

Topic-9

1/1

* Transposition Cipher :-

- Transposition Cipher is a cryptographic algorithm, where the order of alphabets in the plain text is rearranged to form a cipher text.
- Mapping Plain Text into cipher text using transposition technique is called Transposition Cipher.
- In this, Plain Text characters are shifted in some regular pattern to form cipher text.
- The Transposition Ciphers have list of transposition techniques:-

(a) Columnar Transposition Cipher :-

- In this, each character in the Plain Text is written horizontally with specified alphabet width.
- The cipher is written vertically, which creates an entirely different cipher text.

- It is form of transposition cipher in which plain text represent in matrix form.
- Spare spaces are filled with nulls or placed by -
- Encryption Process:

Plain Text :- TREE IS GREEN

Keyword = HACK

length of keyword = 4

order of alphabets

in HACK = 3124

H	A	C	K
3	1	2	4
T	R	E	E
-	I	S	-
G	R	E	E
N	-	-	-

→ Decryption Process:

Cipher Text :- RIR ESE T GNE E

(b) Rail Fence Technique:

In this, the Plain Text is written down as a sequence of diagonals and then read off as a sequence of rows.

example: "all the best for exams".

a l h b s f r x m
l t e e t o e a s

encrypted message is :-

A L H B S F R X M L T E E T O E A S.