Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – May/June 2026

Date: 18-05-2026 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** CSE	
Course Code: CSE2502	**Course Name:** Cryptography and Network Security	
Semester: IV & VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**24**	**24**	**26**	**16**	**10**

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.	Encrypt the plaintext "Asymmetric" using the Caesar Cipher.	**2 Marks**	**L1**	**CO1**
2.	Find the determinant modulo 26 of the matrix: $\begin{bmatrix}23 & 5\\13 & 7\end{bmatrix}$	**2 Marks**	**L1**	**CO1**
3.	State Fermat's Little Theorem.	**2 Marks**	**L1**	**CO2**
4.	What is the avalanche effect?	**2 Marks**	**L1**	**CO2**
5.	What is non-repudiation?	**2 Marks**	**L1**	**CO3**
6.	Define hash function.	**2 Marks**	**L1**	**CO3**
7.	What is a Man-in-the-Middle attack?	**2 Marks**	**L1**	**CO3**
8.	What is the purpose of IPSec policies?	**2 Marks**	**L1**	**CO4**
9.	Define TLS.	**2 Marks**	**L1**	**CO4**
10.	What is the role of a Certificate Authority (CA) in PKI?	**2 Marks**	**L1**	**CO5**

Part B

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

11.	**a.**	Using the Hill Cipher technique, decrypt the ciphertext "ZICVT WQNGRZG" with the key "HILL". The Hill Cipher operates based on matrix multiplication—apply the appropriate steps to recover the original plaintext.	**10 Marks**	**L2**	**CO1**
	b.	Explain rail fence technique and solve, encrypt the message "NETWORKSECURITY" using the Rail Fence cipher with 3 rails.	**10 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Compute the corresponding ciphertext for the message "SECRET" using the Hill cipher with the key $\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$ matrix.	**10 Marks**	**L3**	**CO1**
	b.	Explain the classification of security attacks. List the different types and describe their characteristics.	**10 Marks**	**L2**	**CO1**

13.	**a.**	Discuss the architecture of Advanced Encryption Standard in detail. Explain the complete block enciphering and deciphering processes, and elaborate on the transformations performed in each round of the algorithm.	**10 Marks**	L2	CO2
	b.	Explain the basic structure of a Feistel Cipher.	**10 Marks**	**L2**	**CO2**
		Or			
14.	**a.**	Explain the functionality of a Data Encryption Standard algorithm and also its single round in detail. Support your answer with a neat diagram.	**20 Marks**	**L2**	**CO2**

15.	**a.**	Explain the steps involved in the Diffie–Hellman key exchange algorithm. Consider that Alice and Bob agree on a common prime number q = 157 and a primitive root α = 5. a) If Alice selects a private key XA = 15, compute her public key YA. b) If Bob selects a private key XB = 27, compute his public key YB. c) Determine the shared secret key established between Alice and Bob using the Diffie–Hellman method.	**20 Marks**	L2	CO3
		Or			
16.	**a.**	Explain the steps involved in the RSA algorithm. Consider that Alice generates her RSA keys using two prime numbers p = 17 and q = 11. a) Compute n and $\phi(n)$. b) If the public key exponent is e = 7, determine the private key exponent d.	**20 Marks**	**L2**	**CO3**

		c) Using the generated keys, encrypt the message M = 9 and then decrypt it to verify the original message.			

17.	**a.**	Explain the concept of Kerberos authentication protocol. Illustrate its authentication process with a neat diagram.	**10 Marks**	L2	CO4
	b.	What are the requirements of IP Security policies? Also, explain the operations of the Encapsulating Security Payload (ESP) in detail.	**10 Marks**	**L2**	**CO4**
Or					
18.	**a.**	Describe the working principle of the SSL Handshake Protocol and illustrate its process using a neat state diagram.	**10 Marks**	**L2**	**CO**
	b.	Explain the operations of Pretty Good Privacy (PGP) and its authentication mechanism.	**10 Marks**	**L2**	**CO5**