Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

Make Up Examinations – December 2025

Date: 30 – 12- 2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech	
Course Code: CSE3078	**Course Name:** Cryptography and Network Security	
Semester: MK	**Max Marks**: 100	**Weightage**: 50%

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

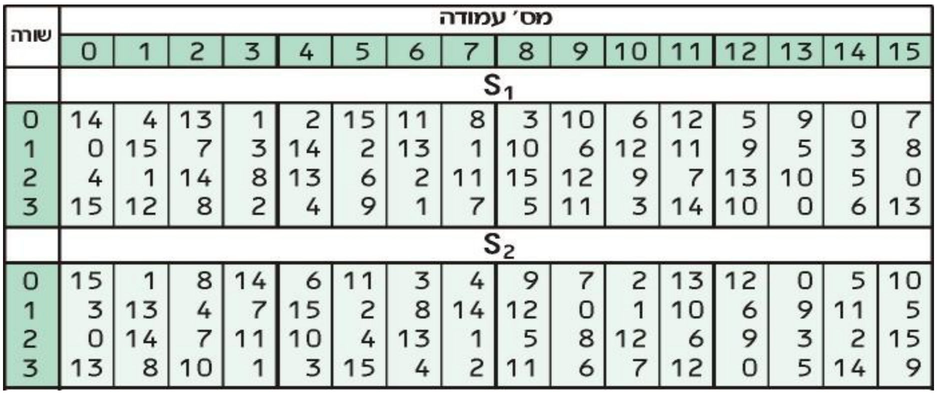
Instructions:

(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	Compare active and passive attacks.	**2 Marks**	**L2**	**CO1**
2	Write a short note on Steganography?	**2 Marks**	**L1**	**CO1**
3	Calculate the determinant mod 26 of $\begin{matrix} 23 & 5 \\ 13 & 7 \end{matrix}$	**2 Marks**	**L2**	**CO2**
4	S-Boxes inputs are s1{111111} & s2{110010} using DES. Find the outputs. 	**2 Marks**	**L2**	**CO2**
5	What is a message authentication code?	**2 Marks**	**L1**	**CO3**

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	4	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	3	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

6	List two disputes that can arise in the context of message authentication.	**2 Marks**	**L1**	**CO3**
7	What is a cryptographic hash function?	**2 Marks**	**L1**	**CO3**
8	Write a short note on IP Security (IPSec)?	**2 Marks**	**L1**	**CO4**
9	How does TLS ensure data confidentiality?	**2 Marks**	**L1**	**CO4**
10	State one difference between PGP and S/MIME.	**2 Marks**	**L2**	**CO4**

Part B

Answer the Questions **Total 80 Marks.**

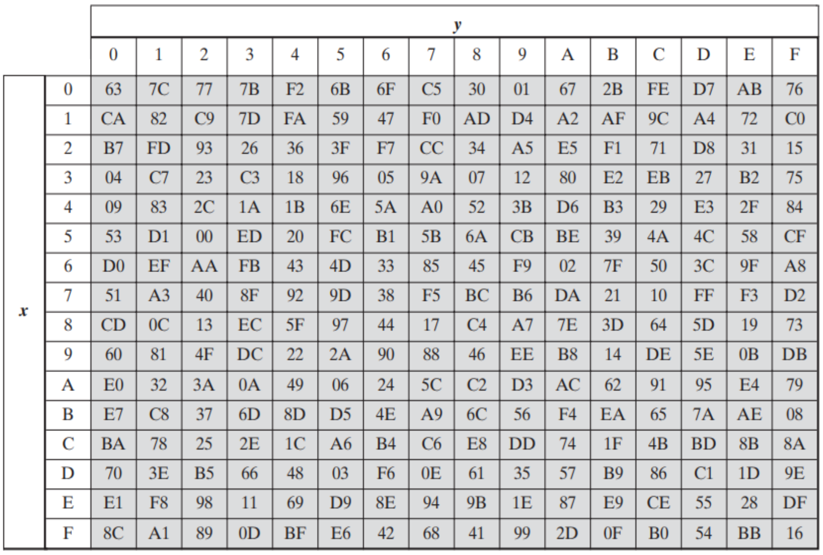
11.	**a.**	**i.** Apply brute-force cryptanalysis for the given ciphertext "sjybtwp xjhzwnyd" to get the original plaintext using Caesar cipher. **(5 Marks)** **ii.** To encipher the message “meet me after the DJ party” with a rail fence of depth 2. **(5 Marks)**	**10 Marks**	**L3**	**CO1**
	b.	Construct a Playfair matrix with the key "PRESIDENCY". Make a reasonable assumption about how to treat redundant letters in the key. Encrypt this message: "I only regret that I have but one life to give for my country".	**10 Marks**	**L3**	**CO1**

Or

12.	**a.**	Determine the inverse mod 26 of $\begin{matrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{matrix}$	**10 Marks**	**L3**	**CO1**
	b.	Compute the corresponding ciphertext for the message “ATTACK” 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**

13.	**a.**	Illustrate the Feistel cipher structure and discuss its design elements in detail.	**10 Marks**	**L2**	**CO2**
	b.	Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key {04040404 04040404 04040404 04040404} for Advanced Encryption Standard. a. Show the original contents of State, displayed as a 4 * 4 matrix. b. Show the value of State after initial AddRoundKey. c. Show the value of State after SubBytes.	**10 Marks**	**L3**	**CO2**

Table 5.2 AES S-Boxes



	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x 0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) S-box

Or

14.	**a.**	Compute the first byte output of the Mix-Columns transformation for the following sequence of input bytes “4D 90 4A D8” 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**
	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.**	What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end differentiate digital signature from digital certificate.	**10 Marks**	**L3**	**CO3**
	b.	Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 11 and a primitive root α = 2. a. If Bob has a public key Y_B = 3, what is Bob’s private key X_B? b. If Alice has a public key Y_A = 9, what is Alice’s private key X_A? c. what is the shared key K with Bob?	**10 Marks**	**L3**	**CO3**

Or

16.	**a.**	Using RSA Algorithm generate decryption key and perform encryption and decryption for the given data: p = 17, q = 11, e = 7 & M = 88	**10 Marks**	**L3**	**CO3**

	b.	Describes a man-in-the-middle attack on the Diffie–Hellman key exchange protocol in which the adversary generates two public–private key pairs for the attack.	**10 Marks**	**L2**	**CO3**

17.	**a.**	Describe in detail about Secure Socket Layer Architecture model 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**

Or

18.	**a.**	Describe the key elements of the Public Key Infrastructure Architectural Model with neat diagram.	**10 Marks**	**L2**	**CO4**
	b.	Evaluate the performance of S/MIME. Compare it with PGP.	**10 Marks**	**L2**	**CO4**