TRANSPOSITION TECHNIQUES

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

RAIL FENCE CIPHER

It is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2,

We write the message as follows:

```
m   e   a   t   e   c   o   l   o   s
  e   t   t   h   s   h   o   h   u   e
```

The encrypted message Cipher text MEATECOLOSETTHSHOHUE

ROW TRANSPOSITION CIPHERS-

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

```
PT =  m e e t a t t
      h e s c h o o
      l h o u s e
```

CT = ESOTCUEEHMHLAHSTOETO

Demerits

- Easily recognized because the frequency is same in both plain text and cipher text.
- Can be made secure by performing more number of transpositions.

STEGANOGRAPHY

In Steganography, the plaintext is hidden. The existence of the message is concealed. For example, the sequence of first letters of each word of the overall message spells out the hidden message.

Various other techniques have been used historically; some examples are the following:

- **Character marking:** Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
- **Invisible ink:** A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
- **Pin punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawback

- It requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless