CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

HILL CIPHER 3x3 EXAMPLE

Vijesh Nair

HILL CIPHER

- Encrypts a group of letters called polygraph.
- It can be digraph, trigraph etc.
- Use of mathematics.
- Key and plain text should be in the form of a square matrix.
- To encrypt;

$$C = K.P \bmod 26$$

ENCRYPTION

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

Let the plain text be "SAFEMESSAGES"

Let key = "CIPHERING" = $\begin{bmatrix} C & I & P \\ H & E & R \\ I & N & G \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

Since key is a 3x3 matrix, plain text should be converted into column ectors of length 3

So we get SAF EME SSA GES

$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \quad \begin{bmatrix} E \\ M \\ E \end{bmatrix} \quad \begin{bmatrix} S \\ S \\ A \end{bmatrix} \quad \begin{bmatrix} G \\ E \\ S \end{bmatrix}$

ENCRYPTION

First is $\begin{bmatrix} S \\ A \\ F \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$$

C = P K moc

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*18 + 8*0 + 15*5 \\ 7*18 + 4*0 + 17*5 \\ 8*18 + 13*0 + 6*5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*18 + 8*0 + 15*5 \\ 7*18 + 4*0 + 17*5 \\ 8*18 + 13*0 + 6*5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix}$$

$$26 \overline{)111} \quad 4, \ 104, \ 7$$

So 111 mod 26 = 7

$$26 \overline{)211} \quad 8, \ 208, \ 3$$

So 211 mod 26 = 3

$$26 \overline{)174} \quad 6, \ 156, \ 18$$

So 174 mod 26 = 18

$$\begin{bmatrix} S \\ A \\ F \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \text{ mod } 26$$

$$C = \begin{bmatrix} 2*18 + 8*0 + 15*5 \\ 7*18 + 4*0 + 17*5 \\ 8*18 + 13*0 + 6*5 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \text{ mod } 26$$

$$C = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix}$$ Now find the corresponding alphabets i.e, = $$\begin{bmatrix} H \\ D \\ S \end{bmatrix}$$

Vijesh Nair

ENCRYPTION

Next is $\begin{bmatrix} E \\ M \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$\begin{bmatrix} E \\ M \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}$$

$$C = P\,K \bmod 26$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*4 + 8*12 + 15*4 \\ 7*4 + 4*12 + 17*4 \\ 8*4 + 13*12 + 6*4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} E \\ M \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*4 + 8*12 + 15*4 \\ 7*4 + 4*12 + 17*4 \\ 8*4 + 13*12 + 6*4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix}$$

$$26 \overline{)164} \quad 6, \ 156, \ 8$$

So 164 mod 26 = 8

$$26 \overline{)144} \quad 5, \ 130, \ 14$$

So 144 mod 26 = 14

$$26 \overline{)212} \quad 8, \ 208, \ 4$$

So 212 mod 26 = 4

$$\begin{bmatrix} E \\ M \\ E \end{bmatrix} \rightarrow \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*4 + 8*12 + 15*4 \\ 7*4 + 4*12 + 17*4 \\ 8*4 + 13*12 + 6*4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix}$$

Now find the corresponding alphabets i.e, $= \begin{bmatrix} I \\ O \\ E \end{bmatrix}$

ENCRYPTION

Next is $\begin{bmatrix} S \\ S \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$\begin{bmatrix} S \\ S \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}$$

$$C = P\,K \bmod 26$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*18 + 8*18 + 15*0 \\ 7*18 + 4*18 + 17*0 \\ 8*18 + 13*18 + 6*0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} S \\ S \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*18 + 8*18 + 15*0 \\ 7*18 + 4*18 + 17*0 \\ 8*18 + 13*18 + 6*0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix}$$

$$\begin{array}{r} 6 \\ 26\overline{)180} \\ 156 \\ \hline 24 \end{array}$$

So 180 mod 26 = 24

$$\begin{array}{r} 7 \\ 26\overline{)198} \\ 182 \\ \hline 16 \end{array}$$

So 198 mod 26 = 16

$$\begin{array}{r} 14 \\ 26\overline{)378} \\ 364 \\ \hline 14 \end{array}$$

So 378 mod 26 = 14

$$\begin{bmatrix} S \\ S \\ A \end{bmatrix} \rightarrow \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \text{ mod } 26$$

$$C = \begin{bmatrix} 2*18 + 8*18 + 15*0 \\ 7*18 + 4*18 + 17*0 \\ 8*18 + 13*18 + 6*0 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \text{ mod } 26$$

$$C = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix}$$

Now find the corresponding alphabets i.e, $= \begin{bmatrix} Y \\ Q \\ O \end{bmatrix}$

Vijesh Nair

ENCRYPTION

Next is $\begin{bmatrix} G \\ E \\ S \end{bmatrix} \rightarrow \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}$

A	B	C	D	**E**	F	**G**	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	**S**	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$\begin{bmatrix} G \\ E \\ S \end{bmatrix} \rightarrow \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}$$

$$C = P\,K \bmod 26$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*6 + 8*4 + 15*18 \\ 7*6 + 4*4 + 17*18 \\ 8*6 + 13*4 + 6*18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} G \\ E \\ S \end{bmatrix} \rightarrow \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*6 + 8*4 + 15*18 \\ 7*6 + 4*4 + 17*18 \\ 8*6 + 13*4 + 6*18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{array}{r} 12 \\ 26 \overline{)\,314} \\ 312 \\ \hline 2 \end{array}$$

So 314 mod 26 = 2

$$\begin{array}{r} 14 \\ 26 \overline{)\,364} \\ 364 \\ \hline 0 \end{array}$$

So 364 mod 26 = 0

$$\begin{array}{r} 8 \\ 26 \overline{)\,208} \\ 208 \\ \hline 0 \end{array}$$

So 208 mod 26 = 0

$$\begin{bmatrix} G \\ E \\ S \end{bmatrix} \rightarrow \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$C = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2*6 + 8*4 + 15*18 \\ 7*6 + 4*4 + 17*18 \\ 8*6 + 13*4 + 6*18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}$$ Now find the corresponding alphabets i.e, $= \begin{bmatrix} C \\ A \\ A \end{bmatrix}$

Viiesh Nair

So the text SAFEMESSAGES became HDSIOEYQOCAA.

THANK YOU

Vijesh Nair