CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

Transposition Techniques - Route cipher

ROUTE CIPHER

- Plaintext is written as a grid of a particular size.
- Then read off using a predetermined pattern called "route".
- This pattern is the key used in Route cipher.
- The size of grid is also passed with the key.
- eg:- Let P = GIVETHEMONEY then write it in a form of grid.

G	1	V	E
Т	н	E	М
0	N	E	Y



or

ENCRYPTION

eg:- Let P = GIVETHEMONEY then write it in a form of grid

G	I	V	E
Т	Н	E	M
0	N	E	Y

G	I
٧	E
Т	Н
E	М
0	N
E	Y

or

let key be the pattern "Read from right to left from top right corner"

Then encrypted text, $C_1 = EVIGMEHTYENO$ $C_2 = IGEVHTMENOYE$

eg:- So C= EVIGMEHTYENO

and key is the pattern "Read from right to left from top right corner" & size =3x4

eg:- So C= EVIGMEHTYENO

and key is the pattern "Read from right to left from top right corner" & size =3x4

G	I	V	E

eg:- So C= EVIGMEHTYENO

and key is the pattern "Read from right to left from top right corner" & size =3x4

G	I	٧	E
Т	H	ш	M

eg:- So C= EVIGMEHTYENO

and key is the pattern "Read from right to left from top right corner" & size =3x4

G	I	٧	E
Т	Н	Е	М
0	Z	ш	Y

So corresponding P = GIVETHEMONEY

ENCRYPTION

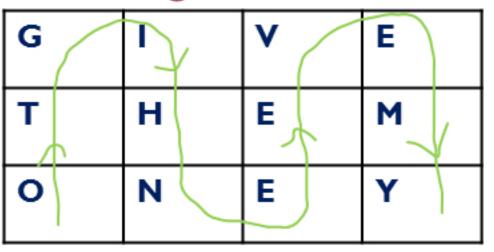
eg:- Let P = GIVETHEMONEY then write it in a form of grid

G	1	V	E
Т	Н	E	М
0	N	E	Y

let key be "Read in zigzag manner starting from bottom left corner in bottom up fashion"

ENCRYPTION

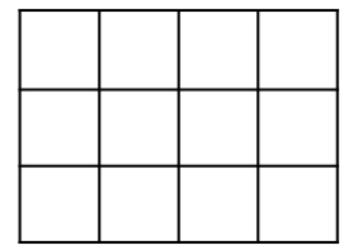
eg:- Let P = GIVETHEMONEY then write it in a form of grid



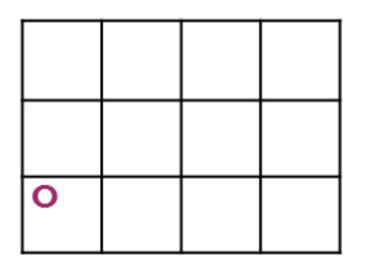
let key be "Read in zigzag manner starting from bottom left corner in bottom up fashion"

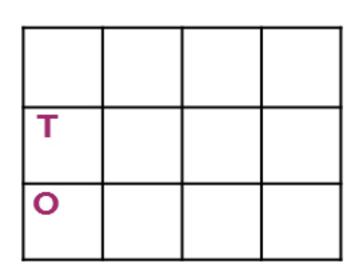
Then cipher = OTGIHNEEVEMY

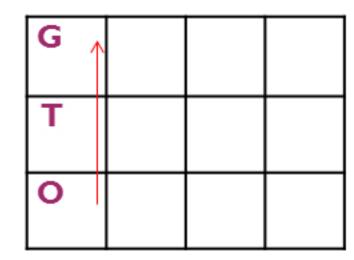
eg:- So C= OTGIHNEEVEMY
and key is "Read in zigzag manner starting from bottom left corner in bottom up fashion"
& size =3x4



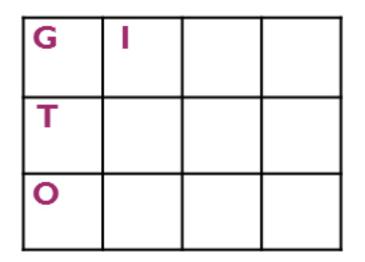
eg:- So C= OTGIHNEEVEMY
and key is "Read in zigzag manner starting from bottom left corner in bottom up fashion"
& size =3x4

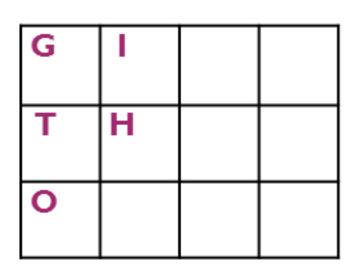


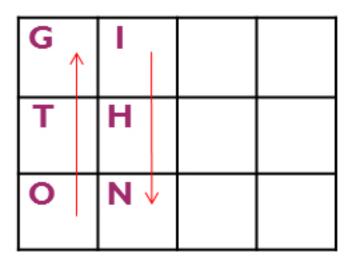




eg:- So C= GTOIHNVEEEMY
and key is "Read in zigzag manner starting from bottom left corner in bottom up fashion"
& size =3x4



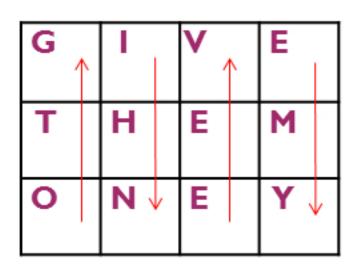




eg:- So C= GTOIHNVEEEMY
and key is "Read in zigzag manner starting from bottom left corner in bottom up fashion"
& size =3x4

G	\	I		V	\	
Т		Н		Е		
0		N	/	Е		

eg:- So C= GTOIHNVEEEMY
and key is "Read in zigzag manner starting from bottom left corner in bottom up fashion"
& size =3x4



So the plain text can be read in row by row.

P = GIVETHEMONEY

THANK YOU

Vijesh Nair