Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – MAY 2025

Date: 23-05-2025 **Time:** 01:00 pm –04:00 pm

School: SOCSE	**Program:** B. Tech- CAI/CBC/CCS/CDV/CIT/ COM/CSD/CSG/CSN	
Course Code: CSE3078	**Course Name:** Cryptography and Network Security	
Semester: IV	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**
Marks	**24**	**24**	**26**	**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. **10Q x 2M=20M**

1	Write short note on Cryptanalysis.	**2 Marks**	**L1**	**CO1**
2	How the polyalphabetic cipher differs from monoalphabetic cipher.	**2 Marks**	**L2**	**CO1**
3	Compare AES-128 and AES-256.	**2 Marks**	**L2**	**CO2**
4	S-Boxes inputs are s1{110010} & s2{100011} using DES. Find the outputs.	**2 Marks**	**L2**	**CO2**

שורה	מס' עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

5	What is a message authentication code?	**2 Marks**	**L1**	**CO3**
6	What are the properties a digital signature should have?	**2 Marks**	**L1**	**CO3**
7	How does a Man-in-the-Middle attack work?	**2 Marks**	**L1**	**CO3**
8	Name two types of cryptographic keys used in S/MIME.	**2 Marks**	**L1**	**CO4**
9	What are the two main layers of the TLS protocol?	**2 Marks**	**L1**	**CO4**
10	How does IPSec ensure data integrity?	**2 Marks**	**L1**	**CO4**

Part B

Answer the Questions **Total 80 Marks.**

11.	**a.**	Discuss the Key expansion process of AES algorithm.	**10 Marks**	**L3**	**CO1**
	b.	Construct a Playfair matrix with the key "*Security*". Decrypt this message: "*FUOQMPXNSPHQYRT*" using Playfair cipher. Use 'Z' as the bogus letter.	**10 Marks**	**L3**	**CO1**

Or

12.	**a.**	Describe the difference between One Time Pad and Vigenere cipher and Using the Vigenère cipher, encrypt the word "cryptographic" using the key "min"	**10 Marks**	**L3**	**CO1**
	b.	Apply Columnar Transposition Technique to encrypt the given plaintext: "plan is made to postponed until further order" Key : 3416725	**10 Marks**	**L2**	**CO1**

13.	**a.**	Using the extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1759. And also determine gcd(72345, 43215) using Euclidean algorithm.	**10 Marks**	**L3**	**CO2**
	b.	Describe the encryption and decryption process of Advanced Encryption Standard with proper diagram.	**10 Marks**	**L3**	**CO2**

Or

14.	**a.**	Compute the first byte output of the Mix Columns transformation for the following sequence of input bytes "97 EC C3 95" using the key matrix. $\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$	**10 Marks**	**L3**	**CO2**

	b.	A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over, If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint: Use Chinese Remainder Theorem).	**10 Marks**	**L3**	**CO2**

15.	**a.**	Brief about RSA Algorithm and also Compute encryption and decryption using RSA for the given data: p = 17, q = 31, e = 7 & M = 2	**10 Marks**	**L3**	**CO3**
	b.	Illustrate the Message Digest Generation using SHA-512 with neat diagram and analyze it Complexity level of Security.	**10 Marks**	**L2**	**CO3**

Or

16.	**a.**	Alice and Bob use the Diffie–Hellman key exchange technique with a Common prime q = 157 and a primitive root α= 5. a. If Alice has a private key X_A = 15, find her public key Y_A. b. If Bob has a private key X_B = 27, find his public key Y_B. c. What is the shared secret key between Alice and Bob?	**10 Marks**	**L3**	**CO3**
	b.	Analyze importance of HMAC and discuss about role of HMAC as authenticator through its functionality.	**10 Marks**	**L2**	**CO3**

17.	**a.**	Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers?	**10 Marks**	**L2**	**CO4**
	b.	Explain the operational description of PGP cryptographic functions in detail with suitable block diagrams.	**10 Marks**	**L2**	**CO4**

Or

18.	**a.**	Illustrate SSL Record Protocol Operation in web security.	**10 Marks**	**L2**	**CO4**
	b.	Illustrate the Encapsulating Security Payload (ESP) security services and functionality with neat diagram in IPsec.	**10 Marks**	**L2**	**CO4**

***** BEST WISHES *****