Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
MID TERM EXAMINATION - MAY 2023

Semester : Semester VI - B.Tech CSE - 2020
Course Code : CSE3078
Course Name : Sem VI - CSE3078 - Cryptography and Network Security
Program : B.Tech. Computer Science and Engineering

Date : 19-MAY-2023
Time : 2.00 PM - 3.30 PM
Max Marks : 60
Weightage : 30%

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. **Write the difference between diffusion and confusion**
(CO1) [Knowledge]
2. **Explain Euler's Theorem.**
(CO2) [Knowledge]
3. **List the components of cryptosystem.**
(CO1) [Knowledge]
4. **what is meant by relatively prime? Give an example**
(CO2) [Knowledge]
5. **Find 11^7 mod 13 using modular exponentiation?**
(CO2) [Knowledge]

PART B

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

6. **Use Vignere Cipher with key "HEALTH" to encrypt the message "Life is full of surprises"**
(CO1) [Comprehension]

7. **Encrypt the message "PAY" using hill cipher with the following key matrix:**

$$\begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

(CO1) [Comprehension]

8. **How is GCD calculated with Euclid's algorithm? Calculate the GCD(1970, 1066).**

(CO2) [Comprehension]

9. **Discuss the operations involved in each round of DES algorithm with necessary block diagram.**

(CO2) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(3 X 10 = 30M)**

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

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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. **Using the extended Euclidean algorithm, find the multiplicative inverse of**
    i. 400 mod 60
    ii. 391mod 52

(CO2,CO1) [Application]

12. **Define the type of security attack in each of the following cases:**
    i. A student breaks into a professor's office to obtain a copy of the next day's test.
    ii. A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.
    iii. A student sends hundreds of e-mails per day to another student using a phony return e-mail address.
    iv. A student received a circular from registrar later she find it as fake circular with the name of registrar.
    v. Ramesh is logged into his mail account and verifying an email from class coordinator. Harish observed his login credentials waiting to logout from his account and then Harish is trying to login with Ramesh credentials.

(CO1) [Application]