Exam Date & Time: 21-May-2022 (10:00 AM - 01:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

VI SEMESTER B.TECH END SEMESTER EXAMINATIONS, MAY 2022
PRINCIPLES OF CRYTOGRAPHY [CSE 4058]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions.

Instructions to Candidates:
Answer ALL questions Missing data may be suitably assumed

1) Illustrate four types of active attacks. (2)

A)

B) Eve captures Bob's Hill cipher machine, which uses a 2 x 2 matrix K. She tries a chosen plaintext attack. She finds that the plaintext BA encrypts to HC and the plaintext ZZ encrypts to GT. What is the matrix K? (4)

C) From the DES key K (in hexadecimal): 133457799BBCDFF1, derive K_1, the first-round subkey (in hexadecimal). Use the following tables in your computation. (4)

Table: PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Table: PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

2) Let $m(x) = x^8 + x^4 + x^3 + x + 1$ be an irreducible polynomial in $GF(2^8)$. Using extended Euclid's algorithm compute $(95)^{-1}$. (5)

A)

B) Design AES key expansion algorithm. (3)

C) Illustrate shiftRows in AES (2)

3) Illustrate two strengths and two weakness of cipher block chaining mode of operation. (2)

A)

B) Using Chinese remainder theorem, find the solution to the simultaneous equations:

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$ (5)

C) Generate a sequence of random numbers using Linear Congruential Generator in which a=5, c=0, X_0=1, and m=32. Is this design generating a full period? (3)

4) With neat table summarize important aspects of symmetric and public key encryption. (3)

A)

B) Perform encryption and decryption using the RSA algorithm for the following:

p = 5, q = 11, e = 3, M = 9 (4)

C) Illustrate three broad categories of applications of public key cryptosystems. (3)

5) With neat table illustrate six requirements for a cryptographic Hash functions. (5)

A)

B) With neat diagram illustrate man-in the-middle attack against hash function. (2)

C) With neat diagram illustrate Merkle hash function. (3)

-----End-----