Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 07-10-2025 **Time:** 09.30am to 11.00am

School: SOCSE	**Program:** B.TECH	
Course Code : CSE2502	**Course Name:** Cryptography and Network Security	
Semester: V	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**24**	**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. **5Q x 2M=10M**

1	What is meant by Avalanche Effect.	**2 Marks**	**L1**	**CO1**
2	Define Brute force attack.	**2 Marks**	**L1**	**CO1**
3	What is the need of S-Box operation in DES Algorithm	**2 Marks**	**L2**	**CO2**
4	Compare confusion and diffusion.	**2 Marks**	**L2**	**CO2**
5	Differentiate Block Cipher and Stream Cipher Enciphering and deciphering process.	**2 Marks**	**L2**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Encrypt the given message "MEETING POSTPONED TOMORROW EVENING FIVE PM" using Railfence transposition technique. Depth=4	**10 Marks**	**L3**	**CO 1**
		Or			
7.	**a.**	Describe the network security model with neat diagram and in detail	**10 Marks**	**L2**	**CO 1**

8.	**a.**	Mr. Veluchamy has sent a message "APADJ TFT" to Mr. Mohammed Rafi. Now that Mohammed Rafi is aware of the following values d=15, K= "HILL" but he doesn't know how to decrypt the message. If Mr.Mohammed Rafi is decrypting the given cipher Text using Hill cipher technique, What will be the Plain text?	**10 Marks**	**L4**	**CO 1**
		Or			
9.	**a.**	Perform Encryption using Vernam Cipher for Plain Text **OAK** Using Key = **SON.**	**10 Marks**	**L3**	**CO 1**

10.	**a.**	Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key {02020202020202020202020202020202} 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**	**CO 2**

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			
11.	**a.**	Illustrate the functionality of Single Round DES encryption algorithm with neat diagram	**10 Marks**	**L2**	**CO 2**

12.	**a.**	Compute the output of the MixColumns transformation for the following sequence of input bytes "87 6E 46 A6" using the Predefined key matrix. $\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$	**10 Marks**	**L4**	**CO2**
		Or			
13.	**a.**	Illustrate Feistal cipher Structure encryption process with neat diagram and mention its importance when compare with stream cipher encryption.	**10 Marks**	**L2**	**CO2**