

**Department of Computer Engineering**

**LMS Assignment 9**

Q. 1 What is Keyless Transposition Cipher? Give an example of rail fence cipher. [5M]

A transposition cipher does not substitute one symbol for another instead it changes the location of the symbols.

Keyless Transportation cipher is simple one which is keyless. In first method the text is written into a table column by column and then row by row. In the second method the text is written into the table row by row and then transmitted column by column.

Example of a Keyless transposition cipher using first method is rail fence cipher.

Example- Encrypt: NOTHING IS AS IT SEEMS

First write it on two lines in a zig-zag pattern (or rail fence). The cipher text is produced by transcribing the first row followed by the second row.In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt