CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

Transposition Techniques -

Columnar transposition with key.

Double Transposition.

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	_	>
E	I	_
М	M	0
N	ш	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	٧
E	Н	-
М	M	0
N	E	Υ

ЦЭ	A	T 2
H-2	A - I	T-3
	, , ,	

G	I	٧
ш	I	_
M	M	0
Z	ш	Y

Now corresponding cipher = IHMEGEMNVIOY

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

H-2	A-I	T-3

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

H-2	A-I	T-3
	I	
	Н	
	М	
	E	

H-2	A-I	T-3
G	_	
E	Ι	
М	M	
N	E	

H-2	A-I	T-3
U	_	>
ш	I	_
Σ	M	0
Z	ш	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	٧
E	H	_
М	М	0
N	Е	Υ

H-2	A-I	T-3
G	_	>
ш	I	_
Σ	Σ	0
N	Е	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.

T.	Н	М
E	G	E
М	N	٧
T	0	Υ

R-3	E -2	D-I
_	I	Σ
Е	G	ш
М	N	٧
I	0	Υ

Now the final cipher after double transposition is MEVYHGNOIEMI

- We have C = MEVYHGNOIEMI & key₁ = HAT & key₂ = RED
- Apply key₂ first.

R-3	E -2	D-I

- We have C = MEVYHGNOIEMI & key₁ = HAT & key₂ = RED
- Apply key₂ first.

R-3	E -2	D - I
		М
		E
		٧
		Υ

R-3	E -2	D-I
	Н	M
	G	Е
	N	٧
	0	Y

R-3	E -2	D-I
I	I	Σ
E	U	ш
М	Z	>
I	0	Y

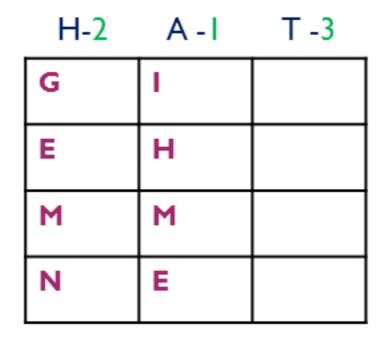
After first step we get IHMEGEMNVIOY

- After first step we got IHMEGEMNVIOY & key₁ = HAT & key₂ = RED
- Apply key_I now.

H-2	A-I	T -3

- After first step we got IHMEGEMNVIOY & $key_1 = HAT$ & $key_2 = RED$
- Apply key_I now.

H-2	A - I	T -3
	I	
	Н	
	М	
	E	



H-2	A-I	T -3
G	_	>
ш	I	_
М	М	0
Z	ш	Y

• Now the final plain text is GIVEHIMMONEY.

THANK YOU

Vijesh Nair