Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 08-12- 2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech	
Course Code: CBD2504	**Course Name:** Data Security and Cryptography	
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.	Define Masquerade attack.	**2 Marks**	**L1**	**CO1**
2.	State the mathematical formula for encryption in the Caesar Cipher.	**2 Marks**	**L1**	**CO1**
3.	If two numbers are relatively prime, identify their GCD.	**2 Marks**	**L1**	**CO1**
4.	In Diffie-Hellman, identify the parameter 'α' be relative to the prime 'q'.	**2 Marks**	**L1**	**CO2**
5.	Identify the type of attack exploits variations in the time taken to perform cryptographic operations.	**2 Marks**	**L1**	**CO2**
6.	Define the role of initial permutation (IP) in the DES algorithm.	**2 Marks**	**L1**	**CO2**
7.	Name any two common attacks against message authentication.	**2 Marks**	**L1**	**CO3**
8.	Define HMAC.	**2 Marks**	**L1**	**CO3**
9.	Outline the Security Association (SA) in IPsec.	**2 Marks**	**L1**	**CO4**
10.	List any two services provided by the ESP (Encapsulating Security Payload).	**2 Marks**	**L1**	**CO4**

Part B

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

11.	**a.**	1, State Euler's Theorem and check the equality for a=3;n=10; ø(10)=4. 2, Explain Euler Totient Function ø(n)	**10 Marks**	**L2**	**CO1**
	b.	Examine the different types of Specific Security Mechanisms as defined in the OSI security architecture.	**10 Marks**	**L3**	**CO1**
Or					
12.	**a.**	1, Encrypt the following text using the PLAYFAIR CIPHER. Keyword: PLANET Plaintext: PUZZLE 2, Encrypt the following text using the Rail Fence cipher d = 3 Plaintext: THE RAIL FENCE CIPHER IS A SIMPLE FORM OF TRANSPOSITION CIPHER	**10 Marks**	**L3**	**CO1**
	b.	1, State Fermat's Theorem and check the equality for P=5 and a=2 2, Estimate the GCD (55,22) using Euclid's GCD Algorithm.	**10 Marks**	**L2**	**CO1**

13.	**a.**	Examine the four transformations used in an AES encryption round.	**10 Marks**	**L3**	**CO2**
	b.	Describe the overall structure and steps of the DES encryption process.	**10 Marks**	**L2**	**CO2**
Or					
14.	**a.**	Perform RSA encryption and decryption for the given values: p = 7, q = 17, e = 11, M = 11	**10 Marks**	**L3**	**CO2**
	b.	Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 23 and a primitive root α = 5. If Bob has a public key YB = 10 , Estimate Bob's private key XB?	**10 Marks**	**L2**	**CO2**

15.	**a.**	Define a Public Key Infrastructure (PKI) and describe its architecture along with its major components.	**10 Marks**	**L2**	**CO3**

	b.	Illustrate and explain the digital signature generation and verification process with a neat diagram.	**10 Marks**	**L2**	**CO3**
Or					
16.	**a.**	Explain the essential requirements of a Message Authentication Code (MAC) and discuss the security mechanisms used to implement it.	**10 Marks**	**L2**	**CO3**
	b.	Explain the different management functions performed within a Public Key Infrastructure (PKI).	**10 Marks**	**L2**	**CO3**

17.	**a.**	Explain the structure and functions of IPsec, highlighting SAD, SPD, and IPsec packet processing.	**10 Marks**	**L2**	**CO4**
	b.	Describe the SSL Handshake Protocol phases in detail.	**10 Marks**	**L2**	**CO4**
Or					
18.	**a.**	What is distributed intrusion detection? Explain issues and architecture.	**10 Marks**	**L2**	**CO4**
	b.	Explain applications of blockchain in cybersecurity, including identity management, IoT security, and secure data sharing.	**10 Marks**	**L2**	**CO4**