CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

Transposition Techniques -

Rail fence method

Columnar method

Vijesh Nair

TRANSPOSITION TECHNIQUES

- Performing some sort of permutation on the plaintext letters.
- Changing the arrangement of letters.
- eg:- NAME ⟶ MEAN

- Security is less.
- Can be easily recognised.
- Multiple transpositions can be done to make it more secure.

RAIL FENCE METHOD

- Plaintext is written as a sequence of diagonals.
- Then read off as a sequence of rows.
- eg:- Let P = GIVESOMEMONEY

- Then write it like this ;

- Now corresponding cipher = GVSMMNYIEOEOE

RAIL FENCE METHOD

- eg:- Let P = GIVESOMEMONEY
- Then write it like this ;

- Now corresponding cipher = GVSMMNYIEOEOE
- Or we can increase key (no. of rows) ;

- Now corresponding cipher = GEMOYISENVOME

COLUMNAR METHOD

- Plaintext is written as a reactangle, row by row.
- Then read it column by column.
- eg:- Let P = GIVEHIMMONEY

- Then write it like this ;

G	I	V
E	H	I
M	M	O
N	E	Y

- Now corresponding cipher = GEMNIHMEVIOY

COLUMNAR METHOD

- eg:- Let P = GIVEHIMMONEY
- Then write it like this ;

G	I	V
E	H	I
M	M	O
N	E	Y

- Now corresponding cipher = GEMNIHMEVIOY
- Or we can change the key (order of matrix).
- Then

G	I	V	E
H	I	M	M
O	N	E	Y

  - Then corresponding cipher is GHOIINVMEEMY

THANK YOU

Vijesh Nair