Columnar transposition is a technique used for scrambling the order of letters in a message to encrypt.

History

The technique was first described by the Bazeries in 1901, although it is also said to date back to ancient times. During World War I and II, columnar transposition was widely used by military forces to encrypt messages. Columnar transposition is also used in combination with other encryption techniques to increase security.

Encryption Process

The plaintext message is first written out in rows of a fixed length. The columns are then rearranged according to a secret key of numbers or letters. The ciphertext is read off row by row to create the final encrypted message. For example, the plaintext message "HELLO WORLD" with a key "3142" would be encrypted as "EOLHWLLROD"

Here's an example of the encryption process for the plaintext message -

"THIS IS MY WIKI ABOUT CYPHERS" with the key "SECURE":

plaintext message in rows of the length of "SECURE" (6):

S E C U R E

T H I S I

S M Y W I

K I A B O

U T C Y P

H E R S

Rearrange the columns according to the key "SECURE":

E U R S C

I T H I S

Y S M W I

B K I A O

P T U C Y

R E H S

Read off the ciphertext row by row:

ITSYBKPURTCSMWHIOHEAISYRE

Security

Columnar transposition is vulnerable to frequency analysis and known plaintext attacks. These attacks can be mitigated by using a longer and more complex key, increasing the length of the plaintext message, and combining columnar transposition with other encryption techniques. Overall, columnar transposition isn't the best method for encryption but can be fun for enthusiasts.