Journal of Criminal Law and Criminology

Volume 26
Issue 6 *March-April*

Article 10

Spring 1936

Cryptography in Criminal Investigations

Don L. Kooken

POLICE SCIENCE

Scientific Crime Detection Laboratory 1930

Editor: Fred E. Inbau

CRYPTOGRAPHY IN CRIMINAL INVESTIGATIONS

Don L. Kooken†

Considerable misapprehension has been present as to the importance of cryptography in criminal investigations. Most investigators are of the belief that cryptograms are seldom encountered in ordinary criminal investigations and that to become proficient in the solution of cipher writings one must have a special aptitude for the work and spend years in training on the subject. They conclude, therefore, that it would be inadvisable to devote a considerable length of time to a study of cryptography. Experience has taught us that these beliefs are ill-founded. It is true that cipher experts such as Major Herbert Yardley, Colonel George Fayban and Colonel Parker Hitt, have devoted many years in the study of complicated military ciphers and codes, and that to become expert in the class represented by these gentlemen would require what Major Yardley chooses to call "cipher brains." However, any person of ordinary intelligence and endowed with a stubborn perseverance can, by careful analysis, solve the simple type of cipher commonly encountered in criminal investigations.

> "The investigating officer who would decipher secret writings must have his heart in his work, perseverance, never-failing interest, an observation that allows nothing to

†Supervising Lieutenant, Indiana State Police.

> escape, and the gifts of combination and deduction. These are indeed general qualities which every investigating officer ought to possess. One might almost say that every man who is of the stuff out of which investigating officers are made is capable of reading ciphers."[1]

Cryptograms are encountered in criminal investigations much more frequently than one would imagine; often, however, they are not recognized as such. If the investigator will carefully scrutinize the notes, memoranda, letters, etc., of a criminal suspect, enciphered documents may be brought to light which otherwise would have gone undetected. A letter seemingly devoid of sense, a note book containing what appears to be pages of meaningless numerals, or an apparently insignificant scrawl on the back of an envelope, may prove to be secret writings, and though little importance is attached to it at the time, if deciphered, the result may alter the entire investigation. Of course, ciphers will be found which, after decipherment, may have no immediate bearing upon the case, but it must always be borne in mind that anything of sufficient importance to be enciphered is likewise of sufficient importance to be deciphered.

The complex operations of organized criminal bands necessitate the keeping of records, and of communication by telegraph and by mail. To protect these records and communications from exposing the nature or extent of the operations of the band should they fall into the hands of the police, ciphers are resorted to. The cipher writings taken from an arrested bank robber may disclose upon decipherment the names and addresses of his associates; the enciphered note book of a thief may, upon solution, prove to be a record of the fences through whom the thief disposes of his loot; and enciphered telegrams and letters may provide the connecting link in working up conspiracy cases.

The old adage "there is nothing new under the sun" is particularly applicable to cryptography. Nearly everyone has at one time or another made use of secret writing. He may have altered slightly a method or system of which he has read or he may have set about to devise a system of his own, but invariably when the non-expert invents a cipher, without knowing it he makes use of a system that has been in use since the reign of Julius Caesar or even before that time, for the origin of cryptography is obscure. History is replete with incidents of the use of cryptograms, and traces of its use pene-

[1] Gross, H., Criminal Investigation (3rd ed., Adam's Trans'l.—Kendal, 1934) 399.

trate the ages until they are lost in the mists of antiquity. It may be assumed, however, that hardly had writing as a means of recording thought been invented when there arose the necessity for evolving a method of writing that would be unintelligible to all except the person for whom the message was intended.

The ciphers encountered in criminal investigations are usually those of the non-expert and the problem of the investigator is to determine the basic principles of the system used and the method of analysis to follow in arriving at a solution. It is the intent of the writer to set out in this article simple rules of classification and analysis, to enable the investigator, with a reasonable amount of study, to recognize the simple types of cipher and proceed intelligently to their solution. For those who desire to attain proficiency in deciphering the more complex ciphers there are many excellent books available.[2]

The method or system of secret writing is called "cipher" and the enciphered message is referred to as a "cryptogram." Codes are arbitrary ciphers; that is, a word or a group of letters is given an abitrary meaning, usually more or less extended. While the sole purpose of ciphers are to preserve secrecy, codes are primarily used to condense messages for transmission. Very elaborate codes are used by governments and by many commercial institutions for the dual purpose of secrecy and economy in transmission. Codes, however, are not adaptable to the needs of the criminal, principally by reason of the hazard of written code books or keys falling into the hands of the police, although some very elementary codes have been encountered in criminal investigations. For practical purposes the criminal requires a system of enciphering that can be easily memorized, that can be frequently changed, and one that is not so involved as to make its use inexpedient.

Cryptograms may be roughly divided into two classes: transpositional, and substitutional. In the former class the letters or words of

[2] See the following, which also constitute the bibliography for this paper:
(a) De Grandpre, A., La Cryptographic Pratique (1905);
(b) Givierge, M., Cours de Cryptographie (1932);
(c) Hitt, P., Manual for the Solution of Military Ciphers (1918); also see Hitt, The A, B, C of Secret Writing (1935);
(d) Josse. H., La Cryptographie et ses Applications a l'art Militaire (1885);
(e) Kasiski, F. W., Die Geheimschriften und die Dechiffrir-Kunst (1863);
(f) Kerckhoffs, A., La Cryptographie Militaire ou des Chiffres Usites en Temps de Guerre (1883);
(g) Langie, A., Cryptography (1922); also see Langie and Soudart. Traité de Cryptographie (1935);
(h) Thomas, P. B., Secret Messages (1929);
(i) Valerio, P., Essai sur les Methodes de Dechiffrement (1893);
(j) Von Wastrowitz, E. B. F., Handbuch der Kryptographie (1881);
(k) Yardley, H. O., The American Black Chamber (1931).

the plain text are retained but are rearranged according to a prearranged plan so as to produce chaos. In the latter class the letters of the plain text are represented by other letters, numerals, characters, or symbols, according to a predetermined scheme or key. Since the method of analysis of the two classes will differ, the initial problem confronting the decodist is the determination of the class of cryptogram under examination.

Cipher experts have found, after considerable research, including the analysis of thousands of words of written text, that certain letters are used more frequently than others and that the frequency of use remains comparatively constant in all texts written in the same language, except on very short messages containing proper nouns or unusual words. It was also found that certain combinations of two and three letters are frequently repeated and that their order of frequency is comparatively constant. Further analysis revealed that the proportion of vowels AEIOU and common consonants LNRST to the total letters in a specimen of writing remains reasonably fixed in all texts of the same language. From these findings, tables were prepared for the various languages studied. These tables are invaluable as a guide in the analysis of all cryptograms.

It is obvious that in the transpositional cipher the frequency of letters will remain the same while in the substitutional cipher the normal frequency of letters will be destroyed. Therefore in this fact we obtain our first rule in the determination of classification of the cryptogram. Slight variations may be expected in short messages, such as those containing many proper nouns or concerning technical subjects. The percentage of vowels and common consonants, however, will not vary more than five per cent.

In the examination of long messages it is not necessary to make a frequency count of the entire message to determine the class. A count made from the first fifteen or twenty words, or if nulls[3] are suspected in the beginning of the message, a like number of words, selected from the body of the message, will suffice.

The language of the plain text may not always be known at the beginning of the examination, but a comparison of the frequency count with tables of frequency of various languages will invariably disclose the language of the plain text. Language characteristics, too, are of great aid in this determination. For example, the absence of

[3] Nulls are letters which are added to the plain text, either at the beginning or end of the message, to bring the total number of letters to a given amount, or they may be introduced throughout the plain text to mark word separations or separation of double letters.

the letters K and W would indicate Spanish, Portuguese, French or Italian; the high frequency of the letter I would indicate Italian; and so on, each language having striking characteristics which are apparent, if the frequency tables are carefully applied.

TABLE NO. I

Consolidated Frequency Table

(On a basis of 200 letters)

	English	English (Telegraphic)	French	German	Spanish	Italian	Portuguese
	(Hitt)	(Hitt)	(Givierge)	(Givierge)	(Givierge)	(Givierge)	(Truesdall)
A	16	16	14	9	24	20	28
B	3	3	2	3	2	2	1
C	6	6	7	6	10	8	7
D	8	8	9	11	10	8	8
E	26	26	34	36	28	25	28
F	4	4	3	3	14	2	2
G	3	4	1	6	3	4	2
H	12	8	1	9	2	2	2
I	13	14	13	14	14	20	12
J	1	1	1	1	12	*	1
K	2	2	*	3	.	*	.
L	7	8	9	8	11	13	6
M	6	6	6	4	6	5	9
N	14	14	17	19	14	13	10
O	16	17	13	5	18	18	22
P	4	5	5	1	6	6	6
Q	.	1	1	*	10	1	3
R	13	14	13	15	13	14	13
S	12	13	13	13	14	12	18
T	17	13	13	13	9	12	9
U	6	6	13	10	7	6	9
V	2	3	3	2	18	3	3
W	3	3	*	3	.	.	.
X	.	1	1	*	4	*	.
Y	4	4	1	*	2	*	.
Z	.	.	1	5	8	2	1

*Occurrence rare—usually in proper names.

Normal frequency tables prepared in graphic form on a basis of two hundred letter count will greatly facilitate the initial comparison. The frequency table of the cryptogram under examination may be increased or decreased to an equal basis and by superimposing the two tables the similarity or differences are strikingly visualized.

The following table of normal frequency of letters in English, French, German, Spanish, Italian, and Portuguese, represents a count of many thousands of letters and has been reduced to a basis of two hundred letters:

In an English text the total number of the vowels AEIOU used will comprise approximately 40% of the text; the common consonants LNRST can be safely taken as 30% and the consonants JKQXY at 2%. It is practically impossible to find five consecutive letters in an English text without a vowel, and a ratio of one to three may be expected. The following table indicates the percentages of vowels and common consonants occurring in English (both ordinary and telegraphic), French, German, Spanish, Italian and Portuguese:

TABLE II

	Vowels	Consonants	
English	38½	32	(Hitt)
English (Telegraphic)	40	30½	(Hitt)
French	42½	32	(Givierge)
German	45½	30½	(Givierge)
Spanish	43½	32½	(Givierge)
Italian	37	34	(Givierge)
Portuguese	49½	28	(Truesdall)

The following additional data is of value in the solution of cryptograms in English:

The order of frequency of doubled letters according to Valerio is: SS EE TT LL MM OO FF.

The order of frequency of trigrams according to Valerio is: THE AND THA HAT EDT ENT FOR ION TIO NDE HAS MEN NCE OFT STH.

The following table, compiled by Hitt, indicates the order of frequency of diagraphs prepared from a count of 2,000 letters based upon a count of 20,000 letters:

Table III

TH	50	AT	25	ST	20
ER	40	EN	25	IO	18
ON	39	EX	25	LE	18
AN	38	OF	25	IS	17
RE	36	OR	25	OU	17
HE	33	MT	24	AR	16
IN	31	EA	22	AS	16
ED	30	TI	22	DE	16
ND	30	TO	22	RT	16
HA	26	IT	20	VE	16

According to Valerio, the commonest diagraphs in the order of their frequency are: TH, HE, AN, ER, ON, RE, IN, ED, ND, AT, OF, OR, HA, EN, NT, EA, etc.

A combination of the substitutional and transpositional methods of encipherment may be used, but in this event the preliminary examination would place the message in the substitutional class and then after solution as such the message would fall under the transpositional class for completion.

Transpositional ciphers may be either monoliteral transpositions, with the letters rearranged singly according to a definite method or key, or they may be route ciphers where whole words or groups of letters are transposed. The number of different combinations possible with even a short text is infinite. For an illustration of this fact a sentence of but twenty letters may be arranged in 2,500,000 billion different combinations. If the decodist were obliged to depend upon the trial and error method and devoted but one second to the scrutiny of each combination, his chances of reaching a solution in less than a thousand years would be remote. The basic method by which these countless transpositions are effected are not so numerous. Success in the solution of transposition ciphers depends largely upon a careful evaluation of the fundamental principles by which the transposition is effected, upon careful calculation of probabilities, and upon an acquaintance with language characteristics. A knowledge of the circumstances under which the message was intercepted and any information relative to the persons concerned is also of great value in the solution of a cryptogram. After having determined that the cryptogram under examination is of the transpositional class the next step is to determine the method of transposition. For this purpose the transpositional class of cipher has been divided into five general groups:

(1) Those where the characters are arranged in the form of a square, rectangle, or other geometric figure, and the individual characters placed within the figure according to a symmetrical design;

(2) Those ciphers employing a grille as a means of effecting the transposition;

(3) This group includes all transpositions effected by rearranging the lines or columns of the text according to a key word;

(4) This group includes all special forms such as reversed writing, padded ciphers, beheadings, etc.;

(5) In this group are placed the route ciphers in which words or parts of words are rearranged according to a definite plan.

In the analysis of group one the number of letters in the message will suggest the size of the square or other figure. For example, a message of one hundred and fifty words would suggest rectangles of 2 x 75, 3 x 50, 5 x 30, 6 x 25, or 10 x 15. By rearranging the letters in the various rectangles suggested by the total number of letters in the message and noting carefully the distribution of vowels in line or in column it is not difficult to recognize the most logical arrangement, and then it is only a matter of further examination to determine the symmetrical patterns followed in the encipherment. The most popular system is the alternate vertical reading first down then up the vertical columns, or the alternate diagonal reading in the same manner except following diagonal lines instead of the vertical. Of course countless designs may be followed but the examiner will be able, after a little practice, to recognize fragments of words that will aid in the determination of the pattern followed.

The grille, described in group two, consists of a square of cardboard or other material in which certain perforations are made. In use, this perforated square is placed upon the paper and the message written by inscribing the letter on the paper through the openings in the grille beginning at the top and writing from right to left in the normal manner, until all the openings are filled. Then the grille is turned one quarter turn to the right exposing new surface of the paper and the message continued. This operation is repeated until all four corners of the grille have occupied the same position. The grille is always a square of an even number and the openings so arranged that there will be no overlapping. The following is a diagram of a grille consisting of sixty-four spaces:

3	2	■	4	2	4	■	4
4	■	2	3	4	■	2	3
3	4	■	4	3	2	3	2
■	3	2	■	2	■	4	■
3	2	3	4	3	4	■	3
4	■	4	■	2	3	2	■
■	4	3	2	■	4	3	2
2	3	2	4	2	3	4	■

Grille is cut as in the above pattern, removing the blocked-out areas. This then leaves openings for letters in the number 1 position. When the grille is turned clockwise 90° the openings (i. e., blocked out areas above) correspond to the squares marked 2. Similarly, when moved through additional 90° turns the openings for the 3 and 4 positions appear.

The grille is not often used by criminals because it necessitates the keeping of a key, and is not particularly adapted for messages of over one hundred letters. The method of analysis is shown later in this article.[4]

Analysis of group three transpositions is the same as that for group one except that after the proper geometrical figure is determined it is then necessary to determine the order in which the columns are read.

Group four represents the simplest form of transpositions and

[4] Example 3, *infra.*

even the novice finds little difficulty in solving them. At best they offer only a temporary delay in the reading of the message.

Group five or route cipher is not particularly popular with criminals because the words are left intact and the general contex of the message can be sensed because of the words used. There are many forms of effecting this transposition. The common form is to write the message in lines of equal number of words, then transcribe the message by reading up or down the columns. The analysis of this type cipher is not particularly difficult, as the choice of words will indicate words that logically should be used together. Moreover, the interval between these words will indicate the number of columns, etc.

Substitutional ciphers may be roughly divided into two groups: first, the simple substitution in which each letter of the plain text is represented by some other letter, character numeral or symbol, and the same substitution is continued throughout the text; second, those wherein multiple alphabets are used either by means of a key word or by specially prepared tables which permit a choice of several characters or numbers to represent each letter of plain text.

The method of analysis of the simple substitution is that of a comparison of frequency tables and recurring bigrams and trigrams. In the second group attention is directed toward the recurring bigrams and trigrams, and by a count of the interval between such recurrences the number of alphabets may be determined, and then the letters falling under each cipher alphabet is considered as a simple substitution cipher.

Some of the simple substitutions make use of several characters or numbers to represent each letter of the plain text. However, because of the increase in length of even a short message they are not commonly used, particularly where the message is intended for telegraphic transmission.

Many devices have been used in effecting substitutions. Following is a discussion of some of the most popular ones.

Blaise de Vigenere, a French diplomat and cryptographer, designed a cipher square or table for use in enciphering and deciphering messages by means of multiple alphabets. This table as it is used today consists of twenty-six alphabets arranged in the form of a square. The first or primary alphabet is in the conventional order and each succeeding alphabet is shifted one letter to the left of its predecessor, the extra letters being carried to the extreme right to complete the line:

	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	abcdefghijklmnopqrstuvwxyz
B	bcdefghijklmnopqrstuvwxyza
C	cdefghijklmnopqrstuvwxyzab
D	defghijklmnopqrstuvwxyzabc
E	efghijklmnopqrstuvwxyzabcd
F	fghijklmnopqrstuvwxyzabcde
G	ghijklmnopqrstuvwxyzabcdef
H	hijklmnopqrstuvwxyzabcdefg
I	ijklmnopqrstuvwxyzabcdefgh
J	jklmnopqrstuvwxyzabcdefghi
K	klmnopqrstuvwxyzabcdefghij
L	lmnopqrstuvwxyzabcdefghijk
M	mnopqrstuvwxyzabcdefghijkl
N	nopqrstuvwxyzabcdefghijklm
O	opqrstuvwxyzabcdefghijklmn
P	pqrstuvwxyzabcdefghijklmno
Q	qrstuvwxyzabcdefghijklmnop
R	rstuvwxyzabcdefghijklmnopq
S	stuvwxyzabcdefghijklmnopqr
T	tuvwxyzabcdefghijklmnopqrs
U	uvwxyzabcdefghijklmnopqrst
V	vwxyzabcdefghijklmnopqrstu
W	wxyzabcdefghijklmnopqrstuv
X	xyzabcdefghijklmnopqrstuvw
Y	yzabcdefghijklmnopqrstuvwx
Z	zabcdefghijklmnopqrstuvwxy

The first line of capitals represent the letters of the plain text; and the column of capitals at the left of the square represent the letters used to form the key word.

To illustrate the method if enciphering by means of this table, assuming it is desired to encipher the word "examined" using the key word FORT. The plain text is written and the key word underneath:

Plain text: E X A M I N E D
Key word: F O R T F O R T

Referring to the table and following down the column headed by the capital letter E of the line of capitals at the top of the square, to the line or alphabet indicated by the capital letter F in the column of capitals at the left of the table, at the point where the column and line intersect the letter J is found. This is the first letter of the cipher text. Repeating the operation with the letters X and O yields L as the second letter of the cipher text. Continuing in the same manner the following is obtained:

Plain text.	E	X	A	M	I	N	E	D
Key word:	F	O	R	T	F	O	R	T
Cipher text:	J	L	R	F	N	B	V	W

Therefore with Vigenere's table the word "Examined" enciphered by means of the key word "fort" becomes JLRFNBVW. To decipher a message the operation is reversed.

Giovanni Battista da Porta, a Neapolitan physician and noted cryptographer of the early sixteenth century, designed a table of multiple alphabets for use in enciphering and deciphering by means of a key word. Porta's table, adapted to the English language, consists of thirteen alphabets arranged in double lines of thirteen letters each, the upper line of each alphabet is in conventional order but the second line of each successive alphabet is moved one letter to the right and the extra letter or letters fill out the space at the extreme left of the line. The letters which serve to form the key word are arranged in double column of capitals at the left of the square, each pair of capitals controlling the alphabet to their right.

AB	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
CD	a	b	c	d	e	f	g	h	i	j	k	l	m
	z	n	o	p	q	r	s	t	u	v	w	x	y
EF	a	b	c	d	e	f	g	h	i	j	k	l	m
	y	z	n	o	p	q	r	s	t	u	v	w	x
GH	a	b	c	d	e	f	g	h	i	j	k	l	m
	x	y	z	n	o	p	q	r	s	t	u	v	w
IJ	a	b	c	d	e	f	g	h	i	j	k	l	m
	w	x	y	z	n	o	p	q	r	s	t	u	v
KL	a	b	c	d	e	f	g	h	i	j	k	l	m
	v	w	x	y	z	n	o	p	q	r	s	t	u
MN	a	b	c	d	e	f	g	h	i	j	k	l	m
	u	v	w	x	y	z	n	o	p	q	r	s	t
OP	a	b	c	d	e	f	g	h	i	j	k	l	m
	t	u	v	w	x	y	z	n	o	p	q	r	s

QR	a	b	c	d	e	f	g	h	i	j	k	l	m
	s	t	u	v	w	x	y	z	n	o	p	q	r
ST	a	b	c	d	e	f	g	h	i	j	k	l	m
	r	s	t	u	v	w	x	y	z	n	o	p	q
UV	a	b	c	d	e	f	g	h	i	j	k	l	m
	q	r	s	t	u	v	w	x	y	z	n	o	p
WX	a	b	c	d	e	f	g	h	i	j	k	l	m
	p	q	r	s	t	u	v	w	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	n

For the purpose of illustration, if the word "examined" is to be enciphered by means of the above table and the key word is FORT, the plain text is written with the key word repeated underneath, as:

Plain text: e x a m i n e d
Key word: F O R T F O R T

Referring to the table, the key letter F is found as the second letter of the third pair of capitals at the left of the table. The letter p is found opposite (in the case above) the letter e in this third alphabet. P is therefore written as the first letter of the cipher text. Using the alphabet indicated by the letter O, which is the second letter of the key word, X the second letter of the plain text is enciphered E. Continuing in the same manner the plain text word "Examined" is enciphered PESQTHWU. Thus:

Plain text: e x a m i n e d
Key word: F O R T F O R T
Cipher text: P E S Q T H W U

Admiral Sir Francis Beaufort, in a cipher which bears his name, employed Vigenere's table but modified the method of encipherment. Beaufort used the top line of capitals to represent the letters of the key word and the column of capitals at the left of the table to represent the cipher text. In operation, the key word is written over the plain text and by descending the column indicated by the first letter of the key word until the first letter of the plain text is encountered the first letter of the cipher text is found to the left of this line. Comparing Vigenere's and Beaufort's systems the word "examined" enciphered with the key word FORT would be:

Vigenere		Beaufort	
Plain text:	E X A M I N E D	Key word:	F O R T F O R T
Key word:	F O R T F O R T	Plain text:	E X A M I N E D
Cipher text:	J L R F N B V W	Cipher text:	Z J J T D Z N K

For a number of years the Mexican government used a modified form of Vigenere's cipher in which the table consisted of mixed alphabets instead of alphabets in their conventional order. The primary alphabet was based on a selected word with the remaining letters of the alphabet written in consecutive order thereafter. For example, if the word "importance" is selected, the primary alphabet would be:

IMPORTANCEBDFGHJKLQSUVWXYZ

This primary alphabet is then used to construct a table of twenty-six alphabets moving each succeeding alphabet one letter to the left of its predecessor as in Vigenere's table. The completed table would appear thus:

```
IMPORTANCEBDFGHJKLQSUVWXYZ
MPORTANCEBDFGHJKLQSUVWXYZI
PORTANCEBDFGHJKLQSUVWXYZIM
ORTANCEBDFGHJKLQSUVWXYZIMP
RTANCEBDFGHJKLQSUVWXYZIMPO
TANCEBDFGHJKLQSUVWXYZIMPOR
ANCEBDFGHJKLQSUVWXYZIMPORT
NCEBDFGHJKLQSUVWXYZIMPORTA
CEBDFGHJKLQSUVWXYZIMPORTAN
EBDFGHJKLQSUVWXYZIMPORTANC
BDFGHJKLQSUVWXYZIMPORTANCE
DFGHJKLQSUVWXYZIMPORTANCEB
FGHJKLQSUVWXYZIMPORTANCEBD
GHJKLQSUVWXYZIMPORTANCEBDF
HJKLQSUVWXYZIMPORTANCEBDFG
JKLQSUVWXYZIMPORTANCEBDFGH
KLQSUVWXYZIMPORTANCEBDFGHJ
LQSUVWXYZIMPORTANCEBDFGHJK
QSUVWXYZIMPORTANCEBDFGHJKL
SUVWXYZIMPORTANCEBDFGHJKLQ
UVWXYZIMPORTANCEBDFGHJKLQS
VWXYZIMPORTANCEBDFGHJKLQSU
```

```
WXYZIMPORTANCEBDFGHJKLQSUV
XYZIMPORTANCEBDFGHJKLQSUVW
YZIMPORTANCEBDFGHJKLQSUVWX
ZIMPORTANCEBDFGHJKLQSUVWXY
```

The method of enciphering is the same as with Vigenere's table, that is, the first line represents the plain text and the left hand or first column the letters of the key word. The letters of the cipher text are found at the junction of the column and line.

The cipher of Saint Cyr uses sliding alphabets by means of which the alphabets may be changed at will. The device consists of a short rule on which the alphabet is inscribed in conventional order and a second rule bearing two consecutive alphabets, thus:

```
       ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
```

The short slide can be moved to the right or left until the letter A coincides with the proper letter of the key word. The short slide represents the alphabet of the plain text and the long slide the cipher alphabets. For example, with the letter A set to the key letter H as indicated in the diagram above, letter E of the plain text would be enciphered as L.

A numerical slide system, similar to the Saint Cyr sliding alphabet was devised to provide multiple alphabets as well as multiple ways of representing each letter with one setting. This system used four slides or rules graduated by equidistant strikes. One short slide bears the alphabet in conventional order; the other short slide is inscribed with the alphabet in reverse order. On one of the long slides are inscribed the numerals 1 to 50; and the other long slide bears the numerals 51 to 100. The following is a diagram of the device:

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
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

If the word ABOUT is to be enciphered with the slides set to the key 7;60 as shown in the above diagram, and using the upper alphabet either of the two numbers falling under each letter may be used at will. For example the word may be transcribed 7;61;21;80;26. Utilizing the lower alphabet with the choice of either of the two lines of figures above it, the same word can be enciphered 85;31;74;12;66. It will be noted that each letter may be represented by any one of four different numerals.

The cipher of Count Grosfeld utilized a numerical key word. The cipher letter was obtained by counting ahead the number of spaces indicated by the key number and transcribing the letter occupying that space as the cipher letter. For example, if it is desired to encipher the word "enemy" with the key number 34567. Counting ahead three spaces from E yields H as the first letter of the cipher text and four spaces ahead of the letter N gives R as the second letter of the cipher text. Continuing in this manner the cipher word should be HRISF.

Plain text:	E	N	E	M	Y
Key number:	3	4	5	6	7
Cipher text:	H	R	I	S	F

Another substitution cipher known as the "Playfair" cipher was used extensively during the World War and has been used in a modified form by criminals. This cipher makes use of a key word or words located in the cipher square by prearrangement. The cipher square is divided into twenty-five spaces and the key word is written in selected lines of the square. Then the other letters of the alphabet that are not included in the key word are added in alphabetical order in the vacant squares. The letters I and J are represented by the same square.

Suppose the key word to be BUCKINGHAM and is to be distributed in the first and third lines of the square then the first operation in building up the square would be as follows:

B U C K IJ
N G H A M

Next the remaining letters of the alphabet are added in conventional order beginning with line two. As:

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

To encipher, the plain text is divided into groups of two letters each, introducing nulls to divide repeated or doubled letters. Each pair of letters are enciphered by substituting letters from the square, as follows:

(1) When the pair of letters occur is a vertical column—substitute the letters immediately below the letter of the plain text.

When the plain text letter is at the foot of the column then substitute for it the letter at the top of the same column;

(2) When the pair of letters occur in a horizontal line substitute the letter that occurs immediately at the right of the plain text letter. When this letter is at the right end of the line then substitute for it the letter at the extreme left of the same line;

(3) When the pair of letters are at opposite corners of a rectangle formed by the small squares, substitute each letter of the pair by the letter in the other corner of the rectangle and in the same horizontal line.

For example suppose we wish to encipher the word "Washington," using the square as shown above. First dividing into groups of two letters each we have wa sh in gt on. We find the pair wa located in the rectangle composed of the lines GHA, QRS, and WXY. Therefore we substitute Y for W and G for A. The next pair is found in the square HA, RS, accordingly we substitute R for S and A for H.

Passing to the next pair (in) we find they are located in the opposite corners of the rectangle formed by the first three lines of the table and we substitute B for i and M for n. The pair gt are in the rectangle GHAM, QRST and the substitution is M for g and Q for t. The last pair (on) are in the rectangle formed by the second and third lines of the square and D is substituted for o and M for n.

Consolidating we have:

Plain text:	wa	sh	in	gt	on
Cipher text:	YG	RA	BM	MQ	DM

It will be noted that the same letter in the plain text may be represented in a number of ways and likewise that the same cipher letter may represent different letters of plain text. In the above cipher letter M represents plain text letters n, g, and n.

The analysis of a "Playfair" cryptogram must proceed along the lines of recurring pairs of letters, and working from the frequency of diagraphs the square can be reconstructed.

A "Playfair" cryptogram always consists of an even number of characters and when divided into pairs of letters there will be no double letter pairs.[5]

(To be concluded in next issue)

[5] Space does not permit a detailed explanation of the various steps in the solution of "Playfair" ciphers. An excellent analysis is given by Langie and Givierge in their works referred to in note 2.