Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

School of Computer Science and Engineering

Mid - Term Examinations - November 2024

Semester: 05	**Date**: 05/11/2024
Course Code: CSE3078	**Time**: 02.00pm to 03.30pm
Course Name: Cryptography and Network Security	**Max Marks**: 50
Program: B.Tech	**Weightage**: 25%

Instructions:

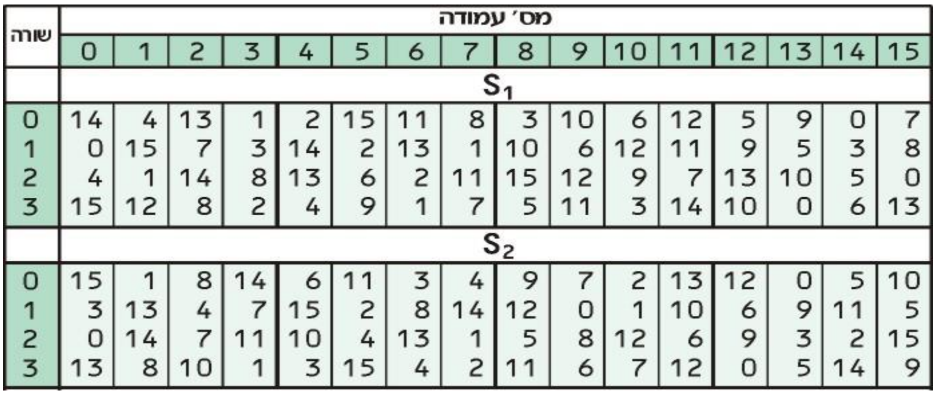
(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **5QX2M=10M**

1	List out the ingredients of symmetric encryption.	**2 Marks**	**L1**	**CO1**
2	What is meant by Denial-of-Service attack? Is it Active attack or Passive attack?	**2 Marks**	**L1**	**CO1**
3	Compare substitution cipher and transposition cipher in cryptography.	**2 Marks**	**L1**	**CO1**
4	List the parameters (block size, key size, and no. of rounds) for the three AES versions.	**2 Marks**	**L1**	**CO2**
5	S-Boxes inputs are s1{010010} & s2{000010} using DES. Find the outputs.	**2 Marks**	**L1**	**CO2**



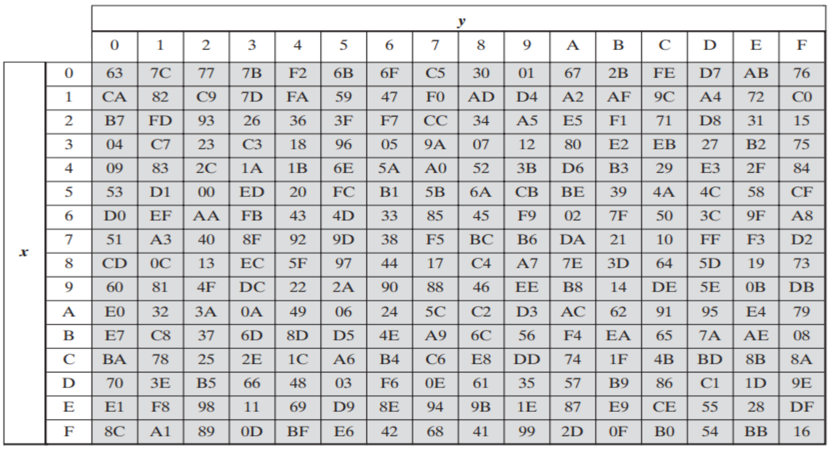
שורה	מס׳ עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12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

Part B

Answer ALL Questions. Each question carries 10 marks. **4QX10M=40M**

6	Compute the corresponding ciphertext for the word “SUNDAY” using the Hill cipher with the key $\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$	**10 Marks**	**L2**	**CO1**
	or			
7	Construct a Playfair matrix with the key “NETWORK SECURITY”. 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**	**L2**	**CO1**
8	**a.** Using the Vigenère cipher, encrypt the word “explanation” using the key “leg”.	**5 Marks**	**L2**	**CO1**
	b. Encrypt the given message "MEETING POSTPONED TOMORROW EVENING FIVE PM" using Railfence transposition technique. Depth=4.	**5 Marks**	**L2**	**CO1**
	or			
9	Determine the inverse mod 26 of $\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$	**10 Marks**	**L2**	**CO1**
10	Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key {03030303030303030303030303030303} 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**	**L2**	**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

d. Show the value of State after ShiftRows.

or

11 **10 Marks** **L2** **CO2**

Illustrate the structure of DES encryption algorithm and specify the operation of single round process in detail.

12 Compute the first byte output of the Mix-Columns transformation for the following sequence of input bytes “F2 4C E7 8C” using the key matrix. **10 Marks** **L2** **CO2**

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

or

13 State Chinese Remainder theorem and compute the value of X for the given set of congruent equations using CRT. Justify the given equation by applying X value. **10 Marks** **L2** **CO2**

$X \equiv 1 (\text{mod } 5)$
$X \equiv 2 (\text{mod } 7)$
$X \equiv 3 (\text{mod } 9)$
$X \equiv 4 (\text{mod } 11)$