WIKIPEDIA
The Free Encyclopedia

Transposition cipher

Columnar transposition

In the middle of the 17th century, Samuel Morland introduced an early form of columnar transposition. It was further developed much later, becoming very popular in the later 19th century and 20th century, with French military, Japanese diplomats and Soviet spies all using the principle.

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the keyword `ZEBRAS` is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword `ZEBRAS` and the message `WE ARE DISCOVERED. FLEE AT ONCE`. In a regular columnar transposition, we write this into the grid as follows:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
```

providing five nulls (`QKJEU`), these letters can be randomly selected as they just fill out the incomplete columns and are not part of the message. The ciphertext is then read off as:

```
EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
```

In the irregular case, the columns are not completed by nulls:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E
```

This results in the following ciphertext:

```
EVLNA CDTES EAROF ODEEC WIREE
```

To decipher it, the recipient has to work out the shape of the enciphering grid by dividing the message length by the key length to find the number of rows in the grid. The length of the grid's last line is given by the remainder. The key is written above the grid, and the ciphertext is written down the columns of the grid in the order given by the letters of the key. The plaintext appears on the rows. A partial decipherment of the above ciphertext, after writing in the first column:

```
6 3 2 4 1 5
. . . . E .
. . . . V .
. . . . L .
. . . . N .
.
```

In a variation, the message is blocked into segments that are the key length long and to each segment the same permutation (given by the key) is applied. This is equivalent to a columnar transposition where the read-out is by rows instead of columns.

Columnar transposition continued to be used for serious purposes as a component of more complex ciphers at least into the 1950s.

-