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

Presented to the Library of the Communications Security Section, Naval Communications Office of 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

RIVERBANK
LABORATORIES
[redacted]
GENEVA
ILLINOIS

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 attemps 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.

- **1*a*.** Cipher consists exclusively of letters.
  - **2*a*.** Cipher contains all or nearly all the different letters of the alphabet.
    - **3*a*.** Cipher groups do not form pronounceable combinations, except a very few, which are evidently the results of chance.
      - **4*a*.** Vowel and consonant count show cipher to be a form of **TRANSPOSITION.** Table IX. Hitt, pp. 23-25.
      - **4*b*.** Vowel and consonant count show cipher to be a form of **SUBSTITUTION.** Table II. Hitt, pp. 23-25.
    - **3*b*.** Cipher groups all form pronounceable combinations, evidently the result of a definite system for their production. (Pseudo-Code.) Table VII, 3*a*.
  - **2*b*.** Cipher contains only a limited number of different letters of the alphabet, five to ten. Table VII, 2*a*.
- **1*b*.** Cipher does not consist exclusively of letters.
  - **2*c*.** Cipher does not consist exclusively of numerals.
    - **3*c*.** Cipher does not consist of plain-text words, except as a result of chance.
      - **4*c*.** 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, 2*b*. Sometimes the substitution of arbitrary letters consistently applied will be useful.
      - **4*d*.** Cipher does not consist of symbols, signs, etc.
        - **5*c*.** Cipher consists of letters chiefly, with scattered numerals or signs at irregular intervals, suggesting sliding alphabets of more than 26 characters. Table IV, 3*b*.
        - **5*d*.** Cipher consists of numerals chiefly, with a limited number of letters or signs, suggesting sliding alphabets of more than 26 characters. Table VIII, 5*b*.
    - **3*d*.** Cipher consists of plain-text words only, but in unintelligible combinations. **ROUTE CIPHER.** Table IX, 2.
  - **2*d*.** Cipher consists exclusively of numerals. **NUMBER CIPHER.** Table. VIII.

[From Table I, 4*b*]

1. SUBSTITUTION CIPHER

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

[Also from Table VIII, 4*a*]

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, 2*a*.

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.

3b. Factoring discloses certain repeatedly recurring factors.
(PERIODIC MULTIPLE ALPHABET SYSTEM.)
Table IV, 3*a*.

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

4b. Substitution not equiliteral, 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 (MONOALPHABET) SYSTEM.
Table III.

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

6c. Substitution digraphic, i.e., pair for pair substitution.

6d. Substitution not digraphic.

7a. **PLAYFAIR SYSTEM**

7b. Substitution by means of a rectangle.
Pages 5-8.

7c. Substitution Trigraphic.
Pages 8-9.

7d. Substitution Polygraphic.
(Approaching Code.)

8a. **ORIGINAL PLAYFAIR SYSTEM**

Solve by Mauborgne or Moorman method.*

8b. **MODIFIED PLAYFAIR SYSTEM**

Solve by combination of Mauborgne and Moorman method.*

* See Mauborgne, J. O., *An Advanced Problem in Cryptography and Its Solution.* Leavenworth Press, 1914. Hitt, *Manual for the Solution of Military Ciphers*, 1st edition, pp. 76-83; 2nd edition, pp. 76-82.

TABLE III

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

1. SINGLE ALPHABET (MONO-ALPHABET) SYSTEM

(Frequency table shows "crests and troughs")

2a. STRAIGHT ALPHABET CIPHER

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

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 4*a* of this table.

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

See Riverbank Publication No. 17, pages 25-36, and Hitt, pages 39-62.

2b. MIXED ALPHABET CIPHER

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

3c. RECIPROCAL ALPHABET

3d. NON-RECIPROCAL ALPHABET

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

See Riverbank Publication No. 17, pages 37-46, and Hitt, pages 44-50.

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

[From Table II, 6b]

1. MULTIPLE ALPHABET SYSTEM

[Also from Table VIII, 4d]

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.**

[Also from Table II, 3b]

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.**

4a. Periodicity governed by the successive single letters of the plain text. **(MONOLITERAL PERIODICITY.)** Compile single frequency tables on the basis of the number of alphabets suggested by the most common factor.

Table V.

4b. Periodicity governed by successive groups of letters of the plain text, groups being equal in length. **(POLYLITERAL PERIODICITY.)** Determine the length of the groups and the number of alphabets employed. (See Valerio, pp. 36-42.) Compile single frequency tables upon these bases, then proceed as in *3a* of this table, except in the application of the plain-text equivalents, substitution must be made on the basis of successive groups of letters governed by the same key letter instead of by the successive single letters.

[Also from Table I, 5c]

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.**

These systems usually employ two concentric disks, or two sliding strips, which are moved regularly 1, 2, 3 . . . spaces after each letter or after a definite number of letters.

4c. 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 Pasanisi Disk, described by Gioppi, pp. 58-62. See Riverbank Publication No. 20.

4d. MIXED ALPHABETS

Break up the message into its constituent cycles and apply the frequency method to them. Attempt a 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.

[Also from Table VIII, 5b]

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. **(A-PERIODIC SYSTEMS.)**

3c. The successive alphabets are applied to word lengths. The various alphabets limited in number by a short key word, or a short key number; or the successive words are enciphered on random generatrices of a Poly-Alphabet.

4e. STRAIGHT ALPHABETS (This case should have been solved under Table II, *2a*.

5a. DIRECT Solve on the ordinary Poly-Alphabet or 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.

4f. MIXED ALPHABETS

5c. KEYWORD ALPHABETS

5d. RANDOM-MIXED, OR ARBITRARILY-MIXED, ALPHABETS

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 enciphered 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.

3d. The successive alphabets are employed irregularly; or the total number of alphabets is large, etc.; ciphers of more or less complexity in decipherment because of the lack of recurrences.

Pages 10-13.

TABLE V

1. MULTIPLE ALPHABET SYSTEM—Continued

[From Table IV, 4*a*]

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

2a. The several alphabets are inter-related and constitute a **PRIMARY ALPHABET SYSTEM.**

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 sub-alphabets (Secondary Alphabets) which are inter-related.

2b. The several alphabets are not inter-related and do not constitute a Primary Alphabet System.

The alphabets are all independent and are made separately. They may be Key-word Alphabets, Arbitrarily-Mixed Alphabets, or Random-Mixed Alphabets.

Each alphabet must be solved independently by the Frequency Table method.

3a. **PRIMARY ALPHABET SYSTEM OF TWO COMPONENTS**

3b. **PRIMARY ALPHABET SYSTEM OF MORE THAN TWO COMPONENTS**
Pages 7-9.

4a. **COMPONENTS IDENTICAL**

4b. **COMPONENTS NOT IDENTICAL**
Table VI.

5a. **BOTH COMPONENTS STRAIGHT ALPHABETS**

5b. **BOTH COMPONENTS MIXED ALPHABETS**

6a. 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. 60-63. 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.

6b. The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Reversed Alphabets. See Hitt, pp. 58-59. This case results from the second Beaufort Method of using a Vigenère Table, or from the use of the U. S. Army Disk, or from the sliding of a Direct Alphabet against a Reversed. Proceed as in 6*a* except applying the Reversed Alphabet sequence. See Riverbank Publication No. 16.

6c. **BOTH COMPONENTS KEY-WORD ALPHABETS**

7a. Both components proceed in the same direction, resulting in a series of 25 Non-reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.

7b. The two components proceed in opposite directions, resulting in a series of 26 Reciprocal Secondary Alphabets, all Arbitrarily-Mixed Alphabets.

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.

6d. **BOTH COMPONENTS ARBITRARILY- OR RANDOM-MIXED ALPHABETS.**

Proceed as in 6*c* of this table, except no assumption can be made on the basis of unbroken sequences, such as BCD, FGH, XYZ, etc.

TABLE VI

[From Table V, 4*b*]

1. MULTIPLE ALPHABET SYSTEM—Continued

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

- **3*a*.** One of the components is a Straight Alphabet.
  - **4*a*.** The Straight Alphabet component is a Direct Alphabet.
    - **5*a*.** 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.
    - **5*b*.** The Mixed Alphabet component is an Arbitrarily-Mixed or a Random-Mixed Alphabet. Proceed as in 5*a* except no assumptions of unbroken sequences in the mixed alphabet component can be made. See Hitt, pp. 63-71.
  - **4*b*.** The Straight Alphabet component is a Reversed Alphabet. Proceed as in 4*a* except applying the Reversed Alphabet sequence to the Straight Alphabet component.
- **3*b*.** Neither of the components is a Straight Alphabet, both Mixed Alphabets.
  - **4*c*.** Both components are Key-word Alphabets.
  - **4*d*.** 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.

TABLE VII

[From Table II, 4*b*]

1. SUBSTITUTION NOT EQUILITERAL

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

[Also from Table I, 2*b*]

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.

$2^n=2^5=32$, a Biliteral Alphabet
$3^n=3^3=27$, a Triliteral Alphabet
$4^n=4^3=64$, a Tetraliteral Alphabet
$5^n=5^2=25$, a Pentaliteral Alphabet
etc., etc.

Example of a Pentaliteral Alphabet, resulting from the use of a rectangle and a key word:

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

Example:
Plain text—T H E
Cipher—NN RA 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, 2*b*. See Hitt, pages 83-85.

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

[Also from Table I, 3*b*]

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

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

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.

5b. Regularity produced by means of a table, or a rectangle on one side of which are consonants only, on the other side vowels only. Each plain-text letter requires two cipher letters.
Compile a frequency table of pairs and attempt reconstruction of the table, or rectangle.

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

6b. Rectangle not based upon Straight Alphabets.

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.

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.

3b. Cipher groups not pronounceable, except as the result of chance. Cipher groups usually the result of a square or a rectangular table, for enciphering not only letters but also syllables, words, phrases, etc. Approaching a code system.

The alphabets at the sides may be Key-Word Alphabets, Arbitrarily-Mixed, or Random-Mixed Alphabets, or numbers.

Solution: Make a frequency table of pairs and apply the frequency table method modified by considerations arising from the frequency of the most common words, for which substitution will have to be made by single pairs. Attempt a reconstruction of the alphabets at the sides.

TABLE VIII

[From Table I, *2d*]

1. NUMBER CIPHER

(Mathematical Ciphers)

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

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.

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.

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.

4c. Factoring discloses no repeatedly recurring factors.

Compile a single frequency table.

5a. Frequency table shows marked "crests and troughs." Single Mixed Alphabet. 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*.

4d. Factoring discloses certain repeatedly recurring factors.

Periodic Multiple Alphabet System.

Proceed as in Table IV, *2a*.

Periodicity may be produced by the use of a key word in conjunction with a basic table. An example of such a system:

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

The values of the letters of a key word are added successively to the values of the plain-text letters. Thus:

Key word—H E L P
Value—17 14 23 27

Plain text—	T	H	E	E	N	E	M	Y	W	I
Plain-text values—	33	17	14	14	25	14	24	40	36	20
Key-letter values—	17	14	23	27	17	14	23	27	17	14
Cipher—	50	31	37	41	42	28	47	67	53	34

2b. Interval between lowest and highest pairs does not approximate 26. The numbers range from 01 to 00 or 00 to 99, implying usually that each plain-text letter has several values used at random.

3c. The several values for each plain-text letter are produced by means of a rectangular table. Rectangle with sides 10x 3, letters within.

4e. 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.

4f. Letters in rectangle not in sequence of Straight Alphabet.

5c. Letters in Key-word Alphabet sequence. Attempt reconstruction of Key-word Alphabet from VWXYZ sequence.

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, *2b*.

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

4g. Alphabets are continuous from 01 to 00.

4h. Alphabets are independent, in cycles of 25 or 26.

Make 4 frequency tables and try to fit each to the normal frequency table.

TABLE IX

[From Table I, 4*a*]

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.

3a. SIMPLE SYSTEM

4a. Vertical writing.

4b. Reversed writing.

4c. Rail fence cipher.

See Hitt, pages 28-30.

3b. MORE COMPLEX SYSTEM

4d. Transposition based upon geometrical designs.

Factoring process applied first to suggest possible rectangles.

5a. Construct rectangles suggested by the factors and attempt reading by all methods. See Hitt, pp. 26-38.

5b. Solve by means of formulae. See Riverbank Publication No. 19.

4e. Transposition not based upon geometrical designs.

5c. Transposition based upon rearrangement of entire columns, or rows, or both.

5d. Transposition based upon rearrangement or redistribution of individual letters by means of a grille. Solve by anagram method and attempt reconstruction of the grille. See Gioppi, pp. 33-31.

6a. COLUMNAR TRANSPOSITION

Factor to suggest possible rectangles. Write the message on strips of cross-section paper and apply method of anagrams.

6b. LINEAR TRANSPOSITION

Same procedure as in 6*a* except working with rows instead of columns.

6c. COMBINED COLUMNAR AND LINEAR TRANSPOSITION

Proceed as in 6*a*, then as in 6*b*, i. e., anagram columns, then horizontal lines.

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

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

Fig. 1

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 accompanying 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:

TH = SA	I—	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Fixed Alphabet
	II—	TUVWXYZABCDEFGHIJKLMNOPQRS	Movable Alphabets
	III—	MQUVWXZSTENOGRAPHYBCDFIJKL	Movable Alphabets
	IV—	CRYPTOGAMSBDEFHIJKLNQUVWXZ	Fixed Alphabet
IS = SL	I—	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Fixed Alphabet
	II—	IJKLMNOPQRSTUVWXYZABCDEFGH	Movable Alphabets
	III—	PHYBCDFIJKLMQUVWXZSTENOGRA	Movable Alphabets
	IV—	CRYPTOGAMSBDEFHIJKLNQUVWXZ	Fixed 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	
A	S C	T R	E Y	N P	O T	G O	R G	A A	P M	H S	Y B	B D	C E	D F	F H	I I	J J	K K	L L	M N	Q Q	U U	V V	W W	X X	Z Z	A
B	T C	E R	N Y	O P	G T	R O	A G	P A	H M	Y S	B B	C D	D E	F F	I H	J I	K J	L K	M L	Q N	U Q	V U	W V	X W	Z X	S Z	B
C	E C	N R	O Y	G P	R T	A O	P G	H A	Y M	B S	C B	D D	F E	I F	J H	K I	L J	M K	Q L	U N	V Q	W U	X V	Z W	S X	T Z	C
D	N C	O R	G Y	R P	A T	P O	H G	Y A	B M	C S	D B	F D	I E	J F	K H	L I	M J	Q K	U L	V N	W Q	X U	Z V	S W	T X	E Z	D
E	O C	G R	R Y	A P	P T	H O	Y G	B A	C M	D S	F B	I D	J E	K F	L H	M I	Q J	U K	V L	W N	X Q	Z U	S V	T W	E X	N Z	E
F	G C	R R	A Y	P P	H T	Y O	B G	C A	D M	F S	I B	J D	K E	L F	M H	Q I	U J	V K	W L	X N	Z Q	S U	T V	E W	N X	O Z	F
G	R C	A R	P Y	H P	Y T	B O	C G	D A	F M	I S	J B	K D	L E	M F	Q H	U I	V J	W K	X L	Z N	S Q	T U	E V	N W	O X	G Z	G
H	A C	P R	H Y	Y P	B T	C O	D G	F A	I M	J S	K B	L D	M E	Q F	U H	V I	W J	X K	Z L	S N	T Q	E U	N V	O W	G X	R Z	H
I	P C	H R	Y Y	B P	C T	D O	F G	I A	J M	K S	L B	M D	Q E	U F	V H	W I	X J	Z K	S L	T N	E Q	N U	O V	G W	R X	A Z	I
J	H C	Y R	B Y	C P	D T	F O	I G	J A	K M	L S	M B	Q D	U E	V F	W H	X I	Z J	S K	T L	E N	N Q	O U	G V	R W	A X	P Z	J
K	Y C	B R	C Y	D P	F T	I O	J G	K A	L M	M S	Q B	U D	V E	W F	X H	Z I	S J	T K	E L	N N	O Q	G U	R V	A W	P X	H Z	K
L	B C	C R	D Y	F P	I T	J O	K G	L A	M M	Q S	U B	V D	W E	X F	Z H	S I	T J	E K	N L	O N	G Q	R U	A V	P W	H X	Y Z	L
M	C C	D R	F Y	I P	J T	K O	L G	M A	Q M	U S	V B	W D	X E	Z F	S H	T I	E J	N K	O L	G N	R Q	A U	P V	H W	Y X	B Z	M
N	D C	F R	I Y	J P	K T	L O	M G	Q A	U M	V S	W B	X D	Z E	S F	T H	E I	N J	O K	G L	R N	A Q	P U	H V	Y W	B X	C Z	N
O	F C	I R	J Y	K P	L T	M O	Q G	U A	V M	W S	X B	Z D	S E	T F	E H	N I	O J	G K	R L	A N	P Q	H U	Y V	B W	C X	D Z	O
P	I C	J R	K Y	L P	M T	Q O	U G	V A	W M	X S	Z B	S D	T E	E F	N H	O I	G J	R K	A L	P N	H Q	Y U	B V	C W	D X	F Z	P
Q	J C	K R	L Y	M P	Q T	U O	V G	W A	X M	Z S	S B	T D	E E	N F	O H	G I	R J	A K	P L	H N	Y Q	B U	C V	D W	F X	I Z	Q
R	K C	L R	M Y	Q P	U T	V O	W G	X A	Z M	S S	T B	E D	N E	O F	G H	R I	A J	P K	H L	Y N	B Q	C U	D V	F W	I X	J Z	R
S	L C	M R	Q Y	U P	V T	W O	X G	Z A	S M	T S	E B	N D	O E	G F	R H	A I	P J	H K	Y L	B N	C Q	D U	F V	I W	J X	K Z	S
T	M C	Q R	U Y	V P	W T	X O	Z G	S A	T M	E S	N B	O D	G E	R F	A H	P I	H J	Y K	B L	C N	D Q	F U	I V	J W	K X	L Z	T
U	Q C	U R	V Y	W P	X T	Z O	S G	T A	E M	N S	O B	G D	R E	A F	P H	H I	Y J	B K	C L	D N	F Q	I U	J V	K W	L X	M Z	U
V	U C	V R	W Y	X P	Z T	S O	T G	E A	N M	O S	G B	R D	A E	P F	H H	Y I	B J	C K	D L	F N	I Q	J U	K V	L W	M X	Q Z	V
W	V C	W R	X Y	Z P	S T	T O	E G	N A	O M	G S	R B	A D	P E	H F	Y H	B I	C J	D K	F L	I N	J Q	K U	L V	M W	Q X	U Z	W
X	W C	X R	Z Y	S P	T T	E O	N G	O A	G M	R S	A B	P D	H E	Y F	B H	C I	D J	F K	I L	J N	K Q	L U	M V	Q W	U X	V Z	X
Y	X C	Z R	S Y	T P	E T	N O	O G	G A	R M	A S	P B	H D	Y E	B F	C H	D I	F J	I K	J L	K N	L Q	M U	Q V	U W	V X	W Z	Y
Z	Z C	S R	T Y	E P	N T	O O	G G	R A	A M	P S	H B	Y D	B E	C F	D H	F I	I J	J K	K L	L N	M Q	Q U	U V	V W	W X	X Z	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Fig. 2

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

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

Fig. 3

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:

THE	REI	SNO	THI	NGT
URV	DDI	CQH	URE	TAN

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.)

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

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

Fig. 4

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.

(2) Multiplex Alphabet Systems. These systems make use of a machine on the principle of the Bazeries disk cipher (Bazeries, pp. 250-261). For a brochure on the subject see Riverbank Publication No. 20; also De Viaris, "*L'Art de Chiffrer*," pp. 99-109.

(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—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
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:

ENEMY	PREPARES
01012	11010101
54535	68561859

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 Gioppi, 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:

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

MESSAGE: Enemy prepares, etc.

	E	N	E	M	Y	P	R	E	P	A	R	E	S
	22 ↗	20 ↗	22 ↗	12 ↗	17 ↗	14 ↗	18	22	14	11	18	22	26
	22	16	12	24	15	3	21	17	5	6	24	20	20
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.

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

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:

	Plain text	Cipher	26	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
I and II—	E	E	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S
	N	K	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E
III—	E	M	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	B	L	J	X	O	C	M	Z	P	B	K
IV—	M	U	M	Z	P	B	K	Y	R	D	N	T	E	Q	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M
V—	Y	B	U	F	S	A	I	W	G	H	V	L	J	X	O	C	M	Z	P	B	K	Y	R	D	N	T	E	Q	U

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. *Opusculi morali* (Chap. on cipher), Venice, 1568.

D'AMBRUM, COMIERS, *Traité de la Parole, etc.*, Brussels, 1691.

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

AURIOL, D' *Manuel de la correspondance secrete postale et télégraphique*, Parigi, 1887.

BARAVELLI, *Cifrario*, Roma, 1895.

BARTELS, *Leitfaden fuer den Unterricht auf dem königlichen Kriegsschulen*, Berlin, 1881.

BAZERIES, ETIENNE, *Etude sur la cryptographie militaire*, 1900.

BAZERIES, ETIENNE, *Les chiffres secrets dévoilés*, 1901.

BECHERUS, *Spirensis Character, notitia linguarum universali*, Frankfort, 1661.

BEAUFORT, *A System of Secret Writing*, London, 1883; 1893.

BELLASO, *Novi et singolari modi di cifrare* (8pp.), Brescia, 1555.

BELLASO, *Vero modo di scrivere in cifra* (16pp.), Brêscia, 1564.

BIBLIANDER, THEODORUS, *Tract, de ratione communarum lingarum.*

BLAIR, WILLIAM, *In Rees's Cyclopaedia, s.v.* "*Cipher.*"

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

BOETZEL ET O'KEENAN, *Écriture secrète*, Paris, 1895.

BOLTON, *Dictionary of Cryptography*, London.

BONTEMPS, *Les systèmes télégraphiques*, Paris.

BRACHET, *Dictionnaire chiffré*, Paris, 1850.

BREITHAUPT, CHR., *Disquisitio historica critica, cun'osa de vanis modis occulte scribendi*, Helmstadt, 1727.

BREITHAUPT, *Ars decifratoria sive occultas scripturas solvendi et legendi scientia*, Helmstadt, 1737.

B(RIDGES), N., *Sténographie and Cryptographie*, London, 1659.

BRUNSWICK, *Dictionnaire pour la correspondance télégraphique secrète*, Paris, 1868.

B(ULWER), J(OHN), *Chirologia and Chiromania*, London, 1644.

CARDANO, GIROLAMO, *De Rerum Varietate* (Bk. XII, Ch. 61), 1557.

CARDANO, *De subtilitate.*

CARLET, DU, *Cryptographie*, Paris, 1644.

CARLET, DU, JEAN ROBERT, *La Cryptographie*, Toulouse, 1644.

CASAUBON, ISAAC, 1559 to 1614.

COLLANGE, GABRIEL DE, *Polygraphie et universelle escriture cabalistique de Trithème*, Paris, 1561.

COLORNO, ABRAM, *Scotographia Italica*, Prague, 1593.

CONRAD, DAVID ARNOLD, *Cryptographia denudata, sive ars decifrandi*, Leiden, 1739.

CORTICELLI, L., *L'Ozio superato nelle cifre discolte*, Bologna, 1702.

COSPI, *Interpretazione delle cifre* (45 pp.), (English translation by Niceron, 1641), Florence, 1639.

DALGARNO, GEORGE, *Ars Signorum*, London, 1661.

DAVYS, JOHN, *Essay on the Art of Deciphering*, London, 1737.

DELASTELLE, F., *Cryptographie nouvelle*, Paris, 1893.

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

FALCONER, JOHN, *Cryptomenysis patefacta* ("Art of Secret Information"), London, 1695.

FLEISSNER, *Handbuch der Kryptographie*, Vienna, 1861.

FRIDERICI, *Cryptographie, oder Geheim-Correspondenz*, Leipzig, 1685.

GIOPPI, L., *La Crittografia* (Manuali Hoepli), 1897.

GLAUBURG, VON, *Expositio ad Polygraphiam Trithemii.*

GRAVEZANDE, *Introduction à la philosophie*, Leyden, 1737.

GROSS, H., *Handbuch fuer Untersuchungsrichter*, Teil II, Munich, 1914.

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

HITT, PARKER, *Manual for the Solution of Military Ciphers*, Leavenworth, 1916 and 1918.

HUGO, GERMANN, *De Origine scribendi.*

HOTTINGA, D., *De Polygraphie*, Groningen, 1621.

HULME, F. EDWARD, *Cryptography*, London, n. d.

JACOB, *Les secrets de nos pères, La Cryptographie*, Paris, 1858.

JOLLIET, *Les écritures secrètes dévoilés*, Paris, 1887.

KASISKI, *Die Geheimschriften und die Dechiffrirkunst*, Berlin, 1863.

KERCKHOFFS, A., *La Cryptographie militaire*, Paris, 1883.

KIRCHER, *Polygraphia nova et universalis*, Roma, 1663.

KLÜBER, J. L., *Cryptographik*, Tübingen, 1809.

KROHN, *Buchstaben und Zahlensysteme fuer die Chiffrirung von Telegrammen*, Berlin, 1873.

LACROIN, P., *Les Secrets*, 1858.

LACROIX, *La cryptographie ou l'art d'écrire en chiffres*, Paris, 1881.

L'ESPRIT, *Éléments de cryptographie*, Paris, 1889.

LOUIS, *Dictionnaire, pour la correspondance secrète*, Paris, 1881.

MAMERT-GALLIAN, *Dictionnaire télégraphique économique et secret*, Paris, 1874.

MARTIN, G. VON, *Cours diplomatique*, 1801.

MAUBORGNE, J. O., *An Advanced Problem in Cryptography and its Solution*, Ft. Leavenworth, 1914.

MEISTER, ALLOYS, *Die Anfänge der modernen diplomatischen Geheimschrift*, 1866.

MEISTER, ALOYS, *Die Geheimschrift im Dienste der päpstlichen Kurie*, Paderborn, 1906.

MENGARINI, *Cifrario*, Rome, 1892.

MICHAEL, GIOVANNI (Venetian Ambassador to England in the reign of Queen Mary), *Dispatches Only Lately Deciphered.*

MILLER, *Ludwig Heinrich*, 1662.

MONTFORT, *Anweisung zur Schnell- u. Geheimschrift Tachygraphie u. Cryptographie*, Berlin, 1893.

MYERS, *Manual of Signals*, New York, 1872.

MYSZKOWSKI, EMILE, *Cyrptographie indéchiffrable* 1902.

NIETHE, *Wörterbuch von Cryptographie*, Berlin, 1877.

PALATINO, M. GIOVAMBATTISTA, *Nel qual s'insegna a scriuere, etc.*, Rome, 1548.

PALATINO, GIOVAMBATTISTA, *Discorso de la Cifra*, 1553.

PETERS, KARL, *Die Geheimschreibekunst, oder Kryptographik*, 1856.

PHIPPS, CHARLES, *The Art of Decyphering* (In The Doctrine of Vulgar and Decimal Fractions), Dublin, 1745.

PORTA, JOHN BAPTIST, *De Furtivis litteraris.*

PORTA, JOHN BAPTIST, *De Literaris antiquis*, 1563.

PORTA, J. B., *De occultis literarum notis*, 1563, 1606.

PORTA, *Magiae Naturalis*, Frankfort, 1607.

PRASSE, DE, *De Reticulis*, Lipsiae, 1799.

PUTEANUS, ERYCIUS, *Epistolae.*

ROMANINI, VESIN DE, *La Cryptographie dévoilée*, Paris, 1857.

ROMANINI (?), *La crittografia svelata*, Firenze, 1858.

SCHNEICKERT, HANS, *Die Geheimschriften im Dienste des Geschäfts-und Verkehrslebens*, 1905.

SCHOTTUS, GASPAR, *Schola Steganographica*, Rome, 1665.

SELENUS, GUSTAVUS, *Cryptomenytices et Cryptographie*, 1624.

SIMONETTA, C., *Regles* (In Ecole des Chartres, Vol. 51, 1890), 1474.

SITTLER, *Dictionnaire abbréviatif chiffré*, Paris, 1858.

TENISON, THOMAS (Archbishop), *Baconiana* (Explanatory references to Biliteral Cipher, pp.-27f.), London, 1679.

THICKNESSE, PHILLIP, *Treatise on the Art of Deciphering, and Writing in Ciphers*, 1772.

TRITHEMIUS, JOHANNES, *Chronologica Mystica*, 1516.

TRITHEMIUS, JOHANNES, *Polygraphie et universelle escriture 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*, Ingoldstadt, 1616.

TRITHEMIUS, JOHANNES, *Libri Polygraphiae, VI, 1606* (date on cover; title-page bears date 1600).

TRITHEMIUS, JOHANNES, *Steganographia Vindicata*, Col. Agrip, 1635.

VALERIO, *De la Cryptographie, Part I*, Paris, 1893; *De la Cryptographie, Part II*, 1896.

VIARIS, HENRI, *L'Art de chiffrer et déchiffrer les dépêches secrètes*, Paris, 1893, 1895.

VIGENÈRE, BLAISE DE, *Traicté des Chiffres*, Paris, 1587.

VIGENÈRE, BLAISE DE, *Traicté du feu et du sel*, Paris, 1618.

VOSSIUS, GERARDUS, *De Gram.*

Walchius, Johannes, Fab. 9.

Walter, *Dechiffrir-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*, 1659.

Wostrowitz, Fleissner von, *Handbuch der Cryptographie*, Wien, 1881.

ARTICLES

Collon, A., "*Etude sur la cryptographie*" in *Revue de l'armée belge*, 1899 to 1902.

Kerckhoffs, *Le Journal des sciences militaires*, 1893.

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.

American Catholic Quarterly, Vol. XVIII, p. 858.

Appleton's, Vol. VII, p. 627.

Century, Vol. LXXIV, p. 290; Vol. LXXXV, p. 83.

Chamber's Journal, Vol. XX, p. 161; Vol. XXIV, p. 134; Vol. XXV, p. 175; Vol. XLIII, p. 193; Vol. XLIV, p. 70.

Cosmopolitan, Vol. XXXVI, p. 475, 584, 716.

Cornhill, Vol. XXIX, p. 172.

Craftsman, Vol. V, p. 207.

Gentleman's Magazine, N. S., Vol. LXV, p. 365.

Harper's, Vol. XCVII, p. 105.

Internation, Vol. VI, p. 405.

Knowledge, Vol. XI, p. 205; Vol. XII, p. 17.

Macmillan's, Vol. XXIII, p. 328.

Mouth, Vol. LXXXI, p. 558.

Murray's, Vol. VIII, p. 433.

North American, Vol. CXXVIII, p. 315.

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

Practical Magazine, Vol. I, p. 314