Roll No .....

MCIT - 201

M.E./M.Tech., II Semester

Examination, July 2015

Information Security System

Time : Three Hours

Maximum Marks : 70

Note : Attempt any five questions.

1. a) The 10 bit key of S-DES is 1010000010. Find the subkeys K_1 and K_2, if
   P_{10} = 3 5 2 7 4 10 19 86 and
   P_8 = 6 3 7 4 8 5 10 9
   b) Describe the block cipher modes of operation in detail.

2. a) Define Message authentication. Explain message authentication code and one way Hash functions.
   b) Explain Chinese remainder theorem with example.

3. a) Explain the algorithms to solve the intractable problems.
   b) What is integer factorization problem? Explain with example.

4. a) In Diffie Hellman key exchange, q = 71, Its primitive root $\alpha = 7$, A's private key is 5, B's private key is 12. Find
      i) A's Public Key
      ii) B's Public Key
      iii) Shared Secret Key
   b) Explain the signing and verifying functions of Digital Signature Algorithm (DSA).

5. a) Explain SSL protocol stack with a neat diagram and define the parameters used in session and connection states.
   b) Explain authentication method based on challenge/Response tokens.

6. a) What are the four basic techniques of choosing Passwords? Compare their relative merits.
   b) Explain MQV algorithm.

7. a) Differentiate between Kerberos Version 4 and Version 5. Define options, and Nonce fields of version 5 dialogue.
   b) Explain elliptic curve cryptography.

8. Write short notes on the following :
   a) Blowfish
   b) Discrete logarithmic problem
   c) Hidden monomial crypto system

******