Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – MARCH 2026

Date: 10 – 03- 2026 **Time:** 02:00pm – 03:30pm

School: SOCSE	**Program:** B.Tech	
Course Code : CSE2502	**Course Name:** Cryptography and Network Security	
Semester: IV & VI	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	24	26	-	-	-

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **5Q x 2M=10M**

1	Define access control.	**2 Marks**	**L1**	**CO1**
2	Solve the Variant : Vigenere Cipher Plain Text : MEET ME AT NOON Secret Key : CASH Cipher text : _____	**2 Marks**	**L1**	**CO1**
3	What is Fermat's little theorem?	**2 Marks**	**L1**	**CO2**
4	Give difference between stream and block cipher.	**2 Marks**	**L1**	**CO2**
5	Define avalanche effect.	**2 Marks**	**L1**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Construct a Playfair matrix with the key "Security". Encrypt this message: "HELLOWORLD BCAV" using Playfair cipher.	**10 Marks**	**L2**	**CO1**
	b.	Explain the various types of security attacks in computer networks. Classify them as active and passive attacks, describe their working, objectives, and provide real-world examples. Discuss the potential impact of these attacks on network security and data confidentiality, integrity, and availability.	**10 Marks**	**L3**	**CO1**
		Or			
7.	**a.**	A message has been encrypted using the Hill cipher with a 2×2 key matrix and transmitted over an insecure channel. During reception, only the ciphertext and the key matrix are available at the receiver. Given: $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ Ciphertext: “HIAT”	**10 Marks**	**L2**	**CO1**
	b.	Apply Columnar Transposition Technique to encrypt the given plaintext: "plan is made to postponed until further order" Key : 3416725	**10 Marks**	**L3**	**CO1**

8.	**a.**	Explain the operation of a single round of the Data Encryption Standard (DES) algorithm with a neat block diagram.	**10 Marks**	**L3**	**CO2**
	b.	Using the Extended Euclidean Algorithm, find the multiplicative inverse of 731 modulo 2027, if it exists	**10 Marks**	**L3**	**CO2**
		Or			
9.	**a.**	Illustrate Feistel cipher Structure encryption process with neat diagram and mention its importance when compare with stream cipher encryption.	**10 Marks**	**L2**	**CO2**
	b.	Describe AES structure and its different bits of Block Enciphering and Deciphering process in detail with its individual processes of single round process	**10 Marks**	**L2**	**CO2**