# Transposition Ciphers

In Cryptography, a Transposition Cipher is a method of encryption by which the positions held by units of plaintext are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

## Types of Transposition Ciphers:

1) Keyless → Railfence
2) Keyed → Single Columnar
   → Double Columnar

## Railfence Cipher

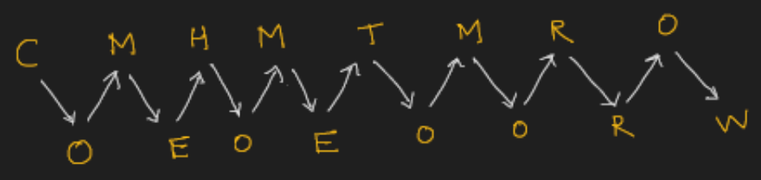
The Rail Fence Technique is an example of transposition. It uses a simple algortihm.

1. Write down the plaintext message as a sequence of diagonals.
2. Read the plaintext written in step 1 as a sequence of rows.

The Rail Fence technique involves writing the plaintext message as a sequence of diagonals and then reading it row by row to produce ciphertext.

Plaintext: Come Home Tomorrow

Encryption:



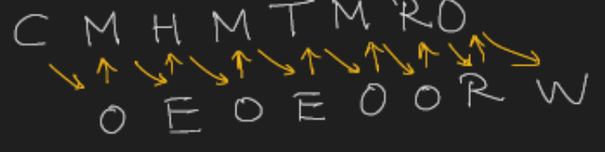

Ciphertext: CMHMTMRO OEOE OO R W

## Decryption:

- Count the number of characters in the ciphertext. Divide it into 2 halves.
- If number of characters are ODD , then add 1 character more in the upper half. For ex: If there are 9 Characters in the CT, the upper half will have 5 characters and 4 in the lower half respectively.
- Write the Characters of respective halves along the rows.
- Read them diagonally and retrieve the Plaintext.

Ciphertext: CMHMTMRO OEOE OO R W

1. Count the no. of characters : 16
2. Divide into 2 halves of 8 characters each.
3. Write the halves one above the other




4. Read them diagonally
5. COME HOME TO MO RROW