Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL 576104

(Constituent College of Manipal University)

FIRST SEMESTER M.Tech (Network Engg.) DEGREE END SEMESTER EXAMINATION, NOV/DEC 2015
SUBJECT: PRINCIPLES OF INFORMATION SECURITY – ICT 505
(REVISED CREDIT SYSTEM)

TIME: 3 HOURS **05/12/2015** **MAX. MARKS: 50**

Instructions to candidates

- Answer any **FIVE FULL** questions.
- Missing data, if any, may be suitably assumed.

1A. Write extended Euclidean algorithm to find the multiplicative inverse of 'd' modulo 'f'. Compute 7^{-1} mod 143.

1B. With neat diagrams explain how can you convert a password to a DES encryption key.

1C. What is the authentication mechanism used in S/MIME? Explain. (5+3+2)

2A. Find the inverse of (x^4+x^3+1) in $GF(2^5)$ using the modulus (x^5+x^2+1).

2B. What is the difference between Authentication Header and Encapsulating Security Payload. Discuss with their formats.

2C. Convert the raw data 145B51 into radix-64. (5+3+2)

3A. With neat block diagrams, explain the directory mechanism of providing security to the objects in a computer system. List and explain the disadvantages of this technique.

3B. Suggest a suitable solution to merge the PKIs shown in Fig Q.3B and also highlight the important features of the solution.

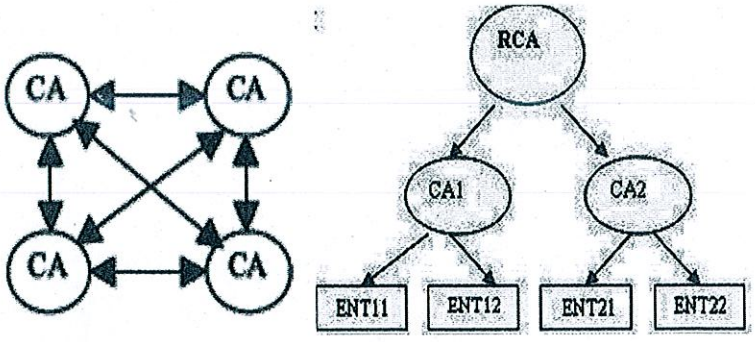

Fig. Q.3B

3C. Highlight the importance of separation mechanisms in multilevel databases. (5+3+2)

4A. List out the difference between Application Level Gateway and Circuit Level Gateway. Write packet-filter firewall security policies for the following:

i. Block all the packets transmitting from the inside host OURHOST through the port 25 to the internet

ii. Allow all the packets transmitting from the outside host THEIRHOST through the port 80 to the inside host OURHOST

4B. Discuss the mechanisms used for detecting database inconsistencies.

4C. What is a Bastion host? Explain its role in the network security. (5+3+2)

5A. What is a cyclic subgroup? Find the cyclic subgroup from the group $\mathbf{G} = \langle Z_6, + \rangle$.

5B. Suppose query Q1 obtains the median *m1* of a set S1 of values. Suppose query Q2 obtains the median *m2* of a subset S2 of S1. If $m1 < m2$, what can be inferred about S1, S2 and the elements of S1 not in S2.

5C. Discuss the header fields of MIME protocol.

(5+3+2)

6A. With a neat diagram explain all the fields of SSL protocol suite.

6B. What are the security problems associated with the cloud computing? Suggest the solutions for them.

6C. List and briefly describe the secure software requirements in cloud. (5+3+2)