Transposition Cipher Techniques in Cryptography

Transposition Ciphers are an essential part of cryptography that uses systematic shuffling of plain text characters or bits to secure data by altering their positions based on some defined way or algorithm. Moreover, unlike substitutive codes where different letters substitute others, in these, you just shift about original letters hence it does not at all look like any message.

The utilization of these strategies in relatively primitive encryption methodologies, which in their simplicity formed the basis for more sophisticated forms of encoding is shown by other historical ciphers like Rail Fence and Columnar Transposition. Columnar transpositions are still being explored and employed today within complex systems. For instance, such as those involving hierarchical structures that are meant to increase message secrecy through extra levels of obscurity.

In this article, we will learn about techniques used to encrypt the message earlier. This article will provide details about the Transposition Cipher Technique. Then we are going to explore various types of Transposition Cipher Technique.

Transposition Cipher Technique

The Transposition Cipher Technique is an encryption method used to encrypt a message or information. This encryption method is done by playing with the position of letters of the plain text. The positions of the characters present in the plaintext are rearranged or shifted to form the ciphertext. It makes use of some kind of permutation function to achieve the encryption purpose. It is very easy to use and so simple to implement.

Types of Transposition Cipher Techniques

There are three types of transposition cipher techniques

- Rail Fence Transposition Cipher
- Block (Single Columnar) Transposition Cipher
- Double Columnar Transposition Cipher

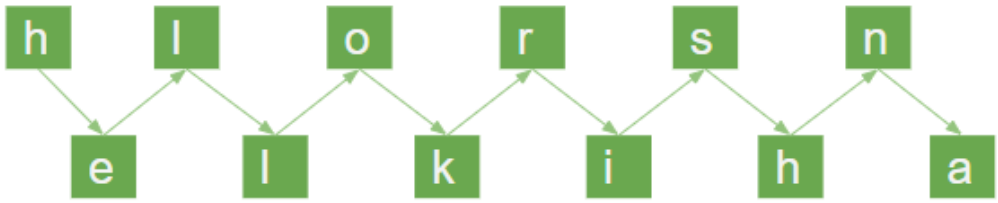
Rail Fence Transposition Cipher

Rail Fence Transposition cipher technique is the simplest transposition cipher technique**its**. It is also termed as a zigzag cipher. It gets its name from the way through which it performs encryption of plain text. The steps to get cipher text with the help of the Rail Fence Transposition cipher technique are as follow-

Technique of Rail Fence Transposition Cipher

Example: The plain text is "Hello Krishna"

Now, we will write this plain text in the diagonal form:



Rail Fence Transposition Cipher
Now, following the second step we get our cipher text.
Cipher Text = "rsnelkiha"

Block (Single Columnar) Transposition Cipher

Block Transposition Cipher is another form of Transposition Cipher which was used to encrypt the message or information. In this technique, first, we write the message or plaintext in rows. After that, we read the message column by column. In this technique, we use a keyword to determine the no of rows.

- Step 1: First we write the message in the form of rows and columns, and read the message column by column.
- Step 2: Given a keyword, which we will use to fix the number of rows.
- Step 3: If any space is spared, it is filled with null or left blank or in by (_).
- Step 4: The message is read in the order as specified by the keyword.

Given Text = KRISHNA RANJAN

Keyword = NICK

N	I	C	K
4	2	1	3
K	R	I	S
H	N	A	_
R	A	N	J
A	N	_	_

Cipher Text = IAN_RNANS_J_KHRA

Block Columnar Transposition Cipher
For example: The plaintext is "KRISHNA RANJAN"
Now we will write the plaintext in the form of row and column.
Cipher Text = IAN_RNANS_J_KHRA

Double Columnar Transposition Cipher

Double Columnar Transposition Cipher is another form of Transposition Cipher Technique. It is just similar to the columnar transposition technique. The main objective of using a Double Columnar Transposition Cipher is to encrypt the message twice. It makes use of the Single Columnar Transposition technique but uses two times. It can use the same or different secret keys. The output obtained from the first encryption will be the input to the second encryption.

- Step 1: First we write the message in the form of rows and columns, and read the message column by column.
- Step 2: Given a keyword, which we will use to fix the number of rows.

Given Text = GEEKSFORGEEKS

Keyword = NICK **Keyword 2= BOAT**

N	I	C	K
4	2	1	3
G	E	E	K
S	F	O	R
G	E	E	K
S	_	_	_

Double Columnar Transposition Cipher:Step 1

- Step 3: If any space is spared, it is filled with null or left blank or in by (_).

Now applying keyword 2:

Given Text = GEEKSFORGEEKS

Keyword = NICK **Keyword 2= BOAT**

N	I	C	K
1	2	3	4
E	E	K	G
O	F	R	S
E	E	K	G
_	_	_	S

Cipher Text = EOE_EFE_KRK_GSGS

Double Columnar Transposition Cipher: Step 2

- Step 4: The message is read in the order in by the keyword.

Now apply step 3:

Given Text = GEEKSFORGEEKS

Keyword = NICK **Keyword 2= BOAT**

B	O	A	T
2	3	1	4
G	E	E	K
S	F	O	R
G	E	E	K
S	_	_	_

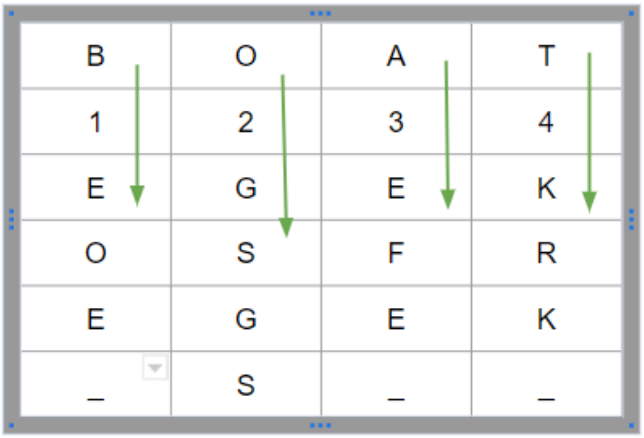
Cipher Text = EOE_GSGSEFE_KRK_

Double Columnar Transposition Cipher: Step 3

- Step 5: Then the output from the first encryption is input to the second.
- Step 6: Now the message is read in Technique in the order specified by the second keyword.

Given Text = GEEKSFORGEEKS

Keyword = NICK **Keyword 2= BOAT**



Cipher Text = EOE_GSGSEFE_KRK_

Double Columnar Transposition Cipher: Step 4
The Cipher Text is: **"S_J_IAN_RNANKHRA"**

Conclusion

In conclusion, Transposition Cipher Techniques are the techniques which are used for encryption of plaintext or messages. There are several types of Transposition Cipher Techniques which include Rail Fence Transposition Cipher, Block (Single Columnar) Transposition Cipher, and Double Columnar Transposition Cipher. Each technique has its way of encrypting the plaintext.