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: CSE2502	**Course Name:** CRYPTOGRAPHY AND NETWORK SECURITY	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
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.	What is the use of extra filler characters in Playfair Cipher.	**2 Marks**	**L1**	**CO1**
2.	Encrypt the Plain Text " Asymmetric " using Caesar Cipher	**2 Marks**	**L1**	**CO1**
3.	Define Substitution and Transposition techniques	**2 Marks**	**L1**	**CO1**
4.	What is Avalanche Effect? :	**2 Marks**	**L1**	**CO2**
5.	Why do you require Fermat's little theorem and write it?	**2 Marks**	**L2**	**CO2**
6.	What do we find the two prime numbers are relatively prime?	**2 Marks**	**L1**	**CO2**
7.	Given p = 3, q = 7, e is Encryption key =5. What is the criteria of e = 5 to act as encryption key in RSA	**2 Marks**	**L3**	**CO3**
8.	State the importance of Diffie–Hellman key exchange technique in Public Key Cryptography?	**2 Marks**	**L2**	**CO3**
9.	List MIME Services and write a line on each	**2 Marks**	**L1**	**CO4**
10.	What is IP Sec. and its importance?	**2 Marks**	**L1**	**CO4**

Part B

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

11	**a.**	**Explain the categories of Active attack in detail.** Using the columnar transposition cipher with the keyword 'KEYWORD', encrypt the message ATTACK AT SIX AM MORNING'.	**10 marks**	**L3**	**CO1**
	b.	Hill Cipher is one substitution technique works on the principle of matrix multiplication. Given ciphertext as "**APADJ TFTWLFJ**" and key is **"HILL".** Decrypt the Given Cipher Text.	**10 marks**	**L3**	**CO1**
		Or			
12.	**a.**	Decrypt the Cipher Text "**ZICVTWQNGKZEIIGASXSTSLVVWLA"** Using Vigenere's Auto cipher with the key stream "**deceptive** "	**10 Marks**	**L3**	**CO1**
	b.	Explain the different security services defined in X.800 standard. List out the Specific security mechanisms. Explain any two in detail.	**10 Marks**	**L2**	**CO1**

13	**a.**	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**
	b.	Consider the equations ($X \equiv 3 \bmod 5$), ($X \equiv 1 \bmod 7$) and ($X \equiv 6 \bmod 8$). Solve for unknown variable 'X' using Chinese Remainder Theorem, find the integer values for different moduli was relatively prime or not?	**10 Marks**	**L3**	**CO2**
		Or			
14.	**a.**	Explain Single Round of DES Algorithm and its entire functionality with neat diagram	**10 Marks**	**L2**	**CO2**
	c.	Compute the first byte output of the Mix-Columns transformation for the following sequence of input bytes "6E 4C 90 EC" using the key matrix. $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$	**10 Marks**	**L3**	**CO2**

15.	**a.**	Justify the Security in Key –Exchange through Diffie-Hellman mechanism.	**10 Marks**	**L3**	**CO3**

	b.	Illustrate Message Authentication and Confidentiality using SHA-512 Logic and steps involved in it	**10 Marks**	**L3**	**CO4**
		Or			
16.	**a.**	Explain with a neat diagram Generic Model of Digital Signature Process	**10 Marks**	**L3**	**CO3**
	b.	Illustarte the message integrity, Message Authentication and Confidentiality using MAC – Authenticator.	**10 Marks**	**L3**	**CO3**

17.	**a.**	Illustrate the Concept of KERBOROS and its Authentication process with neat diagram.	**10 Marks**	**L4**	**CO4**
	b.	What are the requirement of IP Security Policies and ESP operations	**10 marks**	**L4**	**CO4**
		Or			
18.	**a.**	Justify the security services of TLS and its Role in Network Security.	**10 Marks**	**L4**	**CO4**
	b.	With a neat state diagram, Explain SSL Handshake Protocol working Principle in detail.	**10 marks**	**L2**	**CO4**