WIKIPEDIA

Trifid cipher

The **trifid cipher** is a classical cipher invented by Félix Delastelle and described in 1902.[1] Extending the principles of Delastelle's earlier bifid cipher, it combines the techniques of fractionation and transposition to achieve a certain amount of confusion and diffusion: each letter of the ciphertext depends on three letters of the plaintext and up to three letters of the key.

The trifid cipher uses a table to *fractionate* each plaintext letter into a trigram,[2] mixes the constituents of the trigrams, and then applies the table in reverse to turn these mixed trigrams into ciphertext letters. Delastelle notes that the most practical system uses three symbols for the trigrams:[3]

> In order to split letters into three parts, it is necessary to represent them by a group of three signs or numbers. Knowing that n objects, combined in trigrams in all possible ways, give $n \times n \times n = n^3$, we recognize that three is the only value for n; two would only give $2^3 = 8$ trigrams, while four would give $4^3 = 64$, but three give $3^3 = 27$.

Description

As discussed above, the cipher requires a 27-letter mixed alphabet: we follow Delastelle by using a plus sign as the 27th letter.[4] A traditional method for constructing a mixed alphabet from a key word or phrase is to write out the unique letters of the key in order, followed by the remaining letters of the alphabet in the usual order.[5] For example, the key FELIX MARIE DELASTELLE yields the mixed alphabet FELIXMARDSTBCGHJKNOPQUVWYZ+.

To each letter in the mixed alphabet we assign one of the 27 trigrams (111, 112, …, 333) by populating a 3 × 3 × 3 cube with the letters of the mixed alphabet, and using the Cartesian coordinates of each letter as the corresponding trigram.

Layer 1					**Layer 2**					**Layer 3**			
	1	**2**	**3**			**1**	**2**	**3**			**1**	**2**	**3**
1	F	E	L		**1**	S	T	B		**1**	O	P	Q
2	I	X	M		**2**	C	G	H		**2**	U	V	W
3	A	R	D		**3**	J	K	N		**3**	Y	Z	+

From this cube we build tables for enciphering letters as trigrams and deciphering trigrams as letters:

Enciphering alphabet				Deciphering alphabet		
A = 131	J = 231	S = 211		111 = F	211 = S	311 = O
B = 213	K = 232	T = 212		112 = E	212 = T	312 = P
C = 221	L = 113	U = 321		113 = L	213 = B	313 = Q
D = 133	M = 123	V = 322		121 = I	221 = C	321 = U
E = 112	N = 233	W = 323		122 = X	222 = G	322 = V
F = 111	O = 311	X = 122		123 = M	223 = H	323 = W
G = 222	P = 312	Y = 331		131 = A	231 = J	331 = Y
H = 223	Q = 313	Z = 332		132 = R	232 = K	332 = Z
I = 121	R = 132	+ = 333		133 = D	233 = N	333 = +

The encryption protocol divides the plaintext into groups of fixed size (plus possibly one short group at the end): this confines encoding errors to the group in which they occur,[6] an important consideration for ciphers that must be implemented by hand. The group size should be coprime to 3 to get the maximum amount of diffusion within each group: Delastelle gives examples with groups of 5 and 7 letters. He describes the encryption step as follows:[7]

> We start by writing *vertically* under each letter, the numerical trigram that corresponds to it in the enciphering alphabet: then proceeding *horizontally* as if the numbers were written on a single line, we take groups of three numbers, look them up in the deciphering alphabet, and write the result under each column.

For example, if the message is *aide-toi, le ciel t'aidera*, and the group size is 5, then encryption proceeds as follows:

```
a i d e-t   o i l e c   i e l t'a   i d e r a
1 1 1.1 2   3 1 1.1 2   1 1 1.2 1   1 1 1.1 1
3.2 3 1.1   1.2 1 1.2   2.1 1 1.3   2.3 1 3.3
1 1.3 2 2   1 1.3 2 1   1 2.3 2 1   1 3.2 2 1
F M J F V   O I S S U   F T F P U   F E Q Q C
```

In this table the periods delimit the trigrams as they are read horizontally in each group, thus in the first group we have 111 = F, 123 = M, 231 = J, and so on.

Notes

1. Delastelle, pp. 101–3.
2. Hence the name *trifid*, which means "divided into three parts" (*Oxford English Dictionary*).
3. Delastelle, p. 101: "Afin de pouvoir fragmenter les lettres en trois parties…"
4. Delastelle, p. 102: "Mais l'alphabet français ne contenant que vingt-six lettres…"
5. See substitution cipher.
6. Gaines, p. 210.
7. Delastelle, p. 102: "Nous commençons par inscrire *verticalement* sous chaque lettre…"

References

- Delastelle, Félix (1902). *Traité Élémentaire de Cryptographie* (https://archive.org/details/8VSUP3207b). Paris: Gauthier-Villars.
- Gaines, Helen (1939). *Cryptanalysis: A Study of Ciphers and Their Solution*. New York: Dover.