**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, we 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.

**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. 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 theRail Fence Transposition cipher technique are as follow-

**Technique of Rail Fence Transposition Cipher**

**Example**: The plain text is “Hello Krishna”

We will write this plain text in the diagonal form:

h l o r s n

e l k I h a

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.

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