Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 07-10-2025 **Time:** 09.30am to 11.00am

School: SOCSE	**Program:** B. Tech	
Course Code: CBD2504	**Course Name:** Data Security and Cryptography	
Semester: V	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**
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	Differentiate between Plaintext and Ciphertext.	**2 Marks**	**L2**	**CO1**
2	Define Brute Force attack?	**2 Marks**	**L1**	**CO1**
3	List the primary difference between a stream cipher and a block cipher?	**2 Marks**	**L1**	**CO2**
4	Name the two methods suggested by Shannon to frustrate statistical cryptanalysis.	**2 Marks**	**L1**	**CO2**
5	State the purpose of the permutation stage in a Feistel cipher?	**2 Marks**	**L1**	**CO2**

Part B

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

6.	**a.**	Demonstrate Classical Substitution Ciphers and their cryptanalysis.	**10 Marks**	**L3**	**CO 1**
		Or			
7.	**a.**	Decrypt the following cipher text using Hill Cipher. Key: $\begin{pmatrix} H & I \\ L & L \end{pmatrix}$ Ciphertext: FKMFIO	**10 Marks**	**L3**	**CO 1**
8.	**a.**	a) Check the properties of modular arithmetic based on 11 mod 8 = 3; 15 mod 8 = 7 b) Solve 11^7 mod 13	**10 Marks**	**L3**	**CO 1**
		Or			
9.	**a.**	a) Encrypt the following text using the PLAYFAIR CIPHER. Keyword: MODEL Plaintext: LETTER b) Encrypt the following text using the Rail Fence cipher d = 3 Plaintext: INFORMATION SECURITY IS ESSENTIAL IN THE DIGITAL AGE TO PROTECT DATA	**10 Marks**	**L3**	**CO 1**
10.	**a.**	Perform RSA encryption and decryption for the given values: p = 3, q = 7, e = 5, M = 10	**10 Marks**	**L3**	**CO 2**
		Or			
11.	**a.**	Demonstrate the concept of a primitive root in the context of Diffie-Hellman.	**10 Marks**	**L3**	**CO 2**
12.	**a.**	Demonstrate the Diffie-Hellman Key Exchange protocol with its steps and the secret key calculation.	**10 Marks**	**L3**	**CO 2**
		Or			
13.	**a.**	Demonstrate the Feistel Cipher structure in detail with a diagram.	**10 Marks**	**L3**	**CO 2**