Roll No

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - APR 2023

Semester : Semester IV - 2021
Course Code : CSE3078
Course Name : Sem IV - CSE3078 - Cryptography and Network Security
Program : All Programs

Date : 18-APR-2023
Time : 11:30AM - 1PM
Max Marks : 50
Weightage : 25%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(5 X 2 = 10M)**

1. List any two block cipher principles.
(CO1) [Knowledge]

2. How fermat's little theorem and euler's theorem are related each other?
(CO2) [Knowledge]

3. Mention the uses of Euler's theorem.
(CO2) [Knowledge]

4. Compare the key size and plain text size in AES and DES algorithm
(CO2) [Knowledge]

5. List the components of cryptosystem
(CO1) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(4 X 5 = 20M)**

6. Explain the network security model and its important parameters with a neat block diagram
(CO1) [Comprehension]

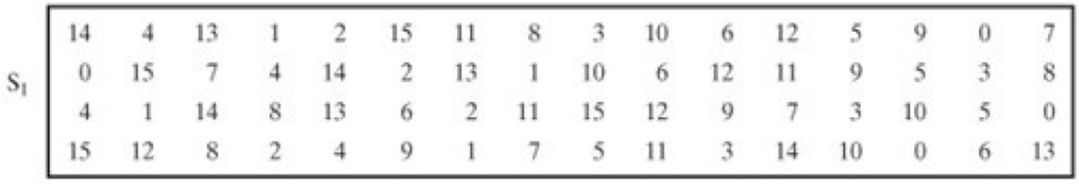
7. Use Brute Force to crack the following Caesar ciphertext, to identify the person encoded: BNQQNFRXYFQQNTLX
(CO1) [Comprehension]

8. Feistel structure is a well-known method to derive block cipher which divides the given input into two halves. Consider the following inputs:

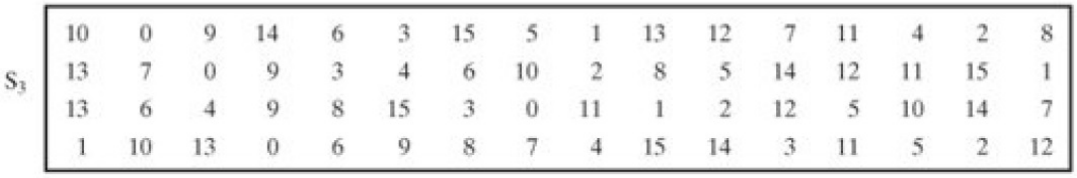
- Choose any 10 bits value as plain text,
- 5 bits key
- number of rounds = 4.
- Consider XOR as round function. Derive the corresponding cipher text using the fiestel structure concept.

(CO1) [Comprehension]

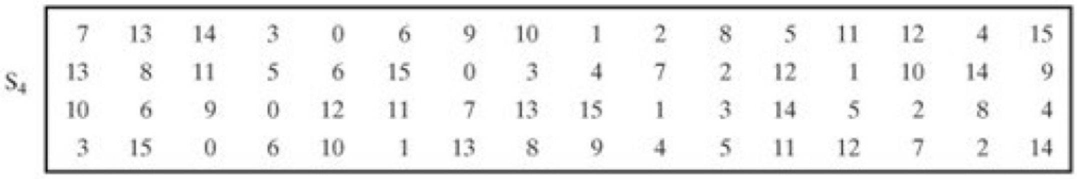
9. calculate the subsitution using DES S-boxes: a. S1(010101) b. S3(101010) c. S4(110110) d. S3(111111) e. S4(101101)



S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12



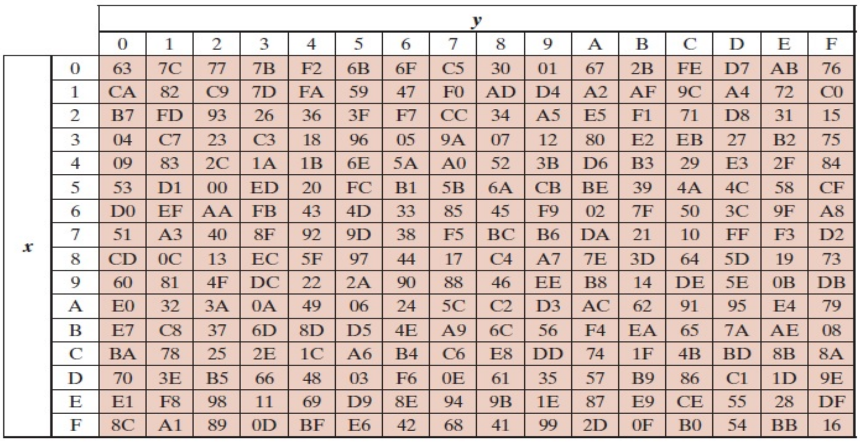
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

(CO2) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(2 X 10 = 20M)**

10. Given the plaintext {0F0E0D0C0B0A09080706050403020100}
a. Show the original contents of State, displayed as a 4 * 4 matrix.
b. Show the value of State after SubBytes using below S-box.
c. Show the value of State after ShiftRows.



		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

(CO2) [Application]

11. a. Compare the playfair cipher and hill cipher
b. Decrypt the following message using playfair cipher with the help of key: "Semester"
Message: XHIZGIMOGAMGOSVCCM

(CO1) [Application]