WIKIPEDIA

# Bifid cipher

In classical cryptography, the **bifid cipher** is a cipher which combines the Polybius square with transposition, and uses fractionation to achieve diffusion. It was invented around 1901 by Felix Delastelle.

## Contents

## Operation

First, a mixed alphabet Polybius square is drawn up, where the I and the J share their position:

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

The message is converted to its coordinates in the usual manner, but they are written vertically beneath:

```
F L E E A T O N C E
4 4 3 3 3 5 3 2 4 3
1 3 5 5 3 1 2 3 2 5
```

They are then read out in rows:

```
4 4 3 3 3 5 3 2 4 3 1 3 5 5 3 1 2 3 2 5
```

Then divided up into pairs again, and the pairs turned back into letters using the square:

```
44 33 35 32 43 13 55 31 23 25
U  A  E  O  L  W  R  I  N  S
```

In this way, each ciphertext character depends on two plaintext characters, so the bifid is a digraphic cipher, like the Playfair cipher. To decrypt, the procedure is simply reversed.

Longer messages are first broken up into blocks of fixed length, called the period, and the above encryption procedure is applied to each block. One way to detect the period uses bigram statistics on ciphertext letters separated by half the period. For even periods, *p*, ciphertext letters at a distance of *p/2* are influenced by *two* plaintext letters, but for odd periods, *p*, ciphertext letters at distances of *p/2* (rounded either up or down) are influenced by *three* plaintext letters. Thus, odd periods are more secure than even against this form of cryptanalysis, because it would require more text to find a statistical anomaly in trigram plaintext statistics than bigram plaintext statistics.[1]

## See also

- Other ciphers by Delastelle:
  - four-square cipher (related to Playfair)
  - trifid cipher (similar to bifid)

## References

1. http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-bifid-cipher/

## External links

- Online Bifid Encipherer/Decipherer with polybius square generator (http://rumkin.com/tools/cipher/bifid.php)