Information Technology University, Lahore, Pakistan

Linear Algebra (MT-121)

Assignment # 3, Fall 2024

Submission Deadline: Wednesday September 25, 2024 Maximum Marks: 100

- Late submissions will not be graded.
- The viva of this assignment will be conducted in the TA session.
- This Assignment will be conducted under the rules and guidelines of the ITU Honour Code, and no cheating will be tolerated (i.e., no discussion about the Assignment with other students, no plagiarism at all). Each student must be able to justify his/her work.

---

1. Inverse matrix **A** using the Gauss-Jordan method by Matlab code. [20]

$$A = \begin{bmatrix} 1 & -5 & 2 \\ 2 & 3 & 1 \\ -3 & 8 & 0 \end{bmatrix}$$

Note: You cannot use Matlab built-in functions in this question 1.

2. Encryption and Decryption of a message can be done using matrix multiplication using the following algorithm.

   (a) Suppose we are going to use the following the following 3×3 key matrix (encoding matrix) to encrypt this message.

$$K = \begin{pmatrix} 3 & 4 & 0 \\ 2 & 5 & 1 \\ 4 & 0 & 7 \end{pmatrix}$$

   (b) Convert the message into numbers as follows:
   Assign 0 to A, 1 to B, 2 to C and so on, and replace the message by numbers.
   e.g., ITU LAHORE can be written as 9, 19, 20, 26, 11, 0, 7, 14, 17, 4.

   (c) Since we are going to use a 3×3 key matrix to encode the message, we break the digital message up into a sequence of 3×1 column matrices as follows:

$$\begin{bmatrix} 9 \\ 19 \\ 20 \end{bmatrix}, \begin{bmatrix} 26 \\ 11 \\ 0 \end{bmatrix}, \begin{bmatrix} 7 \\ 14 \\ 17 \end{bmatrix}, \begin{bmatrix} 4 \\ 26 \\ 26 \end{bmatrix}$$

   (d) Group the message into numerical form. e.g., the above data in step (c) can be grouped as follows:

$$M = \begin{bmatrix} 9 & 26 & 7 & 4 \\ 19 & 11 & 14 & 26 \\ 20 & 0 & 17 & 26 \end{bmatrix}$$

   Note that i have assumed 26 for space (and padding at the end).

   (e) Multiplies each 3×1 vector by the key matrix K to encrypt the message.

   (f) Converts the resulting numbers back to letters (mod 27).

   (g) You can decrypt the message using Inverse of the matrix in part (d).

   Now you task is to assume a 3×3 key matrix **K** of your own choice, and then **write a MATLAB code** that

   (a) Reads a message from the user and converts this message into its numerical form. [10]

   (b) Groups the numbers into 3×1 vectors. [10]

   (c) Multiplies each 3×1 vector by the key matrix K to encrypt the message. [10]

   (d) Converts the resulting numbers back to letters (mod 27). [10]

   (e) Displays the encrypted message on the screen. [10]

(f) Computes the inverse of the key matrix modulo 27. [10]

(g) Multiplies the encrypted message by the inverse matrix to retrieve the original message. [10]

(h) Converts the decrypted numbers back to letters and display it to verify that the original message was recovered. [10]

Instructions:

- Use mod 27 for all calculations.
- If the length of the message is odd, add a padding character (like space=26) to make it even.