Synoptic Tables for the Solution of Ciphers

and

A Bibliography of Cipher Literature

Publication No. 18

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918
Synoptic Tables for the Solution of Ciphers

and

A Bibliography of Cipher Literature

by

William F. Friedman

Publication No. 18

RIVERBANK LABORATORIES
DEPARTMENT OF CIPHERS
RIVERBANK
GENEVA, ILL.
1918
Two Hundred copies of this publication were printed of which this is

No. 122

Copyright, 1918
GEORGE FABYAN
FOREWORD

The tables presented herewith are designed to meet specific pedagogical needs of a course of instruction in modern ciphers. They are not intended, it is frankly admitted, to serve as a guide for the expert in his attempt to analyze complex ciphers such as may be intercepted today.

The method which has been followed in their construction is analogous with that followed in chemical analysis manuals, but only in its broader aspects. The basis for the chemical determination of the nature of an unknown substance consists in the ability to place the unknown successively into one of two alternative classes by means of a series of definite tests until with the last cleavage the solution is reached. It is entirely possible to accomplish this determination with directness and with accuracy in chemical analysis because the laws underlying chemical reactions are definite and unchanging. The tests to be applied are exact, the reagents are all thoroughly understood. It is possible to determine the nature of even the most minute traces of an unknown substance, so refined have the methods of chemical analysis become. Contrast this situation with that which confronts the cipher analyst at the outset of his attempts to solve an unknown. In the first place, except in rare instances in practice, the amount of the unknown is often so limited as to thwart all his attempts at analysis and nothing can be done. In the second place, while it is true that both an unknown chemical substance and a message are composed of definite combinations of discrete units, the former of atoms, the latter of letters, further analogy between them ceases. For while atoms combine in a limited number of ways and positions to form molecules, and the latter combine in a limited number of ways and positions to form more complex substances, letters combine in a limitless number of ways and positions to form words, and words combine in a limitless number of ways and positions to form sentences. True, this difference is only one of degree, not of kind, but whereas the science of chemistry has reached so high a degree of development that each one of the possible combinations may be recognized by at least one test, the science and art of deciphering has not reached such a high level of perfection. In the field of complex ciphers, there is at present no definite means of determining what tests or what methods of solution should be applied because there is no way of determining from external characteristics or even from certain internal signs which one of a great number of complicated and readily modifiable systems of enciphering has been used in the particular message under examination. In fact, in most cases, unless the decipherer is able to secure some information concerning the system used he has no way of knowing what methods to apply until the long and laborious process of elimination has disclosed them.
The analogy between the tables for chemical and for cipher analysis is, therefore, only remote, and it is doubtful whether it can ever be brought closer. But for the purposes for which the tables presented are specifically intended, namely, instruction, it is believed that they will constitute a valuable adjunct to the curriculum of a course in ciphers. It is believed that they will afford the student a means of surveying the most important branches of practical ciphers and to note their similarities and differences. Thus, taken as a whole, they will give a more or less comprehensive bird’s-eye view of the entire field of ciphers. If they will thus enable the student to secure a firmer grasp upon the basic principles underlying this branch of knowledge they will have served the purpose for which they were intended.

The Riverbank Publications referred to in the tables are as follows:

No. 15—A Method of Reconstructing the Primary Alphabet given a Single One of the Series of Secondary Alphabets. 1917.

No. 16—Methods for the Solution of Running-Key Ciphers. 1918.

No. 17—An Introduction to Methods for the Solution of Ciphers. 1918.

No. 19—Formulae for the Solution of Geometrical Transposition Ciphers.* 1918.

No. 20—Several Machine Ciphers and Methods for their Solution.* 1918.

No. 21—Methods for the Reconstruction of Primary Alphabets, Arbitrarily-Mixed Alphabets, Numerical Keys, etc.*

The full titles of works, which in the tables are referred to by only the author’s name, will be found in the Bibliography, Part II, pages 14-16.

*Now in press.
**TABLE I**

Examine the cipher carefully in order to secure from extraneous circumstances such information as may be of value in the subsequent analysis. Certain clues may be found as to language, subject, correspondents, etc.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1a. Cipher consists exclusively of letters.</td>
<td>1b. Cipher does not consist exclusively of letters.</td>
</tr>
<tr>
<td>2a. Cipher contains all or nearly all the different letters of the alphabet.</td>
<td>2b. Cipher contains only a limited number of different letters of the alphabet, five to ten.</td>
</tr>
<tr>
<td>3a. Cipher groups do not form pronounceable combinations, except a very few, which are evidently the results of chance.</td>
<td>3b. Cipher groups all form pronounceable combinations, evidently the result of a definite system for their production. (Pseudo-Code.)</td>
</tr>
<tr>
<td>4a. Vowel and consonant count show cipher to be a form of TRANPOSITION.</td>
<td>4b. Vowel and consonant count show cipher to be a form of SUBSTITUTION.</td>
</tr>
<tr>
<td>5a. Cipher consists of symbols, or signs, or of combinations of these with letters and numbers. Usually of amateurish origin; constitutes a simple Single Mixed Alphabet Cipher. Make a frequency table and proceed as in Table III, 2b. Sometimes the substitution of arbitrary letters consistently applied will be useful.</td>
<td>5b. Cipher consists of numerals chiefly, with a limited number of letters or signs, suggesting sliding alphabets of more than 26 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NUMBER CIPHER.**

Table VIII.

**ROUTE CIPHER.**

Table IX, 2.
1. SUBSTITUTION CIPHER

Set a few groups on the Poly-Alphabet or apply the "running-down" process.

2a. Cipher solvable on the Poly-Alphabet, in the case of a single Straight Alphabet, or in the case of a series of Straight Alphabets wherein the words reappear on different lines.
Table III, 2a.

2b. Cipher not solvable on the Poly-Alphabet.
Apply the process of factoring the intervals separating recurring polygraphs, trigraphs, and digraphs.

3a. Factoring discloses no repeatedly recurring factors.

4a. Substitution equi-literal, i.e., the total number of cipher letters is equal to the total number of plain-text letters.

4b. Substitution not equi-literal, i.e., total number of cipher letters greater than total number plain-text letters, usually a multiple of the latter.
Table VII.

5a. Substitution monographic, i.e., letter for letter substitution, each one enciphered independently.

5b. Substitution not monographic.

6a. Frequency Table shows "crests and troughs."
SINGLE ALPHABET (MONO-ALPHABET) SYSTEM, Table III.

6b. Frequency Table shows no marked "crests and troughs" but is "solid."
NON-PERIODIC MULTIPLE ALPHABET (POLY-ALPHABET) SYSTEM, Table IV, 2b.

7a. PLAYFAIR SYSTEM
7b. Substitution by means of a rectangle.

7c. Substitution Trigraphic.
7d. Substitution Polygraphic.

8a. ORIGINAL PLAYFAIR SYSTEM
8b. MODIFIED PLAYFAIR SYSTEM
Solve by Mauborgne or Moorman method.
Solve by combination of Mauborgne and Moorman method.*

TABLE III

[From Table II, 2a and 6a; VII, 5a]

1. SINGLE ALPHABET (MONO-ALPHABET) SYSTEM

(Frequency table shows "crests and troughs")

2a. STRAIGHT ALPHABET CIPHER

(This should have been solved under Table II, 2a.)

2b. MIXED ALPHABET CIPHER

[Also from Table I, 4c; VII, 2a; VIII, 5a; VIII, 5d]

3a. DIRECT ALPHABET

4a. Solve by the Frequency Table Method, i.e., "fitting the frequency table to the normal" to find A. Substitute the plain-text values in sequence.

4b. Solve by means of a Poly-Alphabet or by applying the "running down" process.

3b. REVERSED ALPHABET

4c. Solve by the Frequency Table Method, same as in 4a of this table.

4d. Find the Reversed Alphabet equivalents for three or four groups and proceed as in 4b of this table. Find the key letter and apply to the entire message.

Make a frequency table with prefixes and suffixes and assume values based upon the frequency of individual letters, digraphs, and trigraphs.


In case of a Reciprocal Alphabet, assignment of values is aided by the reciprocal relation. If the deciphering alphabet when completed exhibits signs of its being a Secondary Alphabet, based upon a Primary Alphabet using a key word, reconstruct the Primary Alphabet; or if the deciphering alphabet when completed exhibits signs of its being derived from a generating rectangle, reconstruct the latter. Sometimes these operations, when attempted upon the basis of partially deciphered material, will result in the complete reconstruction of the alphabet and the consequent entire decipherment. See Riverbank Publications Nos. 15, 16, and 21.
### TABLE IV

(Pages 10-13)

#### 1. MULTIPLE ALPHABET SYSTEM

| 2a. The individual alphabets of the entire system are employed at regular and definite intervals, resulting in either a PERIODIC SYSTEM or a PROGRESSIVE SYSTEM. |
| 2b. The individual alphabets of the entire system are not employed at regular and definite intervals, and do not result in either a Periodic System or a Progressive System. |

| 3a. The individual alphabets are limited in number in any single message, and are employed at definite intervals, thus forming the constituent cycles of a PERIODIC SYSTEM. |
| 3b. The individual alphabets are not limited in number in any single message, all of them being used in straight succession, thus forming the constituent cycles of a PROGRESSIVE SYSTEM. |

#### 4a. STRAIGHT ALPHABETS

Solve by means of the Poly-Alphabet (in the case of Reversed Alphabets first find the Reversed Alphabet equivalents before setting), reading diagonally up or down, or setting the successive cipher letters 1, 2, 3 . . . spaces above or below each other and then reading horizontally. Sometimes one alphabet may be broken into sections which are then rearranged, as in the Psalmist Disk, described by Giolli, pp. 58-62. See Riverbank Publications No. 20.

#### 4b. MIXED ALPHABETS

Break up the message into its constituent cycles and apply the frequency method to them. Attempt reconstruction of the Primary Alphabets. In case one of the alphabets is a Straight Alphabet, the reconstruction process is rendered relatively simple. See Riverbank Publications Nos. 20 and 21.

#### 5a. DIRECT

Solve on the ordinary Poly-Alphabet by applying the "running down" process according to the direct Alphabet sequence.

#### 5b. REVERSED

Find the Direct Alphabet equivalents and proceed as in 5a of this table.

#### 5c. KEYWORD

Assume probable words and attempt to localize them in the message on the basis of repeated letters. In case of 5c, attempt reconstruction of the Key-word Alphabet. When the successive words are encrypted on random generatrices of a Poly-Alphabet which is made up of Keyword, Arbitrarily-Mixed, or Random-Mixed Alphabets, solution of a single message, or even of a series of messages, is a very difficult achievement.
### TABLE V

1. MULTIPLE ALPHABET SYSTEM—Continued

(Periodicity governed by the successive single letters of the plain text.)

<table>
<thead>
<tr>
<th>2a.</th>
<th>The several alphabets are inter-related and constitute a PRIMARY ALPHABET SYSTEM.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Two or more basic alphabets (Primary Alphabets), which when sliding against each other, result in the production of a series of twenty-five or twenty-six subalphabets (Secondary Alphabets) which are inter-related.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2b.</th>
<th>The several alphabets are not inter-related and do not constitute a Primary Alphabet System.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The alphabets are all independent and are made separately. They may be Key-word Alphabets, Arbitrarily-Mixed Alphabets, or Random-Mixed Alphabets.</td>
</tr>
<tr>
<td></td>
<td>Each alphabet must be solved independently by the Frequency Table method.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3a.</th>
<th>PRIMARY ALPHABET SYSTEM OF TWO COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4a.</td>
<td>COMPONENTS IDENTICAL</td>
</tr>
<tr>
<td>4b.</td>
<td>COMPONENTS NOT IDENTICAL</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>5a.</td>
<td>BOTH COMPONENTS STRAIGHT ALPHABETS</td>
</tr>
<tr>
<td>5b.</td>
<td>BOTH COMPONENTS MIXED ALPHABETS</td>
</tr>
<tr>
<td>6a.</td>
<td>BOTH components proceed in the same direction, resulting in the production of a series of 25 Non-reciprocal Secondary Alphabets, all Direct Alphabets. The single frequency tables can be fitted to the normal. Find A in each alphabet and substitute the normal Direct Alphabet sequence in each of the cipher alphabets. See Hitt, pp. 65-62. For the solution of very short messages see page 41 of Riverbank Publication No. 16. This case applies to the original Vigenère System, and to the first Beaufort Method of using the same table.</td>
</tr>
<tr>
<td>6b.</td>
<td>The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Reversed Alphabets. See Hitt, pp. 84-85. This case results from the second Beaufort Method of using a Vigenère Table, or from the use of the U. S. Army Deal, or from the sliding of a Direct Alphabet against a Reversed. Proceed as in 6a except applying the Reversed Alphabet sequence. See Riverbank Publication No. 16.</td>
</tr>
<tr>
<td>6c.</td>
<td>BOTH COMPONENTS KEY-WORD ALPHABETS</td>
</tr>
<tr>
<td>6d.</td>
<td>BOTH COMPONENTS ARBITRARILY OR RANDOM-MIXED ALPHABETS.</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>7a.</td>
<td>Both components proceed in the same direction, resulting in a series of 25 Non-reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.</td>
</tr>
<tr>
<td>7b.</td>
<td>The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.</td>
</tr>
<tr>
<td></td>
<td>Solve each alphabet on the basis of single mixed alphabets. In the case of Key-word Alphabets the assumption of a few values in each alphabet may result in a partial reconstruction of the Primary Alphabet and a consequent more rapid decipherment. For a method see Riverbank Publication Nos. 15, 16, and 21.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8a.</th>
<th>PRIMARY ALPHABET SYSTEM OF MORE THAN TWO COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8b.</td>
<td>Pages 7-8.</td>
</tr>
</tbody>
</table>
TABLE VI
[From Table V, 49]

1. MULTIPLE ALPHABET SYSTEM—Continued

2. Primary Alphabet System of two components which are not identical.

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3a.</td>
<td>One of the components is a Straight Alphabet.</td>
</tr>
<tr>
<td>3b.</td>
<td>Neither of the components is a Straight Alphabet, both Mixed Alphabets.</td>
</tr>
</tbody>
</table>

3. The Straight Alphabet component is a Mixed Alphabet.

4a. The Straight Alphabet component is a Direct Alphabet.

4b. The Straight Alphabet component is an Arbitrarily Mixed or a Random Mixed Alphabet. Proceed as in 5a except no assumptions of unbroken sequences in the mixed alphabet component can be made. See Hutt, pp. 63-71.

4c. Both components are Key-word Alphabets.

4d. Both components are Arbitrarily Mixed or Random Mixed Alphabets. Solve the individual alphabets on the basis of single Mixed Alphabets. Attempt reconstruction of the Primary Alphabets. See Riverbank Publication No. 21.

5a. The Mixed Alphabet component is a Key-word Alphabet. Assume values for several of the high frequency letters in each alphabet and attempt reconstruction of the Mixed Alphabet on the basis of symmetry of position, and also of unbroken sequences, such as BCD, FGH, JKL, etc. Partial reconstruction will proceed simultaneously with decipherment, each aiding the other. Keep watch for the key word applying to the message by noting the successive cipher equivalents of A. See Riverbank Publications Nos. 15 and 22.

5b. The Mixed Alphabet component is an Arbitrarily Mixed or a Random Mixed Alphabet. Proceed as in 5a except no assumptions of unbroken sequences in the mixed alphabet component can be made. See Hutt, pp. 63-71.

5c. The Mixed Alphabet component is a Reversed Alphabet. Proceed as in 4a except applying the Reversed Alphabet sequences to the Straight Alphabet component.
TABLE VII
[From Table II, 4b]

1. SUBSTITUTION NOT EQUILITERAL

Usually, if the number of plain-text letters is 2, the number of cipher letters is 2n, 3n, etc.

[Also from Table I, 23]

2a. The number of different letters in the cipher message limited, usually not more than ten.

Systems using alphabets consisting of the various combinations of 2, 3, 4 . . . elements. (See Myers, pp. 65-165.) The number of characters in each combination is determined by the number of elements in the system. The least number of combinations possible must approximate 26, one for each letter of the alphabet.

2b. The number of different letters in the cipher message approximates 26.

[Also from Table I, 33]

3a. Cipher groups all pronounceable. (Pseudo-code.)

4a. Regular arrangement of vowels and consonants, of the form CVVCVC or VVCVCV, groups all of the same length, either 5 or 10 letters.

4b. No regular arrangement or alternation of vowel and consonant.

Syllable ciphers (Built-up ciphers). Groups of irregular lengths usually. Substitution of letters or syllables for syllables of the plain text. Not often found and difficult to decipher in case of good systems. Solution by frequency of digraphs and trigraphs of the language.

5a. Regularity produced by the insertion of nulls. Compile a frequency table on the basis of every other letter and proceed as in Table III.

Example: GRANT

G A N T
C R E F
A L N S H P
I O T S U T
F W X Y Z

Example: Plain text- THE
Cipher-NNR GT

Solution: Make a frequency table of combinations, or assign arbitrary single letters to each different combination and then make a frequency table. Proceed as in Table III, 23. See Hitt, pages 83-85.

6a. Rectangle based upon Straight Alphabets only. Make a frequency table of pairs and attempt reconstruction of the rectangle.

6b. Rectangle not based upon Straight Alphabets.

Solution by frequency of pairs. Attempt reconstruction of table.

7a. Rectangle based upon a Key-word Alphabet.

7b. Rectangle based upon an Arbitrarily-Mixed or a Random-Mixed Alphabet.

Solution by frequency of pairs. Attempt reconstruction of table.
### TABLE VIII

[From Table I, 34]

#### 1. NUMBER CIPHER

(Mathematical Ciphers)

Divide up the message into pairs of numbers unless already in this form.

1. **NUMBER CIPHER**

2a. Interval between the lowest and the highest pair of numbers approximates 26.

3a. Cipher is solvable by means of the Poly-Alphabet (or by equivalent procedure) as below.

- **Apply the Normal Alphabet sequence to the numbers in sequence.**
- **Apply letter equivalents consistently or continue to deal with the pairs of numbers, and apply the process of factoring the intervals separating recurrences.**
- **Letters in sequence of Straight Alphabet, numbers straight. Make a frequency table and attempt to find arrangement of left hand numbers.** See Hitt, pp. 86-88.

3b. Cipher is not solvable by means of the Poly-Alphabet (or equivalent procedure).

- **Apply letter equivalents consistently or continue to deal with the pairs of numbers, and apply the process of factoring the intervals separating recurrences.**
- **Letters in sequence of Straight Alphabet, numbers straight. Make a frequency table and attempt to find arrangement of left hand numbers. See Hitt, pp. 86-88.**

3c. The several values for each plain-text letter are produced by means of a rectangular table.

- **Rectangle with sides 10x3, letters within.**

3d. The several values for each plain-text letter are given by a series of 4 Direct Alphabets, with letters and numbers in sequence.

4a. **DIRECT ALPHABET**

- Set two or three of the groups on the Poly-Alphabet or apply the "running down" process. Procedure and principles the same as in Table II, 2a.

4b. **REVERSED ALPHABET**

- Find the Reversed Alphabet Equivalents for two or three of the groups and proceed as in 4a, of this table.

4c. Factoring discloses no repeatedly recurring factors.

- **Compile a single frequency table.**

4d. Factoring discloses certain repeatedly recurring factors.

- **Periodic Multiple Alphabet System.**

- Proceed as in Table IV, 2a.


- Proceed as in Table III, 3d.

5b. Frequency table shows no marked "crests and troughs," but is "solid." Multiple Alphabet (Poly-Alphabet System).

- Proceed as in Table IV, 2b.

5c. Letters in Key-word Alphabet sequence.

- Attempt reconstruction of Key-word Alphabet from VVXYZ sequences.

5d. Letters in Random Mixed Alphabet sequence.

- Make frequency tables of sequences from 1 to 10, 11 to 20, etc.; match these, combine and proceed as if Single Mixed Alphabet, Table III, 29.

---

<table>
<thead>
<tr>
<th>Plain text:</th>
<th>H</th>
<th>H</th>
<th>H</th>
<th>B</th>
<th>M</th>
<th>Y</th>
<th>V</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values:</td>
<td>22 17 14</td>
<td>14</td>
<td>25</td>
<td>14</td>
<td>26</td>
<td>48</td>
<td>55</td>
<td>20</td>
</tr>
<tr>
<td>Key-letter values:</td>
<td>17 14 23 37 17 14 22 27 17 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cipher:</td>
<td>55 31 27</td>
<td>61</td>
<td>52</td>
<td>26</td>
<td>47</td>
<td>67</td>
<td>55</td>
<td>56</td>
</tr>
</tbody>
</table>
### TABLE IX

[From Table I, 4a]

**1. TRANSPOSITION CIPHER**

2. Including Route Ciphers, which are only a type of transposition ciphers wherein the words are treated as individual letters. Regard each word as a single letter or apply arbitrary letters or numbers to the words and proceed as below.

<table>
<thead>
<tr>
<th>3a. SIMPLE SYSTEM</th>
<th>3b. MORE COMPLEX SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>4a. Vertical writing.</td>
<td>4d. Transposition based upon geometrical designs.</td>
</tr>
<tr>
<td>4b. Reversed writing.</td>
<td>Factorizing process applied first to suggest possible rectangles.</td>
</tr>
<tr>
<td>4c. Rail fence cipher.</td>
<td>5c. Transposition based upon rearrangement of entire columns, or rows, or both.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>6a. COLUMNAR TRANSPOSITION</th>
<th>6b. LINEAR TRANSPOSITION</th>
<th>6c. COMBINED COLUMNAR AND LINEAR TRANSPOSITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factor to suggest possible rectangles. Write the message on strips of cross-section paper and apply method of anagrams.</td>
<td>Same procedure as in 6a except working with rows instead of columns.</td>
<td>Proceed as in 6a, then as in 6b, i.e., anagram columns, then horizontal lines.</td>
</tr>
</tbody>
</table>

See Hitt, pp. 26-38.
DIGRAPHIC AND TRIGRAPHIC SUBSTITUTION

The chief advantage of digraphic and trigraphic substitution is that it prevents the decipherer from basing his analysis upon the frequency of individual letters in the language, and forces him to base any analysis to be made upon the frequency of digraphs and trigraphs: a circumstance which causes the analysis to become correspondingly difficult and, in addition, lessens the reliance which may be placed in it.

There are several ways of procuring digraphic substitution, of which the Playfair System is by far the most practical. Most of the other systems require tables, the use of which entails the expenditure of much labor, and the loss of one copy of which renders the entire system utterly unsafe. An excellent example of such a table is that shown in Fig. 1, which was taken from La Crittografia, pp. 84 and 85. Here the reciprocal relation
of plain text and cipher text is such that the same table can be used for enciphering and
deciphering. For example:

Enciphering—TH EN EM YP RE PA RE
    YR XR +K AL QK UL QK

Deciphering—YR XR +K AL QK UL QK
    TH EN EM YP RE PA RE

Note that two pairs, even if they involve a common letter, do not have a common
letter in the cipher equivalent, except as a matter of chance. The result of this fact is
that no grouping of cipher pairs representing combinations of E with other letters can be
made upon the basis of a common letter in such cipher pairs.

The process of arranging such a table, however, is very laborious, so that frequent
change is impractical. Another form of such a table which may, on the other hand, be
changed very frequently, but which does not possess the reciprocal relation, is that shown
in Fig. 2, but here there is an added disadvantage—that of having a common cipher letter
as a result in those pairs which represent plain-text pairs having a letter in common. Thus
ER, EN, ES, and ET are enciphered by TU, TK, TV, and WT respectively, or by the
reversals of the latter. These digraphs are found at the intersection of the vertical column
determined by the first letter of each pair as located in the top line, and the row determined
by the second letter of each pair as located in the first column at the left. When the cipher
pair is taken at the intersection of the row determined by the first letter, and the vertical
column determined by the second letter of each pair, the equivalents for these same
combinations are UK, KF, VL, and WN, or their reversals; but note that all the combinations
ending with the same letter will show a letter in common.

The same results may be obtained by employing sliding strips, as shown in the accom­
panying diagram. The direct alphabet, I, and the second mixed alphabet, IV, are fixed;
the first mixed alphabet, III, is mounted upon a movable strip with another direct alphabet,
II; the sliding alphabets are moved so that the first letter of the pair on alphabet II is placed
beneath A on alphabet I, then under the second letter of the pair on I, the two cipher
equivalents of the pair are found on III and IV. Thus, for the word THIS the successive
positions and encipherments are as follows:

\[
\begin{align*}
\text{TH = SA} & \quad \begin{cases}
\text{I—ABCDEFGHIJKLMNOPQRSTUVWXYZ} & \text{Fixed Alphabet} \\
\text{II—TUVWXYZABCDEFGHIJKLMNOPQRS} & \text{Movable Alphabets} \\
\text{III—MQUVWXYZSTENOGRAPHYBCDFIJKL} & \text{Fixed Alphabet} \\
\text{IV—CRYPTOGAMSBDDEFHIJKLMNOP} & \text{Fixed Alphabet}
\end{cases} \\
\text{IS = SL} & \quad \begin{cases}
\text{I—ABCDEFGHIJKLMNOPQRSTUVWXYZ} & \text{Fixed Alphabet} \\
\text{II—IJKLMNOPQRSTUVWXYZABCDGFH} & \text{Movable Alphabets} \\
\text{III—PHYBCDFIJKLMOUVWXZSTENOGRAM} & \text{Fixed Alphabet} \\
\text{IV—CRYPTOGAMSBDDEFHIJKLMNOP} & \text{Fixed Alphabet}
\end{cases}
\end{align*}
\]
Given a single long message or a series of messages in the same alphabets, a frequency table of pairs may be made the basis of solution, by assigning high-frequency-digraph values to the most frequent pairs. In the latter case, where two pairs having a common cipher letter have a common letter in their respective cipher equivalents, this relation would be a great aid in the assignment of values, since it would enable the decipherer to assign his values accordingly. In the case of key-word and direct alphabets the reconstruction of the alphabets may be attempted. Arbitrarily-mixed and random-mixed alphabets may also be used in such tables.

Still another form of table which may be used for digraphic substitution is that shown in Fig. 3. Here there are concerned one mixed and two direct alphabets and a quadricular table. The first letter of a pair is sought in Alphabet I, its equivalent taken in Alphabet II, and by following the horizontal line in the quadricular table determined by the second letter of the pair in Alphabet III to the vertical column determined by the first letter, the cipher letter is taken at the intersection. Thus:

```
TH  ER  EI  SN  OT  HI  NG
UH  RM  RI  CS  GK  EE  TP
```
Note that as far as the first letter in each pair is concerned, the encipherment is merely by means of a single mixed alphabet. It is only the encipherment of the second letter which is multi-alphabetical in nature.

The same table shown in Fig. 3, with one additional alphabet, IV, may be used for trigraphic substitution. The equivalent of the first letter in a group is found in Alphabet II directly beneath that letter in Alphabet I. The equivalent of the second letter is found in Alphabet IV directly opposite the letter in Alphabet III. The equivalent of the third letter is found at the intersection of the horizontal line in the quadricular table determined by the second letter, and the vertical column determined by the position of the third letter in Alphabet I. Thus:

\[
\begin{align*}
\text{THE REI} & \text{ SNO THI NGT} \\
\text{URV DD} & \text{I CQH URE TAN}
\end{align*}
\]

The variations of this system are many; but as far as the two letters in each group of triplets is concerned, encipherment is purely mono-alphabetical. (See Gioppi, pp. 45-46.)
COMPLEX SYSTEMS

When the steps in analysis given in the preceding tables have failed to lead to results, it may be concluded that the cipher is either the result of (1) a modification or a combination of the systems enumerated, such as the combination of Substitution and Transposition systems, or (2) a system simple in itself as regards enciphering, but difficult in its results as far as deciphering is concerned. Some of the latter have been devised by experts who are in possession of all the known methods of attacking ciphers and have elaborated systems which allow no opening for the would-be decipherer. No attempt is made here to enumerate or to elucidate all of these systems, but among them may be mentioned the following:

(1) Running Key Systems
(2) Multiplex Alphabet Systems
(3) Wheatstone Principle Systems
(4) Fractionating Systems
(5) Auto-key Systems
(6) Variable Key Systems

(1) Running Key Systems. These systems make use of the running text of a book, identical copies of which are in possession of the correspondents. For a brochure on the subject see Riverbank Publication No. 16.


(3) Wheatstone Principle Systems, which are based upon a mechanical cryptograph invented by Sir Charles Wheatstone in 1879. For a discussion of such a cipher and methods for solving it see Riverbank Publication No. 20.

(4) Fractionating Systems. The basic principle here is that the cipher letters or cipher numbers are compounded from parts of plain-text letters according to some definite system. A simple example is the following:

Alphabet—ABCDEFGHIJKLMNOPQRSTUVWXYZ
Numerical Value— 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Each letter is represented by two digits. Write the dispatch horizontally, then apply the two digits for each letter one under the other. Thus:
The cipher then is taken in any way in which a rearrangement of the digits may be effected. Thus, a very simple way would be to take the cipher digits in pairs from horizontal lines, and then find their letter equivalents on the conventional alphabet. This dispatch would begin

```
AAVJJ OSI etc.
```

In the case of any cipher number above 26, deduct 26 or a multiple thereof and find the equivalent of the remainder. Variations of the system are legion in number. The plain text may be written in groups of three, four, or five letters and the cipher letters may be selected accordingly upon some different scheme. This system, because of the number of unknown factors which are presented to the would-be decipherer, is a very difficult one to solve. Fractionating systems in which each cipher letter represents the halves, thirds, quarters, and possibly greater fractions of 2, 3, 4, or 5 plain-text letters may be devised, and would tax the ingenuity of the expert decipherer. (See Giropi, pp. 102-114.)

(5) Auto-key Systems. Sometimes called Auto-enciphering Systems. This system was described by Vigenère, reinvented in 1884 by Captain Delauney, and perfected by Josse. The basic principle is that each cipher letter automatically becomes the key for the encipherment of the succeeding plain-text letter. Usually a key-word alphabet or a random-mixed alphabet is used, the letters of which are numbered in sequence. Thus:

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

MESSAGE: Enemy prepares, etc.

```
ENEMY PREPARES
01012 11010101
54535 68561859
```

CIPHER: E K M U B W T Y H V U N N

Each cipher letter is produced in turn by finding the letter-value of the sum of the numerical equivalent of the preceding cipher letter and that of the plain-text letter to be enciphered; when this total exceeds 26, the latter amount is deducted and the letter-value of the remainder is taken as the cipher equivalent.

The great disadvantage of this system is that an error in one place produces errors in all the succeeding letters so that the recipient is caused to lose much time in the translation of a message which has many errors. A method which dispenses with the numerals is to construct a quadricular table from the alphabet as shown in Fig. 6.
Proceeding down the column determined by E (the first letter of the message) in the first horizontal line, to the line determined by the next plain-text letter N, the letter K, at the intersection, is taken as the cipher letter. Proceeding down the column determined by K in the first horizontal line to the line determined by E, the third plain-text letter, the cipher letter M, at the intersection, is taken as the cipher letter, etc. (See Gioppi, pp. 42-44.)

A method which is the equivalent to the quadricular table in its final results and which is easier to operate, makes use of two sliding strips bearing the alphabets; by shifting the lower strip so that the letter which becomes the key letter for the next encipherment, is placed beneath the letter immediately preceding the first letter in the alphabet concerned, the
cipher letter to represent the next text letter is found under the letter itself. The successive positions for the word ENEMY are as follows:

<table>
<thead>
<tr>
<th>Plain text</th>
<th>Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>SAIWGHVLJXOCMZPBKYRDNT EQ UFS</td>
</tr>
<tr>
<td>N</td>
<td>EQUFS A I WGHVLJXOCMZPBKYRDNT E</td>
</tr>
<tr>
<td>M</td>
<td>KYRDNT EQ UF SAIWGHBLJXOCMZPB K</td>
</tr>
<tr>
<td>Y</td>
<td>MZPBKYRDNT EQ UF SAIWGHVLJXOC M</td>
</tr>
<tr>
<td>B</td>
<td>UFSAIWGHVLJXOCMZPBKYRDNT EQU</td>
</tr>
</tbody>
</table>

Such a cipher is poly-alphabetical in nature and is characterized by the small number of repetitions. It is clear that all letters following the same cipher letter belong to the same alphabet. Frequency tables may be constructed upon this basis and combinations may be sought. It should be kept in mind that all the alphabets concerned in such a system are inter-related and come under the classification of Primary Alphabet Systems involving two identical mixed alphabet components.

(6) Variable-key Systems. Examples of these systems are to be found in those cases where the alphabets employed are applied irregularly, for instance, the alphabet may change after the encipherment of every plain-text letter E; or the key word may be broken irregularly, breaks being indicated by an agreed-upon null or indicator. The basic idea in such systems is the elimination of the external manifestations (such as those exhibited in Periodic Systems) by means of which it is possible to determine the number of alphabets and their respective positions. These systems, however, are not often encountered because of the practical difficulties attendant upon their use and the possibilities of error. (See Gioppi, pp. 34-35; Valerio, pp. 36-42; Bazeries, pp. 128-139.)
BIBLIOGRAPHY
OF WORKS ON CIPHER

Alberti, Leo B., *Opuscoli moralí* (Chap. on cipher), Venice, 1568.


Astle, *The Origin and Progress of Writing*, 1803.


Baravelli, Cifrarìo, Roma, 1893.


Becherus, *Spirensis Character, notitia linguarum universalis*, Frankfort, 1661.


Bihlander, Theodorus, *Tract, de ratione communiarum lingarum*.

Blair, William, *In Rees's Cyclopædia, s.v. "Cipher."

Boetzel, A., *Correspondance postale, télégraphique et téléphonique secrète*, 1898.


Breithaupt, Chr., *Disquisitio historica critica, cum osa de canis modis occulta scribendi*, Helmstadt, 1727.

Breithaupt, *Ars decifroria sive occultas scripturas solvensi et legendi scientia*, Helmstadt, 1737.


Cardano, Girolamo, *De Rerum Varietate* (Bk. XII, Ch. 61), 1557.

Cardano, *De subtilitate*.


Casaubon, Isaac, 1559 to 1614.


Colomno, Abram, *Scotographia Italica*, Prague, 1593.

Conrad, David Arnold, *Cryptographia denudata sive ars decifrandi*, Leiden, 1739.


Delastelle, F., *Traité élémentaire de cryptographie*, 1902.


Glauburg, von, *Expositio ad Polygraphiam Tri-themii*.


Haned (Resene Gibronte Reneclus), *Steganographia et Steganographia Nova*, Nürnberg, 1617.


Hugo, Germain, *De Origine scribendi*. 
Hottinga, D., *De Polygraphie*, Groningen, 1621.
Krohn, *Buchstaben und Zahlensysteme fuer die Chiffirung von Telegrammen*, Berlin, 1873.
Martin, G. von, *Cours diplomatique*, 1801.
Mengarini, *Cifrariori*, Roma, 1892.
Michael, Giovanni (Venetian Ambassador to England in the reign of Queen Mary), *Dispatches Only Lately Deciphered*.
Miller, Ludwig Heinrich, 1662.
Myśliowski, Emile, *Cryptography indéchiffurable* 1902.
Palatino, M. Giovambattista, *Nel qual s'insegna a scrivere, etc.*, Roma, 1548.
Palatino, Giovambattista, *Discorso de la Cifra*, 1553.

Porta, John Baptist, *De Furtivis litteraris*.
Porta, John Baptist, *De Literaris antiquis*, 1563.
Porta, J. B., *De occultis litterarum notis*, 1563, 1606.
Porta, Magiae Naturalis, Frankfort, 1607.
Prasse, de, *De Reticulis*, Lipsiae, 1799.
Puteanus, Erycius, *Epistolaria*.
Romanini (?), *La crittografia splenata*, Firenze, 1858.
Selenus, Gustavus, *Cryptomenytics et Cryptography*, 1624.
Tenson, Thomas (Archbishop), *Baconiana* (Explanatory references to Biliteral Cipher, pp. 27f.), London, 1679.
Trithemius, Johannes, *Chronologia Mystica*, 1516.
Trithemius, Johannes, *Polygraphie et universelle écriture cabalistique* (a translation into French by Gabriel de Collanges), republished Amsterdam, 1626.
Trithemius, Johannes, *Steganographia cum Clave*, Frankfort, 1551 and 1606.
Trithemius, Johannes, *Sui Ipsius Vindex*, Ingolstadt, 1616.
Trithemius, Johannes, *Libri Polygraphiae*, VI, 1606 (date on cover; title-page bears date 1600).
Valerio, *De la Cryptographie, Part I*, Paris, 1893; *De la Cryptographie, Part II*, 1896.
Vossius, Gerardus, *De Gram.*
Walchius, Johannes, Fab. 9.

Walter, Dechiffir-Wörterbuch, Winterthur, 1877.

Weker, De Seretis.

Wheatstone, Chas., Scientific Papers of Sir Charles Wheatstone, published by the Physical Society of London, 1879.

Wilkins, John (Bishop), Mercury, London, 1641, 1694.

Wilkins, John (Bishop), Mathematical and Philosophical Works (Containing Mercury), London, 1708.

Worcester, Marquis of (Edward Somerset), Century of Inventions, 1650.


ARTICLES


Mamy, le Génie civil, 1885.

Muirhead (Col.), Lecture in Technical Conferences of the U. S. Army Signal Schools, 1911 to 1912; 1912 to 1913.

All The Year, Vol. XXXV, p. 506.


Macmillan’s, Vol. XXIII, p. 328.

Month, Vol. LXXXI, p. 538.

Murray’s, Vol. VIII, p. 433.


Once A Week, Vol. IX, p. 607.