CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

Transposition Techniques -

Columnar transposition with key.

Double Transposition.

Vijesh Nair

COLUMNAR TRANSPOSITION with keyword.

- Plain text written as row by row.
- Use a keyword.
- Then read it column by column in the order of key.

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

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

COLUMNAR TRANSPOSITION with keyword.

- Plain text written as row by row.
- Use a keyword.
- Give number to the letters in alphabetical order.
- Then read it column by column in the order of key.

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

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

H-2	A -1	T-3
G	I	V
E	H	I
M	M	O
N	E	Y

- Now corresponding cipher = IHMEGEMNVIOY

Vijesh Nair

DECRYPTION.

- We have C = IHMEGEMNVIOY & Key = HAT
- Then write it like this ;

H-2	A - 1	T-3

DECRYPTION.

- We have C = IHMEGEMNVIOY & Key = HAT
- Then write it like this ;

H-2	A -1	T-3
	I	
	H	
	M	
	E	

H-2	A -1	T-3
G	I	
E	H	
M	M	
N	E	

H-2	A -1	T-3
G	I	V
E	H	I
M	M	O
N	E	Y

- Read it row by row.
- Now corresponding plaintext = GIVEHIMMONEY

DOUBLE TRANSPOSITION.

- Similar to columnar transposition.
- Columnar transposition is applied twice.
- Same key or different keys can be applied for both transposition..

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

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

H-2	A -1	T-3
G	I	V
E	H	I
M	M	O
N	E	Y

- Now corresponding cipher = IHMEGEMNVIOY

DOUBLE TRANSPOSITION.

- Now corresponding cipher = IHMEGEMNVIOY
- Now write this ciphertext in the same form.
- And apply columnar transposition again.
- This time let key be RED.

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

R-3	E -2	D -1
I	H	M
E	G	E
M	N	V
I	O	Y

- Now the final cipher after double transposition is MEVYHGNOIEMI

DECRYPTION.

- We have C = MEVYHGNOIEMI & key_1 = HAT & key_2 = RED
- Apply key_2 first.

R-3	E -2	D -1

DECRYPTION.

- We have C = MEVYHGNOIEMI & key$_1$ = HAT & key$_2$ = RED
- Apply key$_2$ first.

R-3	E -2	D -1
		M
		E
		V
		Y

R-3	E -2	D -1
	H	M
	G	E
	N	V
	O	Y

R-3	E -2	D -1
I	H	M
E	G	E
M	N	V
I	O	Y

- After first step we get IHMEGEMNVIOY

DECRYPTION.

- After first step we got IHMEGEMNVIOY & key$_1$ = HAT & key$_2$ = RED
- Apply key$_1$ now.

H-2	A -1	T -3

DECRYPTION.

- After first step we got IHMEGEMNVIOY & key$_1$ = HAT & key$_2$ = RED
- Apply key$_1$ now.

H-2	A -1	T -3
	I	
	H	
	M	
	E	

H-2	A -1	T -3
G	I	
E	H	
M	M	
N	E	

H-2	A -1	T -3
G	I	V
E	H	I
M	M	O
N	E	Y

- Now the final plain text is GIVEHIMMONEY.

THANK YOU

Vijesh Nair