Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 10- 12- 2025 **Time:** 1.00pm to 04.00pm

School: SOCSE	**Program:** B.Tech	
Course Code: IST2502	**Course Name:** Foundations of Cryptography and Information Security	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

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

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. **10Q x 2M=20M**

1.	State Fermat's Little Theorem.	**2 Marks**	**L1**	**CO1**
2.	For a prime number p, identify the value of Euler's Totient Function, ø(p).	**2 Marks**	**L1**	**CO1**
3.	List any two types of Active Attacks.	**2 Marks**	**L1**	**CO1**
4.	Identify the typical number of rounds in a standard Feistel cipher like DES.	**2 Marks**	**L1**	**CO2**
5.	Define block size of the DES encryption algorithm.	**2 Marks**	**L1**	**CO2**
6.	In DES, define the size of the subkey for each round.	**2 Marks**	**L1**	**CO2**
7.	Identify the size of the hash value produced by SHA-512.	**2 Marks**	**L1**	**CO3**
8.	Outline the main objective of message authentication.	**2 Marks**	**L1**	**CO3**
9.	Define the purpose of radix-64 encoding in PGP.	**2 Marks**	**L1**	**CO4**
10.	Name any two content types used in S/MIME.	**2 Marks**	**L1**	**CO4**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	1, Encrypt the following text using the PLAYFAIR CIPHER. Keyword: COMPARE Plaintext: HIDDEN 2, Encrypt the following text using the Rail Fence cipher d = 3 Plaintext: CRYPTOGRAPHY IS THE STUDY OF SECURE COMMUNICATION TECHNIQUES	**10 Marks**	**L3**	**CO1**
	b.	Explain the difference between Passive and Active security attacks with suitable examples.	**10 Marks**	**L2**	**CO1**
Or					
12.	**a.**	Decrypt the following cipher text using Hill Cipher. Key: $\begin{bmatrix} C & D \\ D & G \end{bmatrix}$ Ciphertext: APADJT	**10 Marks**	**L3**	**CO1**
	b.	Estimate the addition modulo 8 and multiplication modulo 8 and list out the additive and multiplicative inverse of modulo 8.	**10 Marks**	**L2**	**CO1**

13.	**a.**	Describe the overall structure and steps of the DES encryption process.	**10 Marks**	**L2**	**CO2**
	b.	Explain the Diffie-Hellman Key Exchange protocol with its steps and the secret key calculation.	**10 Marks**	**L2**	**CO2**
Or					
14.	**a.**	Explain the concept of a primitive root in the context of Diffie-Hellman.	**10 Marks**	**L2**	**CO2**
	b.	Explain the four transformations used in an AES encryption round.	**10 Marks**	**L2**	**CO2**

15.	**a.**	Differentiate between MD5 and SHA family of algorithms.	**10 Marks**	**L2**	**CO3**
	b.	Describe various message authentication requirements in network communication.	**10 Marks**	**L2**	**CO3**

Or					
16.	**a.**	List and explain the requirements of a digital signature.	**10 Marks**	**L2**	**CO3**
	b.	Explain why HMAC remains secure even when the underlying hash function has weaknesses.	**10 Marks**	**L2**	**CO3**

17.	**a.**	Describe the structure of the ESP (Encapsulating Security Payload) header and trailer, explaining each field and its purpose.	**10 Marks**	**L2**	**CO4**
	b.	Explain the phases of the SSL Handshake Protocol in detail.	**10 Marks**	**L2**	**CO4**
Or					
18.	**a.**	Explain statistical anomaly detection and rule-based intrusion detection methods, providing suitable examples.	**10 Marks**	**L2**	**CO4**
	b.	Explain the different types of firewalls, including packet-filtering, stateful inspection, application gateway, and circuit-level gateway firewalls.	**10 Marks**	**L2**	**CO4**