SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

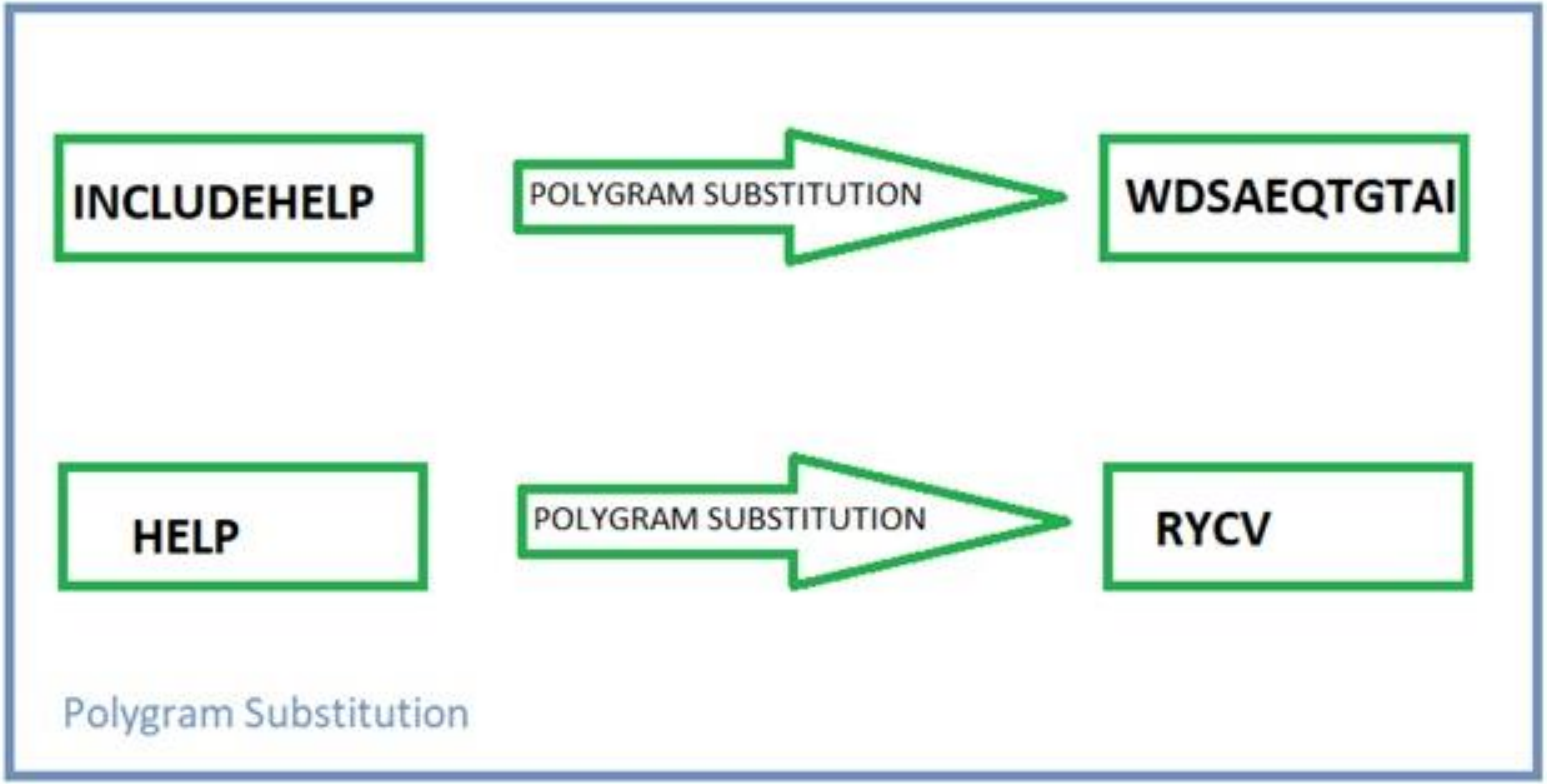
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR /V SEMESTER

Unit 1- Introduction

Topic : Substitution Techniques-02



INCLUDEHELP

POLYGRAM SUBSTITUTION

WDSAEQTGTAI

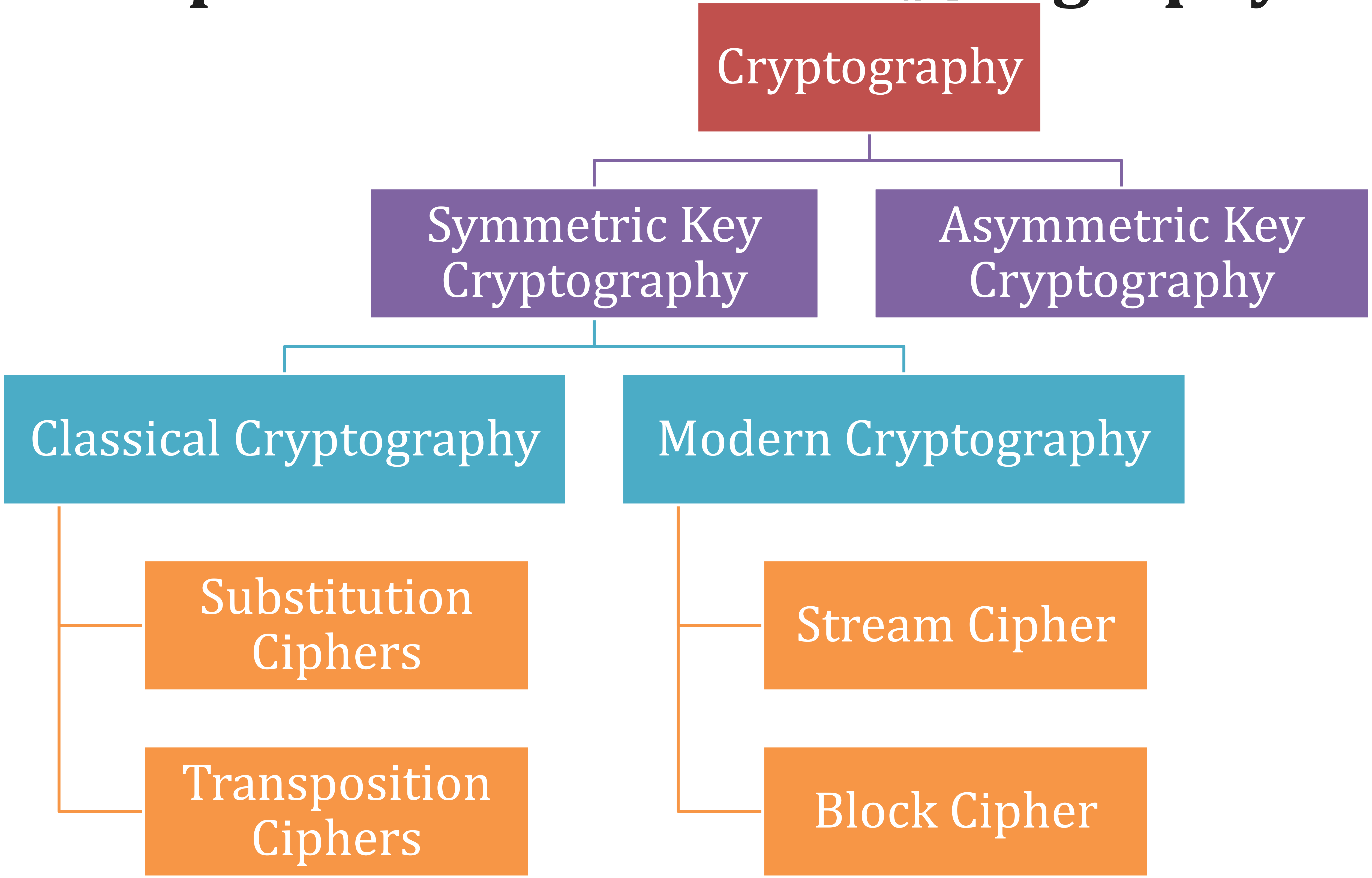
HELP

POLYGRAM SUBSTITUTION

RYCV

Polygram Substitution

Recap : Classification of Cryptography



Substitution Techniques

- □ A substitution technique is one in which the letters of plaintext are **replaced by other letters or by numbers or symbols.**
  - Caesar Cipher
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Ciphers
  - One-Time Pad

Hill Cipher

- Multiletter Cipher
- Lester Hill in 1929 – Mathematician
- Encryption
  - m successive plaintext – Substitutes to m cipher text Letters
  - m = linear
  - Each character assigned with numeric values (a=0,b=1…..z=25)

Hill Cipher

□ If m = 3 , General form

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3)\, mod\ 26$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) mod\ 26$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) mod\ 26$$

Expressed in column vectors and matrices

C= E(K,P) = KP mod 26

P = D(K,P) = K^{-1} C mod 26 = K^{-1} KP = P

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} mod\ 26$$

Hill Cipher

Consider m =3 , the plain text " paymoremoney

$$P = \begin{pmatrix} p & m & e & n \\ a & o & m & e \\ y & r & o & y \end{pmatrix} \qquad P = \begin{pmatrix} 15 & 12 & 4 & 13 \\ 0 & 14 & 12 & 4 \\ 24 & 17 & 14 & 24 \end{pmatrix}$$

- Encryption Key

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Hill Cipher

$$P.T_1 = \begin{bmatrix} p \\ a \\ y \end{bmatrix} = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$$

$$C.T_1 = Key\ x\ P.T_1\ mod\ 26 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}\ mod\ 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$

$$C.T_2 = Key\ x\ P.T_2\ mod\ 26 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix}\ mod\ 26 = \begin{bmatrix} 7 \\ 3 \\ 11 \end{bmatrix} = \begin{bmatrix} H \\ D \\ L \end{bmatrix}$$

Find the Cipher for the rest of the Example

$$P.T_3 = \begin{pmatrix} e \\ m \\ o \end{pmatrix} \qquad P.T_4 = \begin{pmatrix} n \\ e \\ y \end{pmatrix}$$

Decryption using Hill Cipher

Decryption – inverse of K^{-1}

We know that, K K^{-1} = K^{-1} K = I

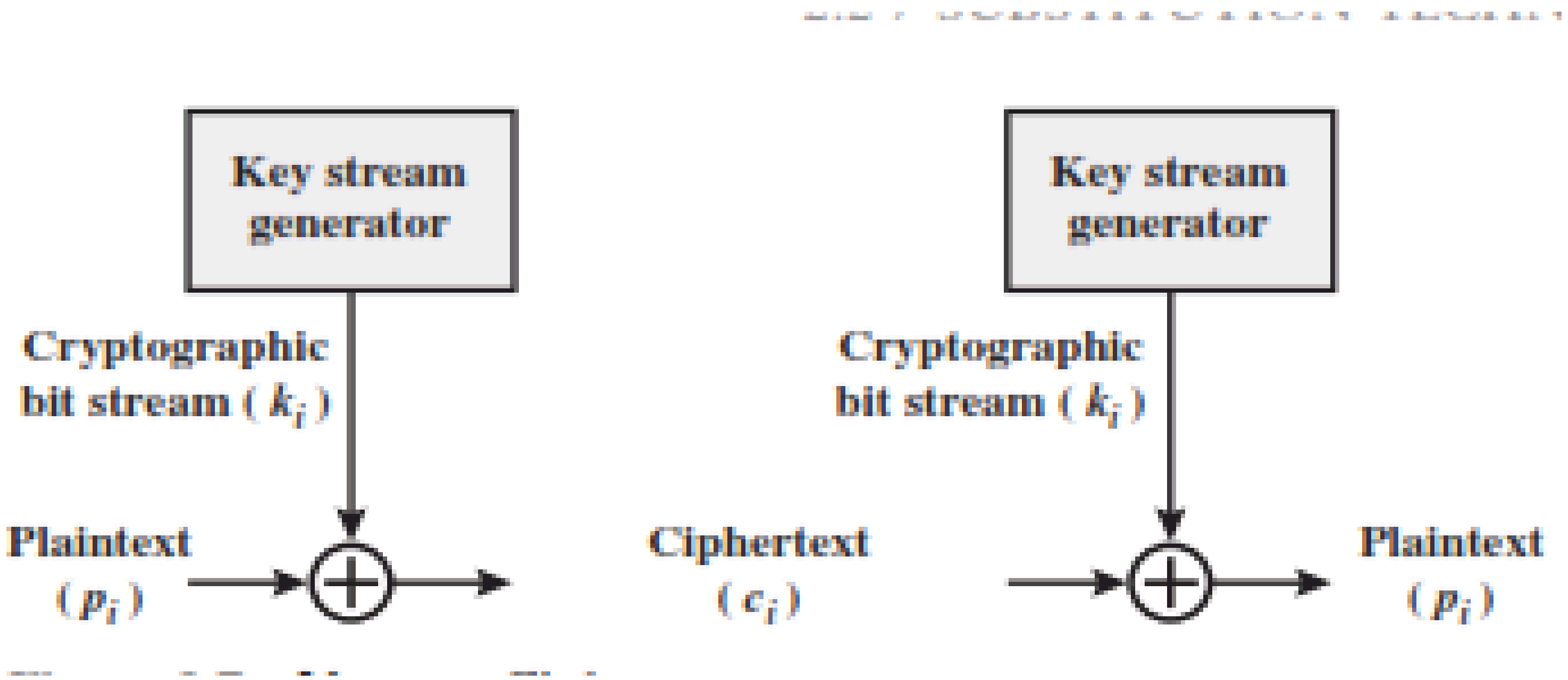
$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \qquad KK^{-1} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$= \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} mod\ 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

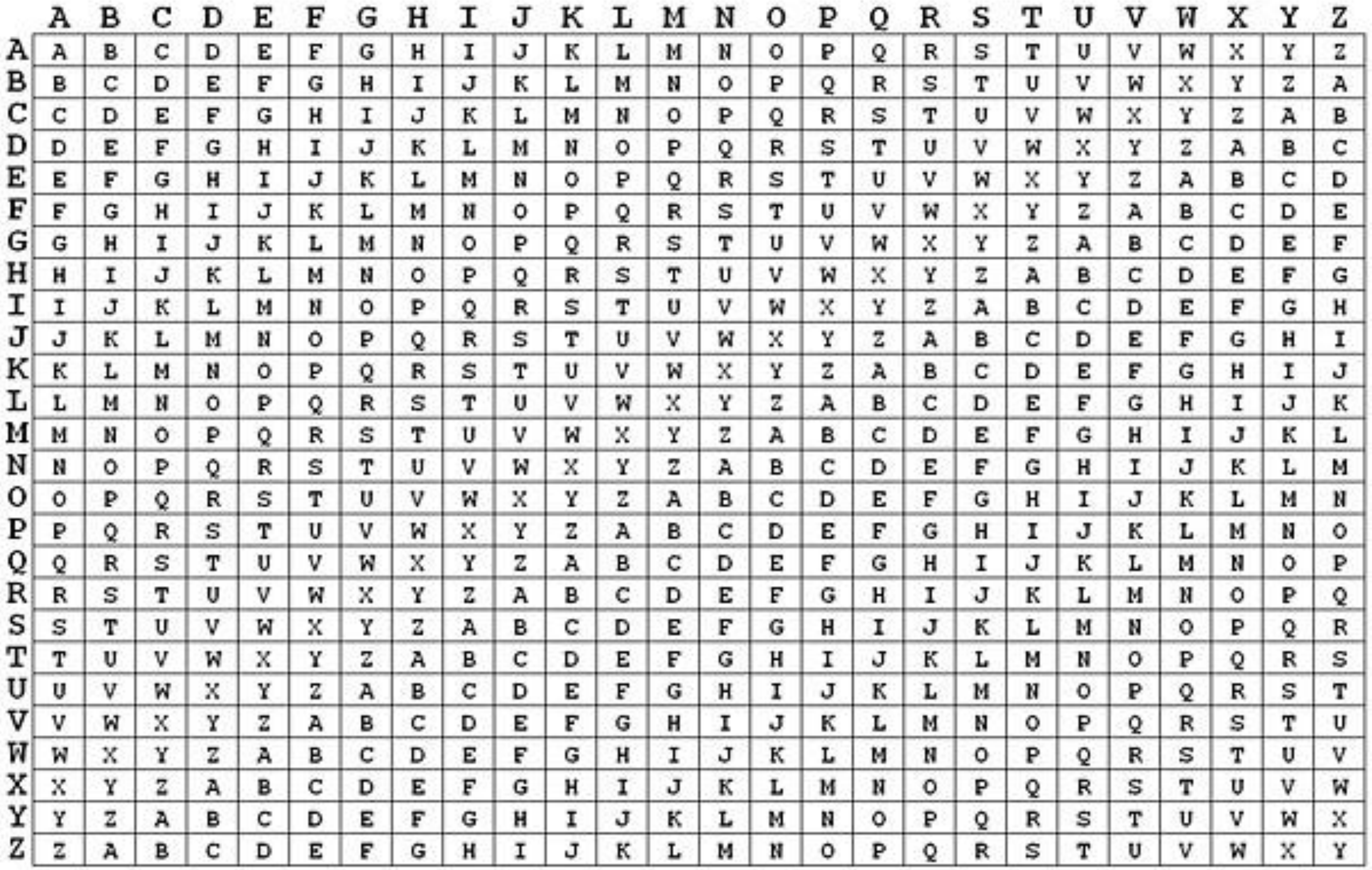
Activity

Polyalphabetic Cipher

- The first known polyalphabetic cipher was the *Alberti Cipher* invented by Leon Battista Alberti in around 1467.
- Vigenère Cipher **$C_i = P_i$ XOR K_i** **$P_i = C_i$ XOR K_i**



Vigenère Cipher Table



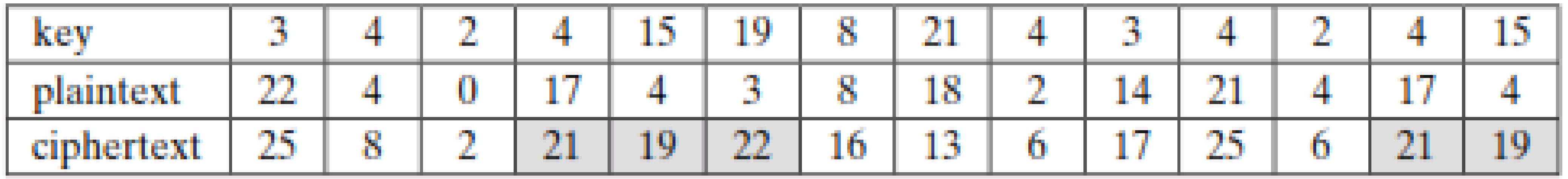
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Let's play a game of hiding the message using Polyalphabetic Cipher

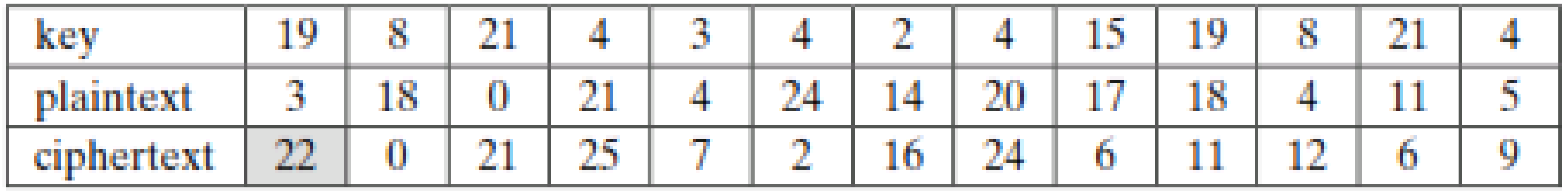
We are discovered save yourself

deceptive

ZICVTWQNGR ZGVTWAVZHC QYGLMGJ



key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19



key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

One Time Pad

- Each new message – requires new key of same length
- Unbreakable
- No relationship to plain Text

Let's play a game of hiding the message using One Time Pad

Mr Mustard with the candlestick in the hall

pxlmvmsydofu
yrvzwc
tnlebnecvgdup
ahfzzlmnyih

ANKYODKYUR
EPFJBYOJDSPL
REYIUNOFDOI
UERFPLUYTS

Assessment

Compute the Ciphertext using Playfair Cipher

Perform Encryption and decryption using Hill Cipher for the following Message PEN and Key: ACTIVATED

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU