# CRYPTOGRAPHY & NETWORK SECURITY

## SYMMETRIC ENCRYPTION

HILL CIPHER 3x3 Decryption

### HILL CIPHER - Decryption

- To encrypt;
   C = K.P mod 26
- To decrypt;
   Find the inverse of key matrix K<sup>-1</sup>
   P = K<sup>-1</sup>C mod 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 → HDSIOEYQOCAA

Vijesh Nair

#### **FINDING INVERSE:**

So C = HDS IOEYQO CAA  
and key = 
$$\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}$$

 $K^{-1} = I Adj(K)$ |d|

We need to find decryption key K-1

So first find the determinant of the matrix:

So here 
$$d = 2 8 15 = 2(4x6 - 13x17) - 8(7x6 - 8x17) + 15(7x13 - 8x4) = 1243$$
  
7 4 17  
8 13 6

So determinant d = 1243;

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

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

So determinant d = 1243;

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

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

Use trial and error method

So multiplicative inverse is 5 here.

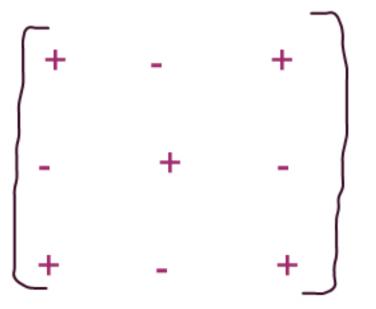
Find co-factor matrix and then find the transpose of that matrix.

#### Finding co-factor matrix:

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

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

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



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

#### Finding co-factor matrix:

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

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

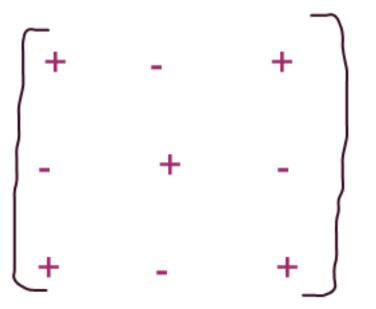
$$\begin{vmatrix}
 2 & 8 & 15 \\
 7 & 4 & 17 \\
 8 & 13 & 6
 \end{vmatrix} = 7 \times 13 - 8 \times 4 = 59$$

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

#### Finding co-factor matrix:

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

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



#### Vijesh Nair

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

#### Finding co-factor matrix:

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

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

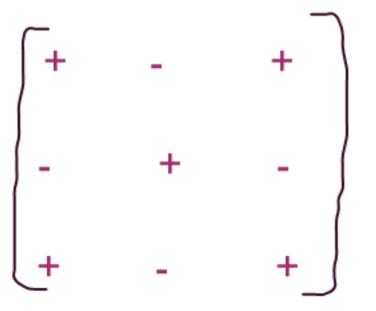
#### Vijesh Nair

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

#### Finding co-factor matrix:

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

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



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

#### Finding co-factor matrix:

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

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

Vijoch Nair

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

#### Finding transpose matrix;

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

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.

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

This is the decryption key K-1

## We have the decryption formula P= K<sup>-1</sup> C mod 26

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

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

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

#### We have the decryption formula $P = K^{-1} C \mod 26$ C = HDS IOEYQO CAA

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

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

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

## We have the decryption formula P= K<sup>-1</sup> C mod 26

C = HDS IOEYQO CAA

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

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

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

## We have the decryption formula P= K<sup>-1</sup> C mod 26

C = HDS IOEYQO CAA

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

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

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

So the text HDSIOEYQOCAA became SAFEMESSAGES.

# THANK YOU

Vijesh Nair