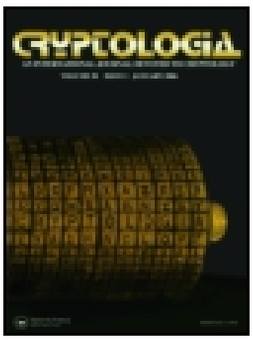


CRYPTOLOGIA

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

A TRIGRAPH CIPHER WITH A SHORT KEY FOR HAND USE

JOSEPH R. KRUSKAL

To cite this article: JOSEPH R. KRUSKAL (1985) A TRIGRAPH CIPHER WITH A SHORT KEY FOR HAND USE, CRYPTOLOGIA, 9:3, 202-222, DOI: 10.1080/0161-118591859933

To link to this article: https://doi.org/10.1080/0161-118591859933

Published online: 04 Jun 2010.

A TRIGRAPH CIPHER WITH A SHORT KEY FOR HAND USE

JOSEPH R. KRUSKAL

ABSTRACT: The cipher presented here is trigraphic, because triples of letters are mapped into triples of letters, and it is truly trigraphic because all three letters of the triple are treated in the same fashion. The key consists of a square or rectangular array of letters (like that used for the Playfair), which must have an odd number of rows and an odd number of columns. The cipher is a very simple algebraic cipher, but it is suitable for hand ciphering and deciphering. It is believed to be almost as easy to use as a Playfair or Delastelle, and possibly more secure against cryptanalysis.

A cipher is presented that is suitable for hand use and is truly trigraphic, i.e., trigraphs are mapped into trigraphs, and each position in the trigraph is treated in the same fashion as every other. In a recent issue of The Cryptogram, "Zenith" [1,2] describes Trifair, an extension of the Playfair cipher to trigraph (and n-graph) ciphers. The Playfair, the Trifair, and our cipher may all be redescribed for theoretical purposes in terms of letter coordinates, using two coordinates to identify each letter. Both the Playfair and the Trifair map pairs of coordinates into pairs of coordinates, so they become digraphic at the coordinate level. Our cipher maps triples of coordinates into triples of coordinates, so at the coordinate level it remains trigraphic.

About 50 years ago, L. S. Hill [3,4] introduced a general class of algebraic ciphers, of which our cipher is almost a special case. However, we provide a simple method of ciphering and deciphering by hand using only a very small and simple table. Nothing of this sort was provided with or possible for Hill's cipher.

On page 404, Kahn [5] reviews polyalphabetic ciphers. Referring to polyalphabetic ciphers other than the work of L. S. Hill [3,4], he states: "Ever since Wheatstone's Playfair ... other cryptographers have tried to extend his geometrical technique to trigraphic substitution. Nearly all have failed. Perhaps the best known effort was ... a pseudo-trigraphic system in which two letters were monalphabetically enciphered and the third depended only on the second.

Finally, about 1929, Jack Levine used six 5 x 5 squares to encipher trigraphs in an ingenious extension of Playfair. But he did not disclose his method." Furthermore, Gaines [6] is not very positive about existing trigraph ciphers either, as may be seen from her chief comments on this topic (page 199): "Occasionally, such a tableau... is made to serve (not very successfully) for trigram encipherment... . But for trigram encipherment, another type of tableau is commoner: ... The exact details of construction are not always the same, and the methods prescribed for using such a tableau are sometimes quite devious, but the results are fairly uniform: We obtain cryptograms in which enciphered pairs have alternated with enciphered (sometimes not enciphered!) single letters."

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

Figure 1.

I do not know how valuable a cipher for hand use is in this age of automated ciphering and deciphering, but it may have at least some conceptual interest, some recreational interest, and conceivably some use as one stage of a ciphering system for an isolated individual who needs to avoid equipment and tables which might betray the fact that he is engaged in secret communication. Our cipher has the following characteristics. (1) Only a short key is required, which is a table like that of the Playfair cipher, so the entire system can easily be committed to memory. (2) The cipher is truly trigraphic, and appears to me more difficult to cryptanalyze than the Playfair, Delastelle, and other digraphic ciphers. (3) Though the methods of hand ciphering and deciphering take longer to learn than that of the familiar digraphic ciphers, once learned they are almost as convenient and only a little slower. (4) It is almost a special case of the cipher invented by L. S. Hill [3,4] (also see Kahn [5], pages 404-408).

This trigraph cipher can be based on a 5 x 5 table like the central part of Figure 1, a 3 x 9 table, or on any m x n table that is large enough to accommodate the alphabet in use, if m and n are <u>both</u> <u>odd</u>. (Plaintext and ciphertext use the same alphabet.) For simplicity, only 5 x 5 tables are discussed below, though other shapes and sizes are also of interest. For convenience, the illustrations are all based on filling the table in alphabetical order, as in Figure 1, though in practice of course the order of the letters in the table constitutes the key. For explanatory purposes, it is convenient to think of the table as surrounded by eight identical tables. In practical ciphering it is helpful to include three rows of the surrounding tables, as in Figure 1, but this surround is not needed for deciphering.

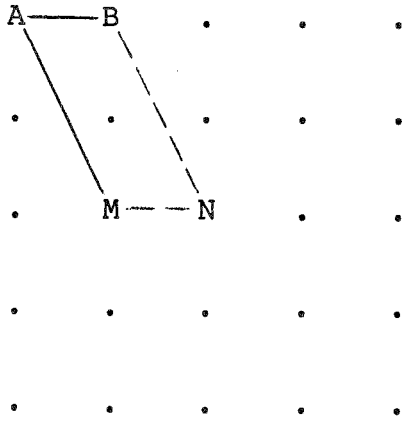


Figure 2.

Plaintext	A M B	U S H
Ciphertext	N Q L	P K E

Figure 3.

CIPHERING

Suppose the plaintext is AMBUSH and consider the first trigraph, AMB. To find the first cipher letter, we locate A, M, and B in the central part of Figure 2, mentally draw lines from A to M and from A to B, and then "complete the parallelogram" as shown in Figure 2, i.e., draw parallel lines from M and B and find where they meet, at N. This is the first cipher letter.

Another way of describing the same step is to see what move is required to get from A to M, namely, 2 down and 1 to the right, and then take that move starting at B. Alternatively, we may see what move is required to get from A to B, namely 1 to the right, and take that move from M.

To find the second cipher letter, start from M and complete the parallelogram to B and A. This takes us out of the central part to Q (in the upper middle part). As an alternative method of finding the second cipher letter, we may use M and B from the central part and A from the lower middle part. When this parallelogram is completed, it leads to the Q in the central part. In general, any copy of a letter may be used, as convenient. If copies are chosen correctly, it is never necessary to go outside the central table by more than two rows or columns. To cipher without surrounding extra rows, it is necessary to reenter the table from the bottom when leaving it from the top, and vice versa; also, to reenter the table from the left when leaving it from the right, and vice versa.

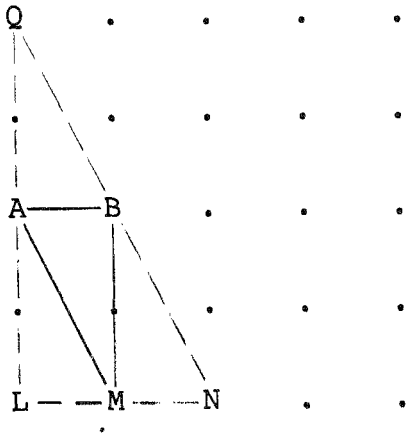


Figure 4.

To find the third cipher letter, start from B and complete the parallelogram to A and M. This yields L, so the ciphertext triple is NQL, as shown in Figure 3. The same method applied to plaintext USH yields FKE. Figure 4

shows all three parallelograms drawn for AMB. Notice that the three cipher letters N, Q, and L are the three outer vertices of the large triangle, and that the three plaintext letters A,M, and B bisect the three sides of this triangle.

With practice a number of simple tricks become apparent, and ciphering becomes much faster than it may seem from this description. These are discussed later under the heading of "Practical Ciphering."

DECIPHERING

One step in deciphering is to find a letter halfway between two ciphertext letters. For example, halfway between A and C is B, and halfway between A and N is G. Several other examples are shown in Figure 5. The first part shows pairs where it is not necessary to go outside the central table.

If the two letters are separated by an odd distance, either horizontally or vertically, so there is no point halfway between, then it is necessary to select an alternative copy of one of the letters outside the central table, in such a way that the two letters will have a point halfway between them. The second part of Figure 5 shows pairs where it is necessary to go one row outside the central table, and the third part shows pairs where it is necessary to go two rows outside the central table.

AC	B	DA	E	GH	K
AN	G	HX	C	GN	Z
FK	H	AT	Z	GO	X
AZ	N	AG	T	NR	E
DY	O	AH	R	IS	L
CZ	O	AM	I	OS	A

Figure 5.

For practical work, however, it is easier never to go outside the central table. Instead, one soon learns to apply the following rules, both to the two rows involved and the two columns involved:

12 → 4 13 → 2 14 → 5 15 → 3.

23 → 5 24 → 3 25 → 1

34 → 1 35 → 4

45 → 2

For example, consider the pair BH. This uses rows 12 and columns 23. Mapping 12 to 4 and 23 to 5 from the table above, the halfway letter is in row 4 and column 5, namely U. The patterns encompassed by the table above are very regular, and easily picked up.

To decipher the second ciphertext trigraph, FKE, proceed as follows. The first plaintext letter is halfway between K and E, namely, U. The second plaintext letter is halfway between E and F, namely, S. The third plaintext letter is halfway between F and K, namely, H. Thus the plaintext is USH. In practice, deciphering goes faster than ciphering.

It is the need to find a letter halfway between two given letters that requires use of an odd number m of rows and an odd number n of columns. For suppose that m is even and n is odd. Then among the pairs of letters, some pairs will have no letter halfway between, and some pairs will have two letters halfway between (which letter we get depends on which copy of the given letters we use). Specifically, half the pairs will be of one type and half of the other, depending on whether the number of rows separating the pair is odd or even.

ALGEBRAIC CIPHER

For theoretical reasons, it is useful to note that this cipher is a very simple algebraic cipher (i.e., it can be described by equations). However, the following description is introduced strictly for the theoretical insight it provides, not as an alternative method of ciphering.

Suppose each letter is described by two coordinates i and j which show its position in the alphabet table. Since we are using a 5 x 5 alphabet table, we will let i and j run from 0 to 4. For example, A = (0,0), B = (0,1), E = (0,4), F = (1,0), and Z = (4,4). When we do arithmetic on coordinates, we do the arithmetic "modulo 5." This means that when any arithmetic result is bigger than 4 or is negative, we add or subtract whatever multiple of 5 is needed to bring it into the range 0 to 4. Thus the final result of every arithmetic operation is 0, 1, 2, 3, or 4. Letters are acted on coordinate by coordinate:

$$(i,j) + (i',j') = (i + i', j + j'),$$

so $(2,3) + (3,4) = (0,2)$.

In any given trigraph, write the coordinate pairs of the plaintext letters as p_1, p_2, p_3, and the coordinate pairs of the ciphertext letters as c_1, c_2, c_3. Then ciphering can be described by three equations,

$$c_1 = -p_1 + p_2 + p_3 ,$$

$$c_2 = +p_1 - p_2 + p_3 ,$$

$$c_3 = +p_1 + p_2 - p_3 ,$$

and deciphering can be described by the equations

$$p_1 = (c_2 + c_3)/2 ,$$

$$p_2 = (c_1 + c_3)/2 ,$$

$$p_3 = (c_1 + c_2)/2 .$$

Note that in arithmetic modulo 5, dividing i by 2 means finding a number whose double is i. Division by 2 is always possible modulo 5, and is the same as multiplication by 3.

More compactly, using the ciphering equations is the same as multiplying (p_1, p_2, p_3) by the ciphering matrix, while using the deciphering equations is the same as multiplying (c_1, c_2, c_3) by the deciphering matrix, which is the inverse of the ciphering matrix:

$$\text{ciphering matrix} = \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}, \quad \text{deciphering matrix} = \begin{bmatrix} 0 & 3 & 3 \\ 3 & 0 & 3 \\ 3 & 3 & 0 \end{bmatrix} .$$

For example, if the plaintext trigraph is THE, and we write the coordinate pairs vertically instead of horizontally, then

$$\begin{matrix} T & H & E \end{matrix} \qquad\qquad \begin{matrix} T & L & W \end{matrix}$$

$$\begin{bmatrix} 3 & 1 & 0 \\ 3 & 2 & 4 \end{bmatrix} \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 4 \\ 3 & 0 & 1 \end{bmatrix}$$

Note that in the 2 x 3 matrix of coordinates for THE, each three-element row of plaintext coordinates can be multiplied by the ciphering matrix separately to give a row of ciphertext coordinates. Thus at the underlying level, this cipher maps triples of coordinates into triples of coordinates.

This gives rise to another feasible method of ciphering, which was pointed out by one of the referees. Since there are only 125 possible triples, one can make up two tables, one for ciphering and one for deciphering, showing how each of the 125 triples is transformed by the ciphering or deciphering matrix. Because this method of ciphering requires transformation of plaintext letters to coordinates and transformation of coordinates to ciphertext letters, as well as looking up entries in the table, it is not clear to me that it has any advantages over the method described in this paper. In addition, if one wishes to avoid possession of tables which might betray one's involvement in secret communication, the two tables must be recalculated for each new ciphering or deciphering session.

Since the fourth power of both the ciphering and deciphering matrices is the identity, applying the ciphering or deciphering equations four times in a row yields the original text, while applying either of them three times is the same as applying the other. Also, applying either of them twice yields a cipher for which ciphering and deciphering are identical.

This cipher is almost a special case of the cipher invented by L. S. Hill [3,4] (also see Kahn [5], pages 404-408). In Hill's cipher, the matrix is not fixed. Instead, the matrix and the alphabet table constitute the key. What makes the present cipher somewhat different is that the underlying elements belong to the two-dimensional vector space over the integers modulo 5, instead of the ring of integers modulo 26. The importance of this difference is that our vectors permit practical application of the required arithmetic operations in geometric fashion as described above, which does not hold true for the integers modulo 26 or 25.

RELATIONSHIP TO THE TRIFAIR CIPHER

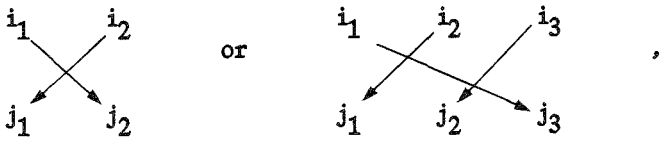
The Trifair cipher of "Zenith" [1,2], which is an extension of the Playfair, is also trigraphic, so it is interesting to see how it is related to our trigraph cipher. All three ciphers are presented geometrically, but can be described in terms of coordinates. They all assign a pair of coordinates to a letter in the same way. To compare them, it is convenient to write the coordinates vertically beneath the plaintext:

T H E A M B U S H W A S . . .

3 1 0 0 2 0 3 3 1 4 0 3 . . .

3 2 4 0 1 1 4 2 2 1 0 2 . . .

The Playfair breaks up the rows into pairs of columns, the Trifair into triples of columns, For each pair or triple, say



the coordinates are recombined into new pairs as shown by the arrows, and each new pair is taken as the coordinates of a ciphertext letter. (As pointed out in [2], it is easy to extend the Trifair to be an n-graph cipher simply by using longer blocks.) Our cipher breaks the columns up into triples like the Trifair does. What happens next, however, is very different. The triples (i_1, i_2, i_3) and (j_1, j_2, j_3) are each multiplied by the ciphering matrix, and each vertical pair in the resulting triple of columns is taken to be the coordinates of a ciphertext letter.

SOME PROPERTIES OF THE CIPHER

If a plaintext trigraph is permuted, then the corresponding ciphertext undergoes the corresponding permutation. Thus, for example, if plaintext ABC corresponds to ciphertext XYZ, then we have the following six correspondences:

ABC corresponds to XYZ,

BCA corresponds to YZX,

CAB corresponds to ZXY,

CBA corresponds to ZYX,

BAC corresponds to YXZ,

ACB corresponds to XZY.

Consider plaintext trigraphs Axy, where A is any fixed plaintext letter and x and y are variable. As x and y vary independently over all 25 possible letters each, the first ciphertext letter varies over all possible 25 values, and takes on each value exactly 25 times. Similar statements hold for plaintext trigraphs xAy and xyA, and also vice versa for ciphertext trigraphs Axy, xAy, and xyA.

Consider plaintext trigraphs ABx, where A and B are any fixed plaintext letters and x is variable. As x varies over all 25 possible letters, the first two ciphertext letters vary over 25 different pairs which have a fixed geometrical relationship. To illustrate this, consider the plaintext trigraph IFx. When x is the letter O, the first two ciphertext letters are LM. As x varies through all 25 values, the first two ciphertext letters vary through all pairs which have the same geometrical relationship in the table as LM, e.g., MN, NO, OP, PL, QR, RS, VW and DE. Similar statements hold for plaintext trigraphs AxB and xAB, and also vice versa for ciphertext trigraphs ABx, AxB, and xAB.

Trigraphs containing repeated letters deserve special consideration. If the plaintext trigraph consists of three equal letters, such as AAA, then the ciphertext is exactly the same. For this reason, I propose that such a trigraph should be avoided by inserting a null in the plaintext.

Nulls could also be used to avoid trigraphs containing pairs of equal letters, but this can lead to rather a lot of nulls so it may not be worthwhile. If the plaintext trigraph has a pair of equal letters, then the cipher text also has a pair of equal letters, and in the same positions. For example plaintext AAB becomes ciphertext BBE. Furthermore, as in this example, the unique letter in the plaintext trigraph is always the same as the repeated letter in the ciphertext. Incidentally, because of this property there is an advantage to using the cipher as described, instead of reversing the ciphering and

deciphering operations. As it stands, only a single letter in the plaintext may be deduced from a double letter in the ciphertext, but if the operations were reversed a pair of equal letters could be deduced.

3	6	2	5	4
5	3	2	4	6
1	1	*	1	1
6	4	2	3	5
4	5	2	6	3

Figure 6.

Straight lines in the table are important in practical ciphering and cryptanalysis. There are 30 of them, of which six run through any given square, as illustrated in Figure 6. It turns out that a plaintext trigraph and the corresponding ciphertext trigraph have a letter in common if and only if the trigraph letters (either plaintext or ciphertext) lie on a straight line. The three ways in which it can happen correspond to three rows of Figure 7. (i) If the plaintext trigraph consists of all equal letters, then all plaintext letters equal all ciphertext letters. (ii) If the plaintext trigraph has a repeated letter and a single letter, the plaintext single letter is equal to two ciphertext repeated letters, and no other equalities occur. (iii) If the plaintext trigraph consists of three distinct letters on a straight line, then exactly one plaintext letter is equal to the corresponding ciphertext letter, and no other equalities occur.

For any table, it is clear than any cyclic permutation of the rows or columns yields an equivalent key. Transposing the table (which makes each column into a row and each row into a column) does also. There are, however, other subtler transformations (including transposition as a special case) which also yield equivalent keys, namely what mathematicians call linear transformations of the "two-dimensional vector space over the integers modulo 5." It turns out that there are 480 such linear transformations (because this is the number of "nonsingular 2 x 2 matrices over the integers modulo 5"). All in all, each

table belongs to a class of 25 x 480 = 12,000 equivalent tables. The number of nonequivalent tables is $25!/12000 = 1.29 \times 10^{21}$, which is not so small as to pose a security hazard for a hand cipher.

TYPE		EXAMPLE(S)	NUMBER
All trigraphs			15,625
Trigraphs which lie on a straight line	Trigraphs with three equal letters	AAA	25
	Trigraphs with two equal letters	AAB ABA BAA	1,800
	Trigraphs with all distinct letters	ABC	1,800
Other trigraphs		ABH	12,000

Figure 7.

PRACTICAL CIPHERING

After trying several procedures for ciphering, the one I like best is this.

Case 1: The trigraph consists of three distinct letters, and it is not obvious that they lie on a straight line in the table. (This procedure is correct whether or not the letters lie on a straight line, and whether or not they are distinct, but faster procedures are available for special cases.)

Find a place in the table where the three letters occur reasonably close to one another. Put two fingers of your nonwriting hand on letters one and three. See what motion is required to go from letter one to letter two. Take this motion both forward and backward from letter three. This yields two letters, which you write down as cipher letters one and two.

Now see what motion is required to go from letter two to letter three. Take this motion both forward and backward from letter one. This yields two

letters. You check that the first one is the same as cipher letter two, already written down, and you write the other down as cipher letter three.

Case 2: The trigraph consists of three distinct letters, and you notice that they lie on a straight line in the table.

A straight line consists of five letters, which we think of as cyclically arranged, i.e., one end of the line is adjacent to the other end. Any three distinct letters must lie in one of two configurations: (i) if they lie in three adjacent positions, call the middle letter special; (ii) if two of them are adjacent while the third one is isolated, call the isolated letter special. Copy the special letter into the cipher trigraph, in the same position it occupies in the plaintext trigraph. The unused two letters of the straight line will be the other two cipher letters. It is only necessary to decide which one goes into which position.

Case 2(a): The special letter is adjacent to both other plaintext letters. The unused letter which is NOT adjacent to the plaintext letter goes into the position of that plaintext letter.

Case 2(b): The special letter is isolated. The unused letter which IS adjacent to a plaintext letter goes into the position of that plaintext letter.

Case 3: The trigraph consists of a repeated letter and a single letter.

Copy the single letter twice into the cipher trigraph, in the positions of the repeated plaintext letter. See what motion is required in the table to go from the single letter to the repeated letter, and take this motion forward from the repeated letter. This yields the remaining ciphertext letter, which you write down in the remaining position.

Case 4: The trigraph consists of three equal letters.

Insert a nonsense letter into the trigraph, and proceed to Case 3.

POSSIBLE VARIATIONS

All the standard variations, such as bisection and nonsense padding at the beginning and end, are available of course. Also, many of the variations available with the Playfair and other digraphic ciphers are available here. For example, this cipher can be seriated:

WRITET	KSOFTH	REEDLE
HETEXT	REEROW	NGTH—
INBLOC	SANDAG	———

and cipher the columns of the blocks. Also the unused letter (J in the examples) can be randomly inserted with appropriate frequency to hide the trigraph boundaries. (The temptation to use this null letter in between equal letters should, however, be resisted, since that would make it much easier to find which letter is the extra one.)

Ciphering by a Delastelle cipher is equivalent to ciphering by Playfair with two added steps: Before making the Playfair digraphic substitution, two different monalphabetic substitutions are applied to the two plaintext letters. After making the Playfair digraphic substitution, two more monalphabetic substitutions are applied to the two letters which result from the digraphic substitution. (Thus there are four potentially different monalphabetic substitution alphabets in all, though a more careful analysis shows that one of them can be omitted.) However, the four extra substitution steps are ingeniously combined with the digraphic substitution and create very little extra effort. A possible variation of our cipher is to apply three different monalphabetic substitution alphabets to the three plaintext letters before applying the trigraphic substitution, and then to apply three more different monalphabetic substitution alphabets to the result of the trigraphic substitution. This can be accomplished in a manner more or less reminiscent of the Delastelle, but the procedure is too awkward for practical use. Better is simply to make use of six simple substitution ciphers written out in conventional fashion.

A more limited version of this idea is simply to apply different fixed motions in the table, either to the plaintext letters before the trigraphic operation and/or to the ciphertext letters after the trigraphic operation. Using the algebraic form of this cipher, however, it can be seen that there is no point in using motions both before and after the trigraphic operation. The same results can be achieved by using motions only (say) after the trigraphic operation. It is also easy to see that there is no point in using motions for all three letters: the same results can be achieved by using them only for (say) the first and second letters. In this variation, plaintext trigraphs consisting of three equal letters would no longer correspond to ciphertext trigraphs with the same property, and ciphertext trigraphs with two equal letters would not immediately yield one plaintext letter.

Like the Playfair, the trigraph cipher can also give special treatment to trigraphs of special type, such as those containing equal letters or those

which lie on a straight line. For example, such trigraphs might be subjected to some fixed motion in the table, either after or instead of the normal trigraphic operation. The motion might be different for different types of special trigraphs. Because the number of trigraphs having two equal letters is 1800, and the number having three distinct letters on a straight line is also 1800, a more intricate possibility is to represent each trigraph of one type by a trigraph of the other type. A simple mapping which can be used for this purpose is the following. If the trigraph has two equal letters, let s be the single letter and r be the repeated letter, so the trigraph is either srr, rsr, or rrs. If the trigraph consists of three distinct letters on a straight line, let s be the letter which is special (as described in the section on Practical Ciphering), and let x and y be the other two letters in cyclic order around the trigraph, so the trigraph is either sxy, ysx, or xys.

Then

$$sxy \rightarrow sxx, \quad ysx \rightarrow xsx, \quad xys \rightarrow xxs$$

gives the mapping one way, and

$$srr \rightarrow srr', \quad rsr \rightarrow r'sr, \quad rrs \rightarrow rr's$$

gives the mapping the other way, where r' is defined as follows: if r is adjacent to s along the straight line, then r' is the other letter adjacent to s; and if r is not adjacent to s along the line, then r' is the other letter not adjacent to s.

CRYPTANALYSIS

How secure is this cipher against cryptanalysis? I invite readers to help find this out, using the problems provided below. All are normal modern English, taken from widely read writings. All use the simplest basic cipher, involving none of the variations. In some problems, word divisions are indicated.

To assure accuracy, short computer programs were used to encipher all plaintexts and to provide the trigraph counts. Other programs were used to decipher the ciphertexts and check them against the plaintexts. In addition, parts of all texts were ciphered by hand and checked manually against the computer encipherments. The computer programs, in "C" and in shell script for use on a Unix system, may be requested from the author.

One cannot expect the basic cipher to withstand computer attack by someone who knows the general system, but one of the variations, used as one step of a multistage cipher, might help provide some degree of security. I would hope that it offers greater security than a Playfair or Delastelle.

If the cipher trigraph and plaintext trigraph share the same letter in the same position, this is very useful in cryptanalysis. For example, suppose cipher EXY is identified as plaintext ENS. Then the five letters E, X, Y, N, S must form a straight line in the table. Furthermore, there is an equivalent table in which the five letters occur in the order XSENY. However, this case will be unusual, since only 1800 out of 15,625 trigraphs yield this kind of information.

ACKNOWLEDGEMENTS

I would like to thank Jim Reeds for many valuable discussions and the interest he showed in this work, especially for his insight into and computer experiments with methods of cryptanalysis. I would also like to thank the referees for bringing References [1,2] to my attention and for other helpful suggestions.

REFERENCES

1. "Zenith". 1983. (March - April). The Trifair Cipher. The Cryptogram. 49(2):3-5,8,23.

2. "Zenith". 1983. (May - June). Trifair Variations and Extensions. The Cryptogram. 49(3):5

3. Hill, L. S. 1929. Cryptography in an Algebraic Alphabet. American Mathematical Monthly. 36:306-312.

4. Hill, L. S. 1931. Concerning Certain Linear Transformation Apparatus of Cryptography. American Mathematical Monthly. 38:135-154.

5. Kahn, D. 1976. The Codebreakers. New York: Macmillan.

6. Gaines, H. F. 1956. Cryptanalysis: A Study of Ciphers and Their Solutions. New York: Dover. (Original edition: 1939. Elementary Cryptanalysis. American Photographic Publishing Co.)

CRYPTOGRAM 1 (WORD DIVISIONS MARKED)

KDV | CHN | YCM | FWP | CHN | RVQ | VCD | FNY | ZPI | AKD | TFX | NFK

BZF | EEG | IZM | KDV | QZR | GDK | QUP | GLH | KFD | YSB | HCN | YQM

HCN | DRF | EHF | XOA | MWB | WVQ | HCN | DBK | ISH | KDV | CSN | CBD

NFG | NGL | VQC | MEO | ZUY | HZB | UBZ | DRV | KDV | PAA | NFH | DRM

OBM | CIH | CYM | RQD | CTY | DKD | NZY | PQX | VAL | CNM | MEO | UAA

DVK | LTL | EHD | BLD | ROR | OKM | AUP | PEG | LUS | EXG | DBW | MBS

VFA | VCD | SQM | CVY | DKB | MAM | OWV | GBZ | QWN | ZEX | SFC | EXG

DBW | OXR | DCV | WBK | EXH | KDV | EAD | VLQ | VDW | OXR | PWR | VYU

OMA | HXF | DQZ | XPL | TNN | FNC | NPG | ROL | YUC | KWV | FYT | AOM

WBK | CXH

Its Trigraphs, With Frequencies, in Alphabetical Order

1	AKD	1	DBK	2	EXG	5	KDV	1	NZY	1	ROR	1	VQC
1	AOM	2	DBW	1	EXH	1	KFD	1	OBM	1	RQD	1	VYU
1	AUP	1	DCV	1	FNC	1	KWV	1	OKM	1	RVQ	2	WBK
1	BLD	1	DKB	1	FNY	1	LTL	1	OMA	1	SFC	1	WVQ
1	BZF	1	DKD	1	FWP	1	LUS	1	OWV	1	SQM	1	XOA
1	CBD	1	DQZ	1	FYT	1	MAM	2	OXR	1	TFX	1	XPL
2	CHN	1	DRF	1	GBZ	1	MBS	1	PAA	1	TNN	1	YCM
1	CIH	1	DRM	1	GDK	2	MEO	1	PEG	1	UAA	1	YQM
1	CNM	1	DRV	1	GLH	1	MWB	1	PQX	1	UBZ	1	YSB
1	CSN	1	DVK	3	HCN	1	NFG	1	PWR	1	VAL	1	YUC
1	CTY	1	EAD	1	HXF	1	NFH	1	QUP	2	VCD	1	ZEX
1	CVY	1	EEG	1	HZB	1	NFK	1	QWN	1	VDW	1	ZPI
1	CXH	1	EHD	1	ISH	1	NGL	1	QZR	1	VFA	1	ZUY
1	CYM	1	EHF	1	IZM	1	NPG	1	ROL	1	VLQ		

Multiple Trigraphs

5	KDV
3	HCN
2	CHN
2	DBW
2	EXG
2	MEO
2	OXR
2	VCD
2	WBK

Series of progressively stronger hints toward solution of Cryptograms 1 and 2 are provided below in cipher.

CRYPTOGRAM 2

THU OPR LEA MNY IXB GSU LQN IVI FXK KFE SZB QWR

PCT HLQ RGX HIW CLU KFE MNF UPF ONA BLA LNZ MSB

KFE YMQ LPA QTH AWH KKF UPF BGH LUR GWT OMW BEG

TFG WPC MKN XRR NZL MWR SBM GWT OMW BEG CLL BSL

NGY YPH ZLC GNL RQR VIB CFN HVY XQH XGF DXP PTD

CPG SOG HXR EKF LRQ KFE QGR XRR IVX AVP BKN ZEO

LSE KEQ TGA RDU MMD FXU SYK YHY XQI XDG ULZ GQL

SKG EAE QGR XRR NZL OMZ GPX LLA ZLC GNL RQR UPF

ANG YHT SZO VII FXK OLS NZL TBO ZPC ENW EGW IWE

HXR EOM MDN BKY MNE QEW OHZ VAN HIZ RXK YDV GKV

NEZ PFD MMD TTH MWC EEF YNQ FZG QNC FUC KNL MOX

IHY WKR PBY WCW ORK YNL UZX LNZ DNK XOI DXP LRN

Its Trigraphs, With Frequencies, in Alphabetical Order

1	ANG	1	EEF	1	HIZ	1	LPA	1	MWR	1	QEW	1	TBO	1	XGF
1	AVP	1	EGW	1	HLQ	1	LQN	1	NEZ	2	QGR	1	TFG	1	XOI
1	AWH	1	EKF	1	HVY	1	LRN	1	NGY	1	QNC	1	TGA	1	XQH
2	BEG	1	ENW	2	HXR	1	LRQ	3	NZL	1	QTH	1	THU	1	XQI
1	BGH	1	EOM	1	IHY	1	LSE	1	OHZ	1	QWR	1	TTH	3	XRR
1	BKN	1	FUC	1	IVI	1	LUR	1	OLS	1	RDU	1	ULZ	1	YDV
1	BKY	2	FXK	1	IVX	1	MDN	2	OMW	1	RGX	3	UPF	1	YHT
1	BLA	1	FXU	1	IWE	1	MKN	1	OMZ	2	RQR	1	UZX	1	YHY
1	BSL	1	FZG	1	IXB	2	MMD	1	ONA	1	RXK	1	VAN	1	YMQ
1	CFN	1	GKV	1	KEQ	1	MNE	1	OPR	1	SBM	1	VIB	1	YNL
1	CLL	2	GNL	4	KFE	1	MNF	1	ORK	1	SKG	1	VII	1	YNQ
1	CLU	1	GPX	1	KKF	1	MNY	1	PBY	1	SOG	1	WCW	1	YPH
1	CPG	1	GQL	1	KNL	1	MOX	1	PCT	1	SYK	1	WKR	1	ZEO
1	DNK	1	GSU	1	LEA	1	MSB	1	PFD	1	SZB	1	WPC	2	ZLC
2	DXP	2	GWT	1	LLA	1	MWC	1	PTD	1	SZO	1	XDG	1	ZPC
1	EAE	1	HIW	2	LNZ

Multiple Trigraphs

4	KFE
3	NZL
3	UPF
3	XRR
2	BEG
2	DXP
2	FXK
2	GNL
2	GWT
2	HXR
2	LNZ
2	MMD
2	OMW
2	QGR
2	RQR
2	ZLC

SOLUTION HINTS IN CIPHER, USING NORMAL ALPHABET AS KEY

Cryptogram 1

IMV HCK ZCO PAX MLT CAB OSQ MWS TSS IET IAB LRT
GYT HZB SLT EOV FUG WHF EAX CKD ZGD IVN EEW LTO
RFQ XNN AKZ WQL EBV WNO YFX BCF UPS VSI VCF IGD
YML LRP TSS IET IBA SUP PQC WOQ AVD HSU TSS IMV
HCK ZCO DCV MVS FBR QKO SHE IVR BBK LBC IIR HUF
NRZ ENH RQU OZQ HBC VPM ZOK SMS FVE DYO DXC TLW
GWC VKR FCV UGP SPM BBK VRP BVP SMW CHP XYI EPC
UFV KKB CPU LUQ MQI IPT WLE TUX RWX GRT FYL WLV
TRY CKH WDK FRT KCH SHK XED IZF RNT XCE XYI EPC
UFV QTF ITR VFC AVA YHR RQN

Cryptogram 2

TLW BEZ XPC MVI PRV DAY OIU BGV NCZ RPH SMW URR
TLW HEB XLE VFE BVC UUL RUT LBK BLZ KAZ LQO CKD
YNP FKB VAD QKW IMV SUS KCD NMY CVB VGW RFR NKC
HAY MWS BFY VAM SUP COB CHY XLT IRV KBA FKB CDA
IBI ZOC TLW TDL NUX RFR NKC HAY MWS TTS BNC CPU
ZGD CAB FDT IID DLP QCB GVB QTF ITR VFC AVA YHR
RQN FCK NAW MVU WDK FRT KCH ACZ AEW IRX OMQ CFB
LCP TLW AKD PXM XIZ PUQ ZSH XKQ DPC EBV XON FKB
KZK CHP CBE OMH ROV DME PDY POW PEH KLO CSI

CRYPTOGRAM 3 (WORD DIVISIONS MARKED)

LGS | TNH | WLG | QUO | GQR | UNM | OQA | GQR | TVR | OSW | DPS | SPX |

RVB | FHX | PWK | VDF | POO | BQP | MBX | XXY | OWF | GLR | ENV | ZXE |

VTB | BXE | VRD | KXN | YXH | CQG | STR | URT | VUZ | QRU | BPS | AQN |

MIM | SWO | ZHM | CNT | YRH | SUP | TNH | OKT | WHE | MBN | TRT | RGS |

UQU | CNT | LHT | CSH | LZD | SHA | DZD | THP | QTK | ZUU | OQA | OCT |

QKC | YXH | XNH | MWG | YRD | TNH | TCS | FIX | LFW | HIY | YLK | QUO |

TPO | CYD | IRY | XWK | UXN | RGR | UQN | QKO | YBM | GMI | SDP | RVT |

PNF | XUM | XWK | UXN | RGR | UQN | SMP | VUZ | IBI | VIB | OKW | WHK |

CQG | XWK | UXN | RGR | UQN | SMP | VUZ | IBI | FLD | OAB | ZUD | SDP |

SYP | PKA | EBD | KXN | NEF | ELH | GUF | BAQ | LFW | EYX | LHX | BQP |

IOI | GBQ | VWU

Multiple Trigraphs

3 RGR
3 TNH
3 UQN
3 UXN
3 VUZ
3 XWK
2 BQP
2 CNT
2 CQG
2 GQR
2 IBI
2 KXN
2 LFW
2 OQA
2 QUO
2 SDP
2 SMP
2 YXH

Its Trigraphs, With Frequencies, in Alphabetical Order

1 AQN 1 FHX 1 LGS 1 OSW 1 RVT 1 TVR 1 WLG
1 BAQ 1 FIX 1 LHT 1 OWF 2 SDP 1 UNM 1 XNH
1 BPS 1 FLD 1 LHX 1 PKA 1 SHA 3 UQN 1 XUM
2 BQP 1 GBQ 1 LZD 1 PNF 2 SMP 1 UQU 3 XWK
1 BXE 1 GLR 1 MBN 1 POO 1 SPX 1 URT 1 XXY
2 CNT 1 GMI 1 MBX 1 PWK 1 STR 3 UXN 1 YBM
2 CQG 2 GQR 1 MIM 1 QKC 1 SUP 1 VDF 1 YLK
1 CSH 1 GUF 1 MWG 1 QKO 1 SWO 1 VIB 1 YRD
1 CYD 1 HIY 1 NEF 1 QRU 1 SYP 1 VRD 1 YRH
1 DPS 2 IBI 1 OAB 1 QTK 1 TCS 1 VTB 2 YXH
1 DZD 1 IOI 1 OCT 2 QUO 1 THP 3 VUZ 1 ZHM
1 EBD 1 IRY 1 OKT 3 RGR 3 TNH 1 VWU 1 ZUD
1 ELH 2 KXN 1 OKW 1 RGS 1 TPO 1 WHE 1 ZUU
1 ENV 2 LFW 2 OQA 1 RVB 1 TRT 1 WHK 1 ZXE
1 EYX

CRYPTOGRAM 4

ULL GIM SAA YIQ SQG FEH TGM NVQ EUL FUU BLD CRF

BQC VWO AUG DZU QCL DVB DKX BVN CER HHD RWR GYA

CHV HFQ XGH PFZ WZR VXH XIZ UOP RTI WIK HGX QLX

OTY NMN EBO RTM MQX FKY DHX MEU FPK LWU SGA EEY

HFB RDZ IET WZR TGM VCE CER HHD RZF VBV VDF UQB

HKL XXH UDX YMP KRD FOH WIT ERC GMA KYI BPV XKP

XKI VBV IKI HSB BAR ONI ZRD UZM VBH RZW MAO BQC

BDF POW OTG APS WMF LCD VBV PAR MGZ PFZ PUQ

Its Trigraphs, With Frequencies, in Alphabetical Order

1 APS 1 DVB 1 GYA 1 MAO 1 PUQ 2 TGM 1 WIK
1 AUG 1 DZU 1 HFB 1 MEU 1 QCL 1 UDX 1 WIT
1 BAR 1 EBO 1 HFQ 1 MGZ 1 QLX 1 ULL 1 WMF
1 BDF 1 EEY 1 HGX 1 MQX 1 RDZ 1 UOP 2 WZR
1 BLD 1 ERC 2 HHD 1 NMN 1 RTI 1 UQB 1 XGH
1 BPV 1 EUL 1 HKL 1 NVQ 1 RTM 1 UZM 1 XIZ
2 BQC 1 FEH 1 HSB 1 ONI 1 RWR 1 VBH 1 XKI
1 BVN 1 FKY 1 IET 1 OTG 1 RZF 3 VBV 1 XKP
2 CER 1 FOH 1 IKI 1 OTY 1 RZW 1 VCE 1 XXH
1 CHV 1 FPK 1 KRD 1 PAR 1 SAA 1 VDF 1 YIQ
1 CRF 1 FUU 1 KYI 2 PFZ 1 SGA 1 VWO 1 YMP
1 DHX 1 GIM 1 LCD 1 POW 1 SQG 1 VXH 1 ZRD
1 DKX 1 GMA 1 LWU

Multiple Trigraphs

3 VBV
2 BQC
2 CER
2 HHD
2 PFZ
2 TGM
2 WZR