National Institute of Technology Calicut
Department of Computer Science and Engineering
Winter Semester 2022-2023

Session: Afternoon | **Subject: CS3093D – Networks Laboratory**
Time: 2PM to 4PM | **Maximum Marks: 40**

---

1. Imagine that you are working for a top-secret government agency, and your team is developing a chat room application to be used by agents for communication. This chat room should be secure to ensure confidential information not intercepted by unauthorized parties. You need to design and implement a secure chat room application to encrypt and decrypt all messages between clients and the server. The application should allow multiple users to connect and communicate with each other in real-time, but only after the server has authenticated them. You are required to use Hill cipher algorithm to ensure that the messages cannot be intercepted or read by unauthorized parties. The 3x3 invertible key matrix for the encryption and the decryption using Hill Cipher is

   Key matrix = [6 2 3]
   [3 1 1]
   [10 3 4]

   Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26, A = 0, B = 1, …, Z = 25. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

   Encryption:
   To encrypt the message "TARGET" using the 3x3 key matrix:
   K = [3 4 5]
   [2 1 3]
   [6 7 8]

   We first map each letter in the message to its corresponding numerical value using the mapping A = 0, B = 1, C = 2, ..., Z = 25:
   T A R G E T
   19 0 17 6 4 19

We then divide the plaintext into blocks of three letters each because the key is of a 3x3 matrix:

T A R
19 0 17
G E T
6 4 19

For each block, we multiply it with the key matrix modulo 26:

[3 4 5] [19] [10]
[2 1 3] x [0] = [1]
[6 7 8] [17] [20]

[3 4 5] [6] [23]
[2 1 3] x [4] = [1]
[6 7 8] [19] [22]

We then convert the resulting numerical values back to letters using inverse mapping.

10 1 20 23 1 22
K B U X B W

Therefore, the ciphertext for the message "TARGET" with the 3x3 key matrix is "KBUXBW."

Decryption:

To decrypt the ciphertext "KBUXBW" using the 3x3 key matrix, we first calculate the inverse of the key matrix modulo 26:

K^-1 = [-29 4 7]
[12 -1 -3]
[-3 1 0]

We then divide the ciphertext into blocks of three letters each:

K B U
10 1 20
X B W
23 1 22

For each block, we multiply it with the inverse key matrix modulo 26:

$$\begin{bmatrix} -29 & 4 & 7 \\ 12 & -1 & -3 \\ -3 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 10 \\ 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} -29 & 4 & 7 \\ 12 & -1 & -3 \\ -3 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 23 \\ 1 \\ 22 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 19 \end{bmatrix}$$

We then convert the resulting numerical values back to letters using inverse mapping.

19 0 17 6 4 19

T A R G E T **(20 marks)**

2. Suppose you work as a network administrator for a medium-sized company that has several departments, including HR, marketing, accounting, and IT. The company's network is segmented into different VLANs to enhance security and manage network traffic efficiently. However, the VLANs are currently isolated, and there is no communication between devices on different VLANs. Your director has tasked you with configuring inter-VLAN routing using Cisco Packet Tracer to enable communication between devices on different VLANs within the network. There are 4 VLANS (HR, marketing, accounting, and IT) and 4 subnetworks in the company, each subnetwork has 4 PCs of 4 different VLANS. You need to design and implement a simulation of the network using Cisco packet tracer. Label the devices and interfaces with proper IP addresses to make it understandable to your director. Show the communication between VLANS using message transfer or using ping.

(20 marks)

Annexure I

Finding Inverse of a Matrix:

Let's consider the following 3x3 matrix:

A = [1 2 3]
[4 5 6]
[7 8 9]

➔ The first step in finding the inverse of a matrix is to calculate its determinant. To calculate the determinant of a 3x3 matrix,

[a11 a12 a13]
[a21 a22 a23]
[a31 a32 a33]

we can use the following formula:

det(A) = a11(a22a33 - a23a32) - a12(a21a33 - a23a31) + a13(a21a32 - a22a31)

where aij represents the element in the i-th row and j-th column of the matrix A.

⇨ Using this formula, we can calculate the determinant of matrix A as follows:

det(A) = 1(5*9 - 6*8) - 2(4*9 - 6*7) + 3(4*8 - 5*7)
= 1(45 - 48) - 2(36 - 42) + 3(32 - 35)
= -3 - 12 + 9
= -6

Since the determinant of A is nonzero (-6 in this case), A is invertible.

➔ Next, we need to calculate the matrix of cofactors, which is a matrix where each element is the determinant of a 2x2 matrix obtained by removing the row and column containing that element from the original matrix and multiplying it by -1 if the sum of the row and column indices is odd. The matrix of cofactors can be denoted as C.

⇨ To find the matrix of cofactors for matrix A, we can use the following formula:

Cij = (-1)^(i+j) * det(Aij)

where Aij represents the matrix obtained by removing the i-th row and j-th column of matrix A.

⇨ Using this formula, we can calculate the matrix of cofactors for matrix A as follows:

C = [(5*9 - 6*8) -(4*9 - 6*7) (4*8 - 5*7)]
[-(2*9 - 3*8) (1*9 - 3*7) -(1*8 - 2*7)]
[(2*6 - 3*5) -(1*6 - 3*4) (1*5 - 2*4)]

$$= \begin{bmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{bmatrix}$$

➔ Next, we need to find the **adjoint matrix, which is the transpose of the matrix of cofactors.** The adjoint matrix can be denoted as adj(A).
To find the adjoint matrix for matrix A, we need to transpose the matrix of cofactors:

$$\text{adj}(A) = \begin{bmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{bmatrix}$$

➔ Finally, we can find the inverse of matrix A by dividing the adjoint matrix by the determinant:

$$A^{-1} = \text{adj}(A) / \det(A)$$

$$= \begin{bmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{bmatrix} / -6$$

$$= \begin{bmatrix} 1/2 & -1 & 1/2 \\ -1 & -2 & 1 \\ -1/2 & 2 & -1/2 \end{bmatrix}$$

Annexure II

Finding Modulo:

$a = a \bmod 26$

$-a = (-a+26) \bmod 26$