TRANSPOSITION CIPHER

- In the transposition technique the positions of letters/numbers/symbols in plain text is changed with one another.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

TRANSPOSITION CIPHER TECHNIQUES

1. **Rail Fence Cipher**
2. **Columnar Transposition**
   - Simple Columnar Transposition
   - Double Columnar Transposition

1. RAIL FENCE CIPHER

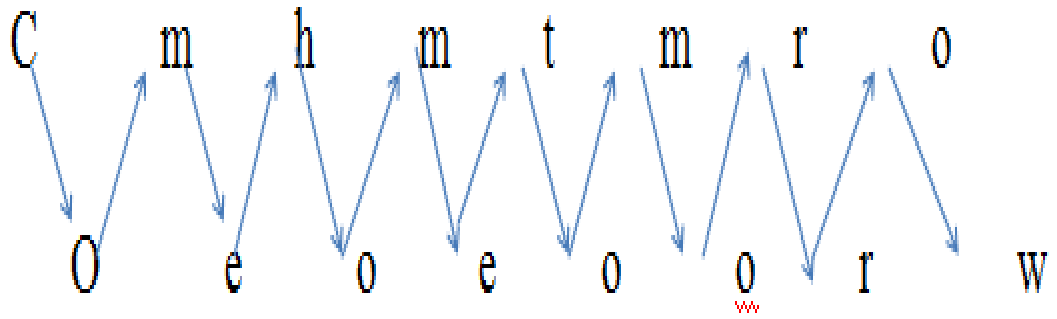
- In this method plain text is written downwards on “rails of fence “ , starting a new column when bottom is reached.
- **Algorithm:**

1. First write down plain text message as a sequence of diagonals.
2. Read the plain text written in first step as a sequence of rows.

1. RAIL FENCE CIPHER

Example:

Plain text: come home tomorrow



Cipher text: cmhmtmrooeoeoorw

1. Simple Columnar Transposition

- In this method the message is written in rows of fixed length and then read out column by column
- Column are selected in some in some scrambled order.
- The number of columns are defined by the length of key.
- **Algorithm:**

1. Write the plain text message row by row in a rectangle of predefined size.(length of key)
2. Read the message column by column according t the selected order thus obtained message is a cipher text.

1. SIMPLE COLUMNAR TRANSPOSITION

Key: ZEBRAS

plain text: welcome home

Order : 6 3 2 4 1 5

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Cipher text: MLOEHCMWEOE

2.Double Columnar Transposition

- Single columnar transposition can be attack by guessing possible column lengths.
- Therefore to make it stronger double transposition is used.
- This is simple columnar transposition technique applied twice.
- Here same key can be used for transposition or two different keys can be used.

2.DOUBLE COLUMNAR TRANSPOSITION

- First apply simple columnar transposition

Key: ZEBRAS

plain text: welcome home

Order : 6 3 2 4 1 5

1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Cipher text: MLOEHCMWEOE

2.DOUBLE COLUMNAR TRANSPOSITION

Cipher text 1: MLOEHCMWEOE

Order : 6 3 2 4 1 5

1	2	3	4	5	6
M	L	O	E	H	C
M	W	E	O	E	

Final Cipher Text: COELWEOMMHE

Substitution Cipher	Transposition Cipher
A substitution technique is one in which the letters/number/symbols of plain text are replaced by other letters/numbers/symbols.	In the transposition technique the positions of letters/numbers/symbols in plain text is changed with one another.
It is easy to understand.	It is difficult to understand.
Methods: 1.Caesar's Cipher 2.Mono-Alphabetic Cipher 3.A Homophonic Substitution Cipher 4.A Polygram Substitution Cipher 5.A Polyalphabetic Substitution Cipher 1. e.g.Vigenere Cipher 6. One time Pad(Vernam Cipher)	Methods: 1.Rail Fence Cipher 2.Columnar Transposition – Simple Columnar Transposition – Double Columnar Transposition