TRANSPOSITION TECHNIQUES

Transposition technique is a cryptographic technique that converts the plain text to cipher text by performing permutations on the plain text i.e change the position of each character of plain text for each round

Transposition techniques :

1. Rail-Fence Technique
2. Columnar Transposition Technique
3. Vernam Cipher

1) Rail-Fence Technique:

Rail-Fence is the simple Transposition technique which involves writing plain text as a sequence of diagonals and then reading it row by row to produce the cipher text.

→ In this instead of key there will be a depth value

Example

Plain-Text = MEET ME AFTER THE PARTY

Depth = 3

Given the depth is 3 so construct a table with depth 3

M								A				R				E				R		
	E		T		M				F		E				H				A		T	
		E				E				T				T				P				Y

After constructing the table write the text in row wise so that the cipher text will be

Cipher-Text = M _ARERETM_FE_H_ATEETTPY

2) Columnar Transposition Cipher

i. The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.

ii. Width of the rows and the permutation of the columns are usually defined by a keyword.

Example
Key = HACK
Plain-Text = CRYPTOGRAPHY

Now the size of key is 4 we need to form a table of 4 columns and write all the letters in the plain text into the table

H	A	C	K
C	R	Y	P
T	O	G	R
A	P	H	Y

Now arrange the column in alphabetical order considering the key so that the table looks like

A	C	H	K
R	Y	C	P
O	G	T	R
P	H	A	Y

Now write all the letters in a column wise
Hence the Cipher-Text = ROPYGHCTAPRY

3) Vernam Cipher

i. A subset of Vernam cipher is called a one-time pad because it is implemented using a random set of nonrepeating characters as an input cipher text(Key).

ii. In this the length of key should be equal to the length of text

Example :

Plain-Text = SATWIK

Key = RSAVNA

Now

1) Assign a number to each character of the plain-text and the key according to alphabetical order.
2) Add both the number (Corresponding plain-text character number and Key character number).

S	A	T	W	I	K
18	0	19	22	8	10
R	S	A	V	N	A
17	18	0	21	13	0

Now add the numerical values of key and plain text so that

35	18	19	43	21	10

Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

After subtracting

9	18	19	17	21	10
J	S	T	R	V	K

Hence the Cipher-Text = JSTRVK

THANK YOU