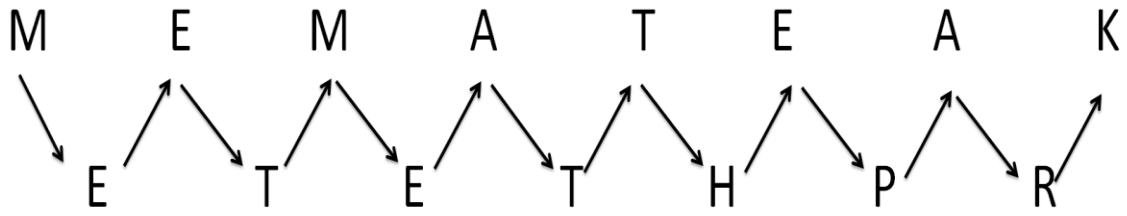
Chapter four
Classical Symmetric Cipher

- **Transposition (or permutation) cipher:** Transposition cipher keeps the letters the same, but rearranges their order according to a specific algorithm.
- **Substitution cipher:** replacing each element of the plaintext with another element.
- **Product cipher:** using multiple stages of substitutions and transpositions

Transposition cipher

١. **Keyless Transposition Ciphers: -** Simple transposition ciphers, which were used in the past, are keyless. A good example of a keyless cipher using the first method is the **rail fence cipher.** The ciphertext is created reading the pattern row by row. For example, to send the message (**Meet me at the park**) to Bob, Alice writes



- She then creates the ciphertext (**MEMATEAKETETHPR**).

2. Columnar Transposition Ciphers.

- Write the message in rows of a fixed length, and then read out again column by column.
- The columns are chosen in some scrambled order.
- Both the length of the rows and the permutation of the columns are usually defined by a key.

Example: Let the plaintext is (WE ARE DISCOVERED FLEE AT ONCE) the key word be: ZEBRA.

Z	E	B	R	A
W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
F	L	E	E	A
T	O	N	C	E

- The ciphertext:

EODAEASRENEIELORCEECWDVFT

Double Columnar Transposition.