

Transposition Cipher

Transposition cipher (also called permutation cipher): transforms a message by rearranging the positions of the elements of the message without changing the identities of the elements. It is widely used in the constructions of modern block ciphers.

❑ **Columnar Transposition:** It is one of transposition ciphers. In which, 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.

Example: Use columnar transposition cipher to encrypt the following message


plaintext: defend the east wall of the castle

key: GERMAN

Solution: To encrypt the above message using the given key, we do the following steps:

- (1) The row length that is used is the same as the length of the keyword, i.e (6).
- (2) We write out the plaintext in a row-wise.

Note that the plaintext has been padded with (x) so that it neatly fits in a rectangle. This is known as a **regular columnar transposition**. An **irregular columnar transposition** leaves these characters blank, though this makes decryption slightly more difficult.



G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e	x	x

(3) We reorder the columns alphabetically according to the key letters.

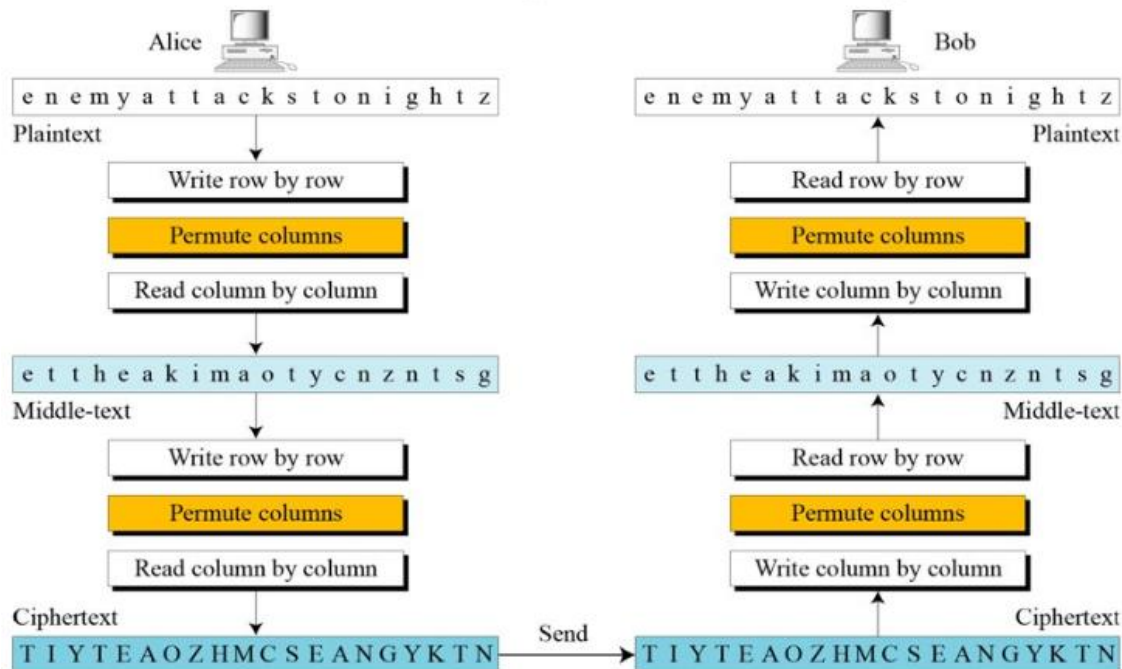
(4) The ciphertext is read off along the columns.

ciphertext: nalcxehwttddtfseeleedsoaxfeahl

Note: The keys can be composed of either letters or numbers.

A	E	G	M	N	R
n	e	d	e	d	f
a	h	t	e	s	e
l	w	t	l	o	a
c	t	f	e	a	h
x	t	s	e	x	l

❑ **Double Transposition:** a single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns and then trying to find the plaintext content. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.



Double Columnar Transposition Cipher (Conti.)

To perform a Double Columnar Transposition we write out the key as column header. The key is numbered in alphabetical order. If two letters of the key are the same, the first in the key gets the lowest number.

Example:

Plaintext : THIS IS A SECRET MESSAGE

1st Columnar Key: LEONARDO

2nd Columnar Key: DAVINCI

Note that, in reality, two keywords with a length up to 20 letters each were used to encipher a message.

The plaintext is written out in successive rows beneath the headers:

L	E	O	N	A	R	D	O
4	3	6	5	1	8	2	7

T	H	I	S	I	S	A	S
E	C	R	E	T	M	E	S
S	A	G	E				

Decode message is read off in columns in order of the headers:

First ciphertext: ITAEHCATESSEEIRGSSSM

Next, we write it down again, in successive rows, and perform the second transposition.

D	A	V	I	N	C	I
3	1	7	4	6	2	5

I	T	A	E	H	C	A
T	E	S	S	E	E	I
R	G	S	S	S	M	

Again, we read off the ciphertext by the column and write down the text in groups of five:

The final cipher text: TEGCE MITRE SSAIH ESASS

To decode the message we first use the 2nd columnar key and then the 1st columnar key. We write out the header and reconstruct the table with long and short rows. We fill in the code column by column in the order of the key.

Classical Ciphers: Usefulness and Security

- Polyalphabetic ciphers and transposition ciphers are stronger than simple substitution ciphers. However, if the key is short and the message is long, then various cryptanalysis techniques can be applied to break such ciphers.
- Classical ciphers, even simple substitution ciphers can be secure in a *very strong sense* if the use of cryptographic keys follows certain conditions. In fact, with the proper key usages, simple substitution ciphers are widely used in cryptographic systems and protocols.