts: *t, o, n*).
(b) *S Z* might represent (*II*) — *A I H*. (Compare the facts: *a, c*).
(c) *V K X* might represent (*III*) — *E N R*. (Compare the facts: *e, h, l*).

While such a classification is probably never 100% accurate, the writer has still to find a cryptogram (unless among the very badly manipulated " aristocrats ") in which at least part of the assumptions are not correct. We are dealing, however, with the *very short cryptogram*, in which a single occurrence of a letter in a given position can be regarded as of some importance.

Ordinarily, the most frequent letter of (c) will represent *e*, as it does here. This letter is famous as a final letter, and any printed page will show it at the end of 17 or 18 words in every hundred. There is not so clear a distinction between *T* and *S* of class *I*.

The most vulnerable of the groups, however, is (b). Of the three letters which may be represented here, two are vowels, concerning which we are to hear more, and not one is readily doubled. When *Z*, tentatively included in this group, is found to have been doubled near the beginning of a word, it is seen to be wrongly classified.

This method, as mentioned, is intended merely as a suggested means for effecting an entry. The correct identification of only four letters, as we have seen, will make enormous inroads into the contents of a cryptogram.

Other points which will at times prove helpful are as follows: In words of three and five letters, the central one is nearly always a vowel, taking it for granted that the words *the* and *and* will never be present in any difficult cryptogram. In the longer words, the favorite positions of the vowels are the two positions which follow the initial letter and the two positions which precede the final letter. The favorite position of *I*, in fact, is well known as the third-to-last. About half the words used in any written text are of the type called *negative*, or *empty;* that is, the pronouns and auxiliary verbs, and particularly the various kinds of connectives *without which no sentence can be put together*. If your cryptogram is an " aristocrat," you will probably find that most of your prepositions begin with *A: amongst, amidst, adown*, etc. Every sentence contains a verb, and these are more or less limited in their possible terminations. Any letter used only two or three times, and always followed by the same letter, is good material for *Q*. With what has been said, the student should have no trouble in dealing with the first fifteen " aristocrats " which follow the next chapter. As to the remaining thirty-five of Mr. Lamb's collection, we need say only this: It is impossible to avoid every characteristic of the English language and still write English.

The General Case. — Now let us examine carefully Fig. 64, where the foregoing cryptogram is repeated without its word-separations, and is followed by its frequency and contact data. The various devices indicated in this figure are all of a more or less optional nature. Concerning the preparation of the cryptogram itself, the chief requirement is that it be done in ink, or typewritten, on paper which

Figure 64

```
5 10 11  3  3  2  1  9  4  4  2 11 10  1 10  6  4  9  6  2  1  3 11  4
F  D  R  J  N  U  H  V  X  X  U  R  D  M  D  S  K  V  S  O  P  J  R  K

5 10  3  5  5  3  4  1  6 11 11  9  3  1  3 11  3 10  2 11  3 10  5  9
Z  D  Y  F  Z  J  X  G  S  R  R  V  T  Q  Y  R  W  D  A  R  W  D  F  V

11  4  9 10 11  4  9  3 10  5  6  5  5 10  3  5 11 10  3  3  9  2  9  3
 R  K  V  D  R  K  V  T  D  F  S  Z  Z  D  Y  F  R  D  N  N  V  O  V  T

 6  4  6  2  3  9  5 11
 S  X  S  A  W  V  Z  R
```

Ordinary Frequency Count:

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

Contact-Information:

(High-frequency symbols)

R	D	V	S	F	Z	K	X
D.J	F.R	H.X	D.K	..D	K.D	S.V	V.X
U.D	R.M	K.S	V.O	Y.Z	F.J	R.Z	X.U
J.K	M.S	R.T	G.R	D.V	S.Z	R.V*	J.G
S.R	Z.Y*	F.R	F.Z	D.S	Z.D	R.V*	S.S
R.V	W.A	K.D	T.X	Y.R	V.R		
Y.W	W.F	K.T	X.A				
A.W	V.R	N.O					
V.K	T.F	O.T					
D.K	Z.Y*	W.Z					
F.D	R.N						
Z..							

(Low-frequency symbols)

G	H	M	P	Q
X.S	U.V	D.D	O.J	T.Y

(Moderate-frequency symbols)

J	N	T	W	Y	A	O	U
R.N	J.U	V.Q	R.D*	D.F*	D.R	S.P	N.H
P.R	D.N	V.D	R.D*	Q.R	S.W	V.V	X.R
Z.X	N.V	V.S	A.V	D.F*			

will suffer a great deal of erasure. The placing of its frequency figure above each letter is highly recommended, but not vital. Many solvers will underscore all possible repeated sequences, and will indicate in some other manner all reversals of digrams; others will underscore only the repeated trigrams and longer sequences; and still others do not underscore at all, being content to have all of these repetitions and reversals listed before them in the contact data.

As to the preparation of the contact data, most of the expert decryptors seem to prefer the vertical arrangement of Fig. 63 to the one shown here. But, in simple substitution, a full listing, made for all letters, is not necessary in dealing with the average cryptogram. Usually, it will serve the purpose to make a frequency count

first, and then prepare a listing of contacts which includes only chosen letters, those of very high frequency and those of very low frequency; with many cryptograms, no listing at all need be prepared. The contact data, however, are valuable. Each pair of contact-letters actually indicates a trigram. Examining, for instance, the listing under *R:* The first expression, *D.J.*, represents a trigram *DRJ* in which the central letter was omitted in order to conserve time and space. When we find, lower down in the same listing, another letter *D*, we see in this a repeated digram *DR*. Considering the right-hand side of the same listing: When we find *K* used three times, we see this as a digram *RK* used three times. *By finding its duplication, under K* (left side), we are able to see that two of these repetitions are continued as parts of a repeated trigram *RKV*. In the list of contacts for *D*, we find a repeated trigram *ZDY*, which may be traced, under *Y*, as part of a longer repeated sequence, *ZDYF*. It is usually best to underscore these longer repeated sequences on the cryptogram; often, they can be identified from the list of frequent trigrams. But repeated digrams, as a rule, are so numerous as to be in the way when noted on the cryptogram itself. With digrams, only those which are repeated oftenest need be underscored; they can nearly always be identified direct from the list of frequent digrams. The solver, then, prepares his cryptogram and sequence data to suit himself, varying his method according to the difficulty of the given example. With this done, his usual method of solution follows the process popularly known as "vowel-spotting."

The Vowel-Solution Method. — Using this process, the first step is that of separating the vowels from the consonants; the second is that of assigning identities to the selected vowels, and afterward to the most recognizable of the consonants.

For assistance in applying this method, suppose we extract certain information from the digram chart and have this concretely before us in a series of numbered "pointers":

1. The vowels *A E I O* are normally found in the high-frequency section of the frequency count; the vowel *U* in the section of moderate frequencies, and the vowel *Y* in the low-frequency section.
2. Letters contacting low-frequency letters are usually vowels.
3. Letters showing a wide variety in their contact-letters are usually vowels.
4. In repeated digrams, one letter is usually a vowel.
5. In reversed digrams, one letter is usually a vowel.
6. Doubled consonants are usually flanked by vowels, and vice versa.
7. It is unusual to find more than five consonants in succession.
8. Vowels do not often contact one another. If the letter of highest frequency can be assumed as *E*, any other high-frequency letter which never touches *E* at all is practically sure to be another vowel, and one which contacts it very often cannot be a vowel. (This will apply equally to other vowels, wrongly assumed as *E*.)

With a text of reasonable length, say 150 letters, it is sometimes possible to determine with certainty just which of the cryptogram-letters represent the six vowels; with shorter cryptograms, we can usually find four; sometimes only three. But once the separation has been made, individual vowels can usually be established as follows:

The most frequent one is ordinarily *E*. The one which never touches it is most likely to be *O*. Both of these are very freely doubled, and for that reason are often confused with each other, but seldom with any other vowel. They rarely touch each other.

The vowel which follows *E* and almost never precedes it, is *A*.

The vowel which reverses with it is *I*.

The same two observations will apply to the vowel *O;* but a distinction occurs when the vowel *U* can be found; this vowel precedes *E* and follows *O*.

The only vowel-vowel digrams of any real frequency are *OU, EA, IO.*

Three vowels found in succession may represent *IOU, EOU, UOU, EAU.*

As to identification of the consonants: Those letters still remaining in the high-frequency section of the frequency count will usually include *T N R S H*. Of these, the most easily identified is *H*, which precedes all vowels and seldom follows one; it may be identified often as part of repeated sequences *TH, HE, HA.*

Next to *H*, the most recognizable of the consonants, aside from frequency, is probably *R*, which reverses freely and indiscriminately with all vowels, and has a strong affinity for other high-frequency letters.

The consonant *T* can usually be identified by its frequency, by its tendency to precede vowels rather than follow them, and by its almost inevitable combination with *H* on more than one occasion. It is also notably difficult to distinguish from the vowels.

The letter *N* has characteristics which are to some extent the opposite of those mentioned for *H;* it prefers to follow vowels and precede consonants, and, to a lesser extent, the same is true of *S*, according to some charts. However, *N, S,* and *T* are all readily reversible with vowels, and are sometimes hard to tell apart.

The only frequent reversals of two consonants are *ST-TS* and *RT-TR.*

The doubles *TT* and *SS* are among the most frequent in the language.

Having this information, together with what we know of frequent digrams and frequent trigrams and very common short words, we are well armed against the longer cryptograms. Those which are shorter will give more trouble; but it takes a very short cryptogram indeed to be really resistant.

Our foregoing cryptogram contains only 80 letters.

Figure 65

(Cryptogram Frequencies:)

R	D	V		S	F	Z	K	X
11	10	9		6	5	5	4	4
E	T			A	O	N	I	R	S	H

(Normal Grouping)

To apply "pointers" in this case, let us begin by considering the individual frequencies of the letters *E T A O N I R S H*. Their frequencies per 100, according to our own chart, are about as follows: *E*, 12; *T*, 10; *A*, 8; *O*, 8; *N*, 7; *I*, 7; *R*, 6; *S*, 7; *H*, 5. Thus, when frequency alone is considered, *E* and *T* have a tendency to draw away from the others and form a private high-frequency group of their own. The distinction among the others is not so clear, and not always the same in all tables; we can only say of these that *A* and *O* will always outrank the rest, and will be closely followed by one of the others, usually *N*, and that *H* will always rank last.

Thus, the high-frequency group itself tends to sub-divide more or less clearly into three minor groupings: *E T — A O N — I R S H*. Of these, the first minor group shows one vowel, the second shows two, and the third shows one; the vowels *U* and *Y* are not present.

Now if the eight leading letters of our cryptogram, already listed as *R D V S F Z K X*, be examined in this respect, it is found that these, also, have a tendency toward separation into groups of differing frequency, which more or less correspond to the normal groupings, as indicated roughly in Fig. 65.

Normally, we expect the highest of these subdivisions to contain one vowel and one consonant, specifically *E* and *T*. When we find that the corresponding subdivision of the cryptogram contains three letters, the supposition is that one of the vowels, *O* or *A*, has moved up into this section; in that case, it has taken part of the frequency of *E*, making it not at all unlikely that the most frequent letter of the cryptogram will not represent *E*, and will not, in fact, represent a vowel. And if, as we believe, there are two vowels in the highest section, then we are not likely to find more than one in the central subdivision, especially when we note that it contains only three letters. This would leave the fourth vowel to be found in the third subdivision.

Thus, we have applied pointer No. 1. For the application of pointer No. 2, we turn to the contact data. Comparing first the three letters *R D V*, and making a careful inspection of all cryptogram letters whose frequency is 3 or lower, we find that, of our three letters, the letter *R* has 7 contacts with low-frequency letters, the letter *D* has 9, and the letter *V* has 8. Thus, the letter *R*, though having a higher frequency than the other two, has fewer low-frequency contacts than either, and so begins to draw away and assume the aspect of a consonant.

The application of pointers Nos. 3, 4, and 5, provides no satisfactory distinction. But in pointer No. 8, we find a very clear distinction: *D* and *V* have touched each other only once, while *R* has contacted both with a total of six contacts — a great many for a cryptogram of this length.

We decide, then, that *R* is a consonant, and that *D* and *V* are vowels.

Considering the central subdivision, where we expect to find one vowel: Application of pointer No. 2 shows that *S* has four of the low-frequency contacts, while *F* has two and *Z* has only one. Further examination of *S* by pointer No. 3 shows that it has an unusual variety in its contact-letters. Thus, *S* would appear to be the vowel here.

As to the third section, there is so little difference in frequency between these letters and some others not included in the high-frequency class, that any distinction found would not be convincing.

The individual cryptogram, however, has happened to contain the sequences *VXXU, SRRV, SZZD, DNNV*. Application of pointer No. 6 confirms our previous selection of *D, V, S*, as vowels, and suggests that the letter *U* might also represent a vowel. Since the frequency of this letter is only 2, we cannot feel so confident in drawing conclusions about it; however, a glance at the contact data shows that it has touched four different letters, which is 100% variety, that one of these four letters is an accepted consonant, and that none of the other three, so far, is an accepted vowel (pointers 3 and 8). The chances are that this letter *U*, with its low frequency, represents *y* in some such formation as *ally, ully, etty*, etc.

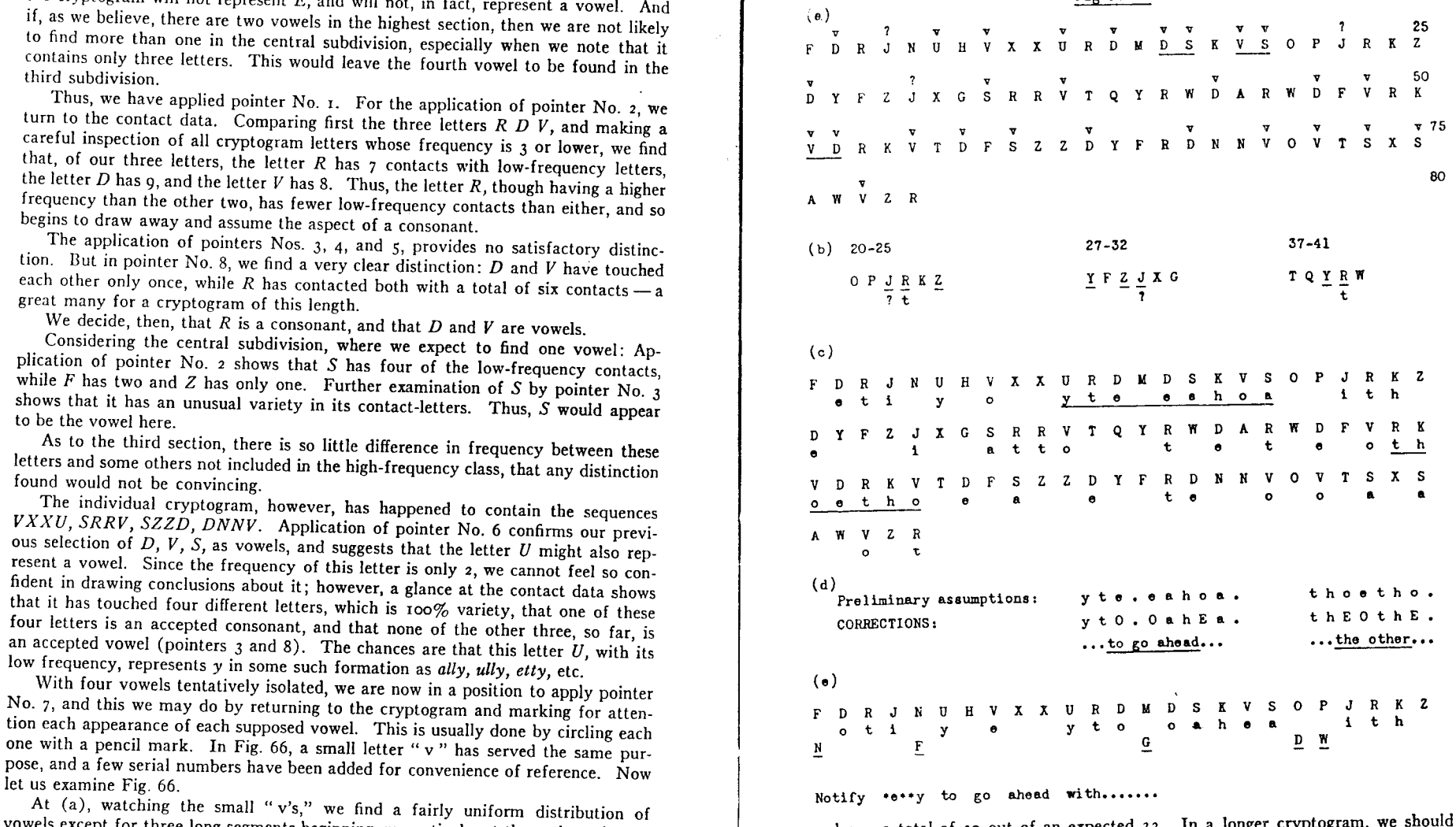
With four vowels tentatively isolated, we are now in a position to apply pointer No. 7, and this we may do by returning to the cryptogram and marking for attention each appearance of each supposed vowel. This is usually done by circling each one with a pencil mark. In Fig. 66, a small letter "v" has served the same purpose, and a few serial numbers have been added for convenience of reference. Now let us examine Fig. 66.

At (a), watching the small "v's," we find a fairly uniform distribution of vowels except for three long segments beginning, respectively, at the 20th, 27th, and 37th letters. For convenience, these have been copied out at (b). The two of these which are longer, and therefore most likely to contain at least one of the missing vowels, are both found to have included *Z* and *J*. Of these two letters, *Z* is one which was previously discarded (from the central section of the high-frequency group) during our preliminary investigation. Examining it again, to make sure, we find it now as a double between two supposed vowels, and having two additional

contacts with supposed vowels (pointers 6 and 8). But *J*, we find, has never contacted any supposed vowel; it reverses with a supposed consonant, and shows as much variety as could be expected of a letter appearing only three times.

The acceptance of *J* provides five of the vowels, with frequencies of 10, 9, 6, 2, and 3 — a total of 30 out of an expected 32. In a longer cryptogram, we should probably look for the sixth vowel among those letters having approximately the correct frequency for making up the expected 40%. As to the present case, we should have no trouble selecting it from the five-letter segment at (b); but this would cause us to spot also the short word in which it is used, and our immediate concern is that of spotting vowels only through their known characteristics as vowels. We will assume, then, that the last vowel cannot be found.

Figure 66



The next step demands that we assign to the most frequent of the supposed vowels the value *e*, which happens to be a wrong assumption. Concerning this, it may be well to repeat here something which has already been said: In dealing with the simplest of cryptograms, there is often a short detour into trial and error. Also, the average decryptor, accustomed to the work, and fully aware of what he may expect from only 80 letters of text, will usually pause at this point and make some further observations before filling in any of his substitutions. However, there is value even in the making of wrong substitutions; the actual placing of supposed plaintext values in their supposed positions puts the plaintext possibilities before us *in visual form*, causing us to note easily those very points for which the experienced decryptor examines in advance.

Figure 67

1. F D R J N U H V X X U R D M D S K V S O P J R K Z D Y F Z J
X G S R R V T Q Y R W D A R W D F V R K V D R K V T D F S Z
Z D Y F R D N N V O V T S X S A W V Z R.
(80 letters).

2. H V X X U T V W D T R A Z D Y F Z J X T V S O U R D S Z R N
S E D T S Q X U L K S E V O T D W W V O D R K V T G S R R V
T Q Y R A Y M M V A R P V A K D Y X O H V V W K S G G V T J
F M S R R K J A R K T D Y M K T J Z K S T O A L R K J F H R
K V U G S U M T S F R R K V A Y Q A J O U R K S R U D Y A W
D H V D N.
(155 letters. - Total for both cryptograms: 235).

At (c), then, we have made our substitutions. We have assumed that the most frequent vowel, *D*, is representing *e*. Having noted the v-v digrams *DS*, *VD*, *VS*, we have selected *S*, rather than *V*, as the substitute for *a*, preferring a digram *oa* (*DS*) to a digram *ao* (*VD*). This leaves the vowel of second frequency, *V*, to represent *o*. This will cause the third of the v-v digrams (*VS*) to represent *oe*, not frequent, but better than the digram *ao* previously mentioned. *J*, then, probably represents *i*, and *U* may represent *y*.

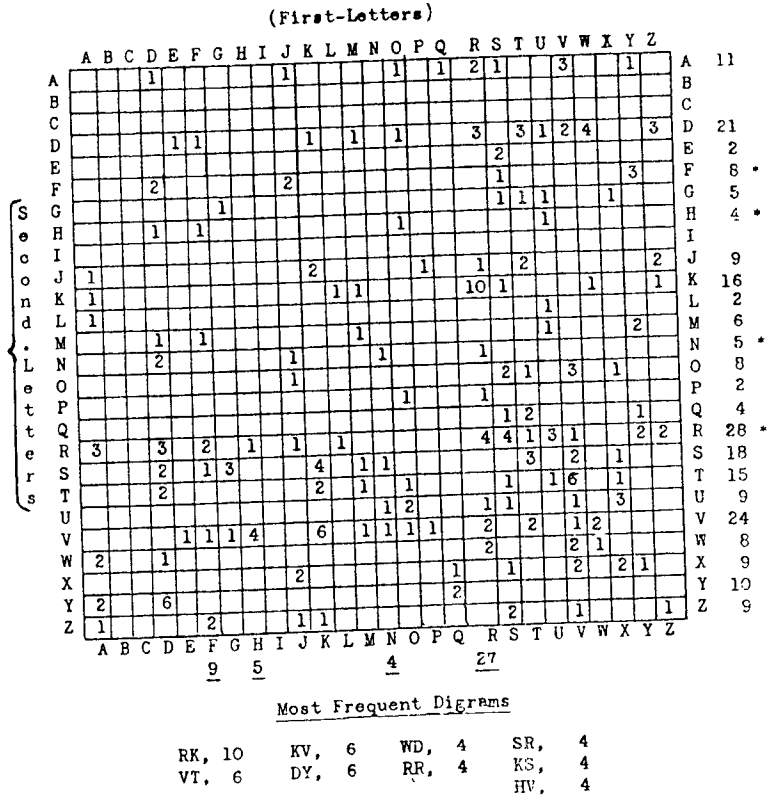
As to consonants, we have assigned the value *t* to the most frequent one, *R*, and there has been no difficulty in identifying *h* in the letter *K*, which three times has followed *R*. But our present cryptogram is too short to provide any clear distinction among letters which might represent *n*, *r*, *s*. With the seven substitutions made, as shown at (c), notice how quickly it becomes possible to spot the incongruity of sequences *tho*, more than once, in a short text which contains not a single occurrence of *he* or *ha*. Notice again, at (d), how quickly the mere exchanging of the values *e* and *o* will bring out word-suggestions.

At (e), the first line of the cryptogram is repeated, as it would appear after the making of this exchange. The beginning of the message can almost be read: The first word appears to be ***notify***, furnishing two new substitutes. Three more can be furnished in the suggested sequence *to go ahead with*. And here, the word ***with*** would be tried in any case, because it is a common word, and because the frequency

of the letter *P* is suggestive of *w*. Arrived at this point, we begin to notice patterns: *postpone, council, account, matter*, and so on; so that the rest of the solution is largely a matter of filling in framework. In the given example, it would also be noticed that *F* and *N* have resulted from reciprocal encipherment; this may not be the case with other letters, but it presents a possibility which is always well-worth investigating.

Figure 68

Digram Count for the Longer Cryptograms



Most Frequent Digrams

RK, 10	KV, 6	WD, 4	SR, 4
VT, 6	DY, 6	RR, 4	KS, 4
			HV, 4

The Digram-Solution Method. — This method, representing another of our many debts to M. E. Ohaver, may be used either in conjunction with the vowel method, or independently, as the fundamental method of attack. For a satisfactory demonstration, however, we need more material, and Fig. 67 shows our cryptogram again, together with a suspected reply. Thus we have a length of 235 letters, so that the preparation of contact-notations, which we found sufficient in the preceding case, becomes here an irksome task.

For these longer cryptograms, it is usually best to put all of our data into the form of a *digram-count*, as indicated in Fig. 68. This is most easily done as follows: Using a sheet of cross-section paper, mark off the limits of a 26 x 26 square;

write the normal alphabet across the top, so that each of its letters will govern a column; and write it again along one side, so that each letter will govern a row. For added convenience, these two alphabets may be repeated, as they are shown in the figure. Now, remembering that each letter in the text is the first letter of a digram (except the two which are finals), our two texts, with their total of 235 letters, are to provide a count on 233 digrams. Taking letters one by one, just as they come in the cryptograms, find each letter in the upper alphabet; find, in the side alphabet, the letter which immediately follows it in the cryptogram, and count this digram by placing a tally-mark in the cell at which the column and row governed by these two letters are found to intersect. In the figure, the tally-marks have been replaced with numbers showing their totals. It will be noted that the process described is identically the method which would have been used by Meaker in preparing the digram chart; and, just as in the case of the digram chart, the counting of the digrams has automatically counted the single letters. To obtain their frequencies, we may total either the columns or the rows, taking the larger figure in those few discrepancies caused by initial or final letters. With the chart understood, the digram-method of solution can be shown in a nutshell.

An inspection of this chart enables us to find quickly that the leading digrams are those listed: *RK, VT, KV, DY,* etc. These, almost certainly, are the substitutes for digrams ranking high on the normal list, and many others, having a frequency of 3, are very likely indeed to be substitutes for digrams from that same high-frequency class. Our text, of course, is still short, even with 235 letters, and we do not invariably find, in texts of this length, that the ranking digram (in this case *RK,* frequency 10) is the substitute for *th,* though the chances are, at all times, that it is. And should it prove here that *RK* does not represent *th,* then we may be quite sure that *th* is represented in one of the digrams *VT, KV, DY,* having the next frequency, 6. With the single exception of *RR,* each digram of the nine which are listed below the chart can be checked against three other digrams: Its own reversal; the doubling of its first letter; and the doubling of its second letter. In addition, it may be checked through the individual frequencies of its two component letters. These points of comparison, made for each of the nine leading digrams, have been tabulated in Fig. 69, so that the discussion may be easily followed.

Examining *RK,* assumed to represent *th:* Its reversal, *KR,* has not appeared on the chart, which is satisfactory for a digram of no greater frequency than its supposed original, *ht.* The doubling of its first letter, *RR,* has appeared four times, which is satisfactory for *tt,* one of the leading doubles of our language. The doubling of its second letter, *KK,* has not appeared, which is eminently satisfactory for a digram as rare as *hh.* Its first letter, *R,* has a frequency of 28, the highest in the cryptogram, which is not at all unusual in the case of *t;* and its second letter, *K,* has a frequency of 16, a little high for *h,* but not unsatisfactory. Thus, we find nothing, so far, to contradict the supposition that the digram *RK* is the substitute for *th.* But if *K* represents *h,* it should be possible to find digrams beginning with *K* which will check equally well as the substitutes for *he* and *ha.* We do, in fact, find *KV* and *KS.* But which is which? Examination of Fig. 69 shows that one of these, *KS,* has a reversal, *SK,* frequency 1; but this is not informative, since it would be equally expected of *eh* or *ah.* Further examination shows that *V* has been doubled, which is far more characteristic of *e* than of *a.* Also, the individual frequency of *V,* 24, is the second highest in the cryptogram, and more likely to be that of *e* than that of *a.* Thus we may assume that *KV* represents *he* and that *KS* represents *ha.* This automatically identifies the digram *SR* as *at.* As to *VT,* this, apparently, involves the only reversal of any prominence in the cryptogram. Its first letter has already been identified as *e,* and the outstanding reversal of the language is *er-re.* This is not so certain as in the preceding cases, but the frequency of *T* is satisfactory as that of *r.*

Thus we have identified the letters *t, h, e, a, r,* which is as far as the tabulation has been carried. Having the substitute for *h,* we may now bring in the vowel-solution method through examination of digrams *KD, KJ, KT, KZ;* or continue with the digram-solution method by looking over the field for some of the other *h*-digrams: *sh, ch, wh, ph, gh,* and so on. The first of these should be easily identified by the frequency of *s,* and, in addition to the regular three check-digrams, we might check this against a possible *st,* another of our leading English digrams. With the process explained, we need not go further; the substitution of letters *t, h, e, a, r, s,* will surely break any simple substitution cryptogram. Possibly, enough has not been said as to the use of the trigram list, the consideration of common affixes, common short words, and so on; but these are all points which the student can best develop for himself.

Figure 69

Digram		Doubled Letter		Letter Frequency		Supposed
Original	Reversed	1st	2d	1st	2d	Identity
R K 10	K R...	R R 4	K K...	R 28	K 16	t h
V T 6	T V 2	V V 1	T T...	V 24	T 15	e r
K V 6	V K...	K K...	V V 1	K 16	V 24	h e
D Y 6	Y D...	D D...	Y Y...	D 21	Y 10	?
W D 4	D W 1	W W 1	D D...	W 8	D 21	?
S R 4	R S...	S S...	R R 4	S 18	R 28	a t
K S 4	S K 1	K K...	S S...	K 16	S 18	h a
R R 4	....	....	....	R 28		t t
H V 4	V H...	H H...	V V 1	H 5	V 24	? (-e)

Another point, however, must not be overlooked: *the long repeated sequences HVXXU, ZDVFZJX, DRKVT, GSRRVT.* Repeated sequences of these lengths will usually come from *repeated whole words,* making it possible, to some extent, to attack the cryptogram by word-division methods. It is, in fact, the repetition of sequences, these and many others, which, in the beginning, has led us to assume that both cryptograms are using the same key. As to the recovery of this key, we need not wait until solution is complete. Even in simple substitution, it is well, during the identification of substitutes, to have before us a sort of skeleton key, in which the plaintext alphabet has been written out in normal order, so that the substitutes, as fast as their identities are discovered, can be placed below their originals.

Thus, having identified as many as twelve letters in our present cryptogram, this skeleton key, or framework, might begin to assume the appearance which is indicated in the upper tabulation of Fig. 70. Here, we are able to note a reciprocal encipherment between *A* and *S, F* and *N, R* and *T,* and *U* and *V,* suggesting that the whole encipherment may have been reciprocal; if so, we have the identities of four additional substitutes: *O, I, H, E,* representing *d, j, k, v,* respectively. If they are present in the cryptogram, these four substitutions may be tried; but with or without their presence in the cryptogram, they can be added to the skeleton key, as in the lower tabulation of the figure. Notice that when this has been done, the cipher alphabet is beginning to show alphabetical sequences (reversed). We find *H I J K,* and, just before this, *D F,* which is an alphabetical sequence if the letter *E* has been taken out for use in a key-word. Between *DF* and *HIJK* of the cipher alphabet, we need only *G* to fill out the sequence; therefore either *l* or *m* must belong to the key-word; comparing this with what is found at the other end of the sequence, we find that either *L* or *M* would be the substitute for *g.* Between *NO,* we find *V,* evi-

Figure 70

Supposing 12 substitutes to have been identified:

```
Plaintext alphabet:  a b c d e f g h i j k l m n o p q r s t u v w x y z
CIPHER ALPHABET:     S     V N   K J       F D     T A R Y       U
```

Assuming reciprocal substitution:

```
Plaintext alphabet:  a b c d e f g h i j k l m n o p q r s t u v w x y z
CIPHER ALPHABET:     S     O V N   K J I H     F D     T A R Y E     U
                     Q?P? *   L?          G?        C?B?*       *     T?
                              M?
```

dently misplaced; and, following *O* and preceding *S*, we find two positions which may be occupied by two of the letters *PQR*, of which *R* has already been placed (under *t*). That is, where the encipherer has used a key-word-mixed alphabet without troubling to carry it through a transposition process of any kind, we are often able to build it up again, and make it help us in the solution. This is especially true if he has used reciprocal encipherment; with the substitutes which may actually be found in our foregoing cryptograms, a little rearrangement is all that is needed in order to discover exactly what the original key was. When the cipher alphabet has been carried through a transposition block, it is not so easy to recover during the actual process of solution; afterward, however, it is not usually difficult to treat it by one of the transposition processes, just as if it were a transposition cryptogram of 26 letters. In the examples which follow, the key-word-mixed alphabets were used as they stood, though we believe that none of the encipherment was reciprocal. In one case, however, the plaintext and cipher alphabets were both mixed, according to different key-words, so that the recovery of this key may prove troublesome.

45. By PICCOLA.

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

46. By PICCOLA. (Plaintext and Cipher Alphabets have each a key-word).

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

47. By PALOMITA. (No key-word).

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

48. By PICCOLA. (Of these two, one has normal word divisions; the other has not).

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

49. By PICCOLA.

P B K L A B E I C D J D B I L Y P K L D O I X L Y I P K V Y A L ?
A G F Y A M I L K L Y I K I D C A G G L D O I X-V D J R K L Y I C P B R P B N
X D Q A J I ? Q K J I S P B R K L Y A L A B R M X Q F P L F P E O L D
I B R V Y P E Y O B D V X D Q P C E G I A J F I J C I E L G X P K
S I A B P B N P L K. A J P K L D E J A L A B B D L P K L Y P K B D !