REG. NO										

प्रज्ञानं ब्रह्म

Manipal

INSPIRED BY LIFE

MANIPAL INSTITUTE OF TECHNOLOGY
(Constituent Institute of Manipal University)
MANIPAL-576104

VI SEM B.Tech (CSE) DEGREE END SEM MAKE UP EXAM
CSE 324: CRYPTOGRAPHY & NETWORK SECURITY
DATE : xx- 05-2014

TIME : 3 HOURS MAX.MARKS : 50

Instructions to Candidates
- Answer any **FIVE** full questions.
- Missing data if any, may be suitably assumed.

1A. 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?

1B. What is the difference between diffusion and confusion?

1C. From the DES key K (in hexadecimal): 133457799BBCDFF1, derive K_1, the first-round subkey (in hexadecimal). Use the following tables in computation. (4+2+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

2A. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? Give examples.

2B. If the input to AES MIX Column transformation is "D4 BF 5D 30" (in bytes). Compute the output (in bytes).

2C. Explain output feedback (OFB) mode encryption and decryption process with neat diagram. State one advantage and one disadvantage of OFB. (2+4+4)

3A. Alice and Bob have the same modulus n for RSA, and encryption exponents e_A and e_B with $\gcd(e_A, e_B) = 1$. Charles sends them the same message m encrypted with these keys, resulting in the ciphertexts c_A and c_B. Eve intercepts both c_A and c_B. How can she find m?

3B. Perform encryption and decryption using RSA algorithm for the following:

$p = 17; q = 31; e = 7; M = 2$

3C. What primitive operations are used in RC4?

3D. The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality? (2+4+2+2)

4A. List and define the seven requirements for a cryptographic hash function?

4B. With neat diagram briefly explain five steps of message digest generation using SHA-512.

4C. Explain 3 approaches for producing message authentication. (3+4+3)

5A. Explain with neat diagram overall operation of the SSL record protocol.

5B. What is R64 conversion? Why R64 conversion useful for an email application?

5C. Distinguish between two modes of IPSec .

5D. With neat diagram explain the structure of PGP private key ring. (3+2+2+3)

6A. Define Authentication Header (AH) and state the security service it provides.

6B. Explain the difference between statistical anomaly detection and rule-based intrusion detection.

6C. What is the difference between worms and viruses? Give an example for each.

6D. State three advantages and three disadvantages of circuit-level firewalls. (2+3+2+3)