CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC ENCRYPTION

HILL CIPHER 3x3 Decryption

Vijesh Nair

HILL CIPHER - Decryption

- To encrypt;

  $C = K.P \bmod 26$

- To decrypt;

  Find the inverse of key matrix K^{-1}

  $P = K^{-1}C \bmod 26$

- Eg:- Plain text P = SAFEMESSAGES

  Key K = CIPHERING = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

  When encrypted using Hill cipher method, we get C = HDSIOEYQOCAA

  ie., SAFEMESSAGES $\longrightarrow$ HDSIOEYQOCAA

FINDING INVERSE:

$$K^{-1} = \frac{1}{|d|} \text{Adj}(K)$$

So C = HDS IOEYQO CAA

and key = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$

We need to find decryption key K^{-1}

So first find the determinant of the matrix :

$$d = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a(ei - hf) - b(di - gf) + c(dh - ge)$$

$$\text{So here } d = \begin{vmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{vmatrix} = 2(4x6 - 13x17) - 8(7x6 - 8x17) + 15(7x13 - 8x4) = 1243$$

So determinant d = 1243;

Now find the multiplicative inverse of the determinant.
ie., $d\ d^{-1} \equiv 1 \bmod 26$

So $1243 * d^{-1} \equiv 1 \bmod 26$

So determinant d = 1243;

Now find the multiplicative inverse of the determinant.
ie., $d\ d^{-1} \equiv 1 \bmod 26$

So $1243 * d^{-1} \equiv 1 \bmod 26$ So $d^{-1} = 5$

Use trial and error method

1 mod 26 = 1
1243 * 5 mod 26
= 6215 mod 26 = 1

So multiplicative inverse is 5 here.

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 4 \times 6 - 13 \times 17 = -197$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 7 \times 6 - 8 \times 17 = -94$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 7 \times 13 - 8 \times 4 = 59$

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 4 \times 6 - 13 \times 17 = -197$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 7 \times 6 - 8 \times 17 = -94$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 7 \times 13 - 8 \times 4 = 59$

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

$\begin{bmatrix} -197 & 94 & 59 \\ & & \\ & & \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 8 x 6 - 13 x 15 = -147

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 2 x 6 - 8 x 15 = - 108

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 2 x 13 - 8 x 8 = -38

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 8 \times 6 - 13 \times 15 = -147$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 2 \times 6 - 8 \times 15 = -108$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 2 \times 13 - 8 \times 8 = -38$

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

$\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ & & \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 8 x 17 - 4 x 15 = 76

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 2 x 17 - 7 x 15 = -71

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ = 2 x 4 - 7 x 8 = -48

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding co-factor matrix:

So here K = $\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 8 \times 17 - 4 \times 15 = 76$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 2 \times 17 - 7 \times 15 = -71$

$\begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}$ $= 2 \times 4 - 7 \times 8 = -48$

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

$\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding transpose matrix;

$$\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix} = \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$$

Now find the adjoint of the matrix.

- Find co-factor matrix and then find the transpose of that matrix.

Finding transpose matrix;

$$\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix} = \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$$

this is the adjoint matrix

So here Adj (K) = $\begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$

To remove the negative sign, add 26 n times to the negative numbers.

So we get $\begin{bmatrix} -197+(7*26) & 147 & 76 \\ 94 & -108+(n*26) & 71 \\ 59 & 38 & -48+(2*26) \end{bmatrix} = \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix}$

Now multiply this with the multiplicative inverse of determinant.

So $5 * \begin{bmatrix} 11 & 147 & 76 \\ 94 & 22 & 71 \\ 59 & 38 & 4 \end{bmatrix} = \begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix}$

Now find its modulo 26 to simplify.

$$\text{ie.,} = \begin{bmatrix} 55 & 735 & 380 \\ 470 & 110 & 355 \\ 295 & 190 & 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

This is the decryption key K^{-1}

We have the decryption formula $P = K^{-1} C \bmod 26$

C = HDS IOEYQO CAA

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

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

So corresponding plain text ,

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3*7 + 7*3 + 16*18 \\ 2*7 + 6*3 + 17*18 \\ 9*7 + 8*3 + 20*18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 330 \\ 338 \\ 447 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} = \begin{bmatrix} S \\ A \\ F \end{bmatrix}$$

We have the decryption formula $P = K^{-1} C \bmod 26$

C = HDS IOEYQO CAA

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

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

So corresponding plain text ,

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3*8 + 7*14 + 16*4 \\ 2*8 + 6*14 + 17*4 \\ 9*8 + 8*14 + 20*4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 186 \\ 168 \\ 264 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ M \\ E \end{bmatrix}$$

We have the decryption formula $P = K^{-1} C \bmod 26$

C = HDS IOEYQO CAA

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

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

So corresponding plain text ,

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3*24 + 7*16 + 16*14 \\ 2*24 + 6*16 + 17*14 \\ 9*24 + 8*16 + 20*14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 408 \\ 382 \\ 624 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} = \begin{bmatrix} S \\ S \\ A \end{bmatrix}$$

We have the decryption formula $P = K^{-1} C \bmod 26$

C = HDS IOE YQO CAA

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

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

So corresponding plain text ,

$$P = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3*2 + 7*0 + 16*0 \\ 2*2 + 6*0 + 17*0 \\ 9*2 + 8*0 + 20*0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} G \\ E \\ S \end{bmatrix}$$

So the text HDSIOEYQOCAA became SAFEMESSAGES.

THANK YOU

Vijesh Nair