*Total No. of Questions : 8]* *[Total No. of Printed Pages :2*

**Roll No** ..................................

# MCIT - 201

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

Examination, June 2016

## Information Security System

*Time : Three Hours*

***Maximum Marks : 70***

*Note:* i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Describe conventional encryption model. What are the requirements for secure use of conventional encryption. 7

   b) What are the block cipher design principles and their modes of operation? 7

2. a) What are the differences between conventional encryption and public key encryption? 7

   b) What are three broad categories of applications of public-key cryptosystems? 7

3. a) Explain why the security of RSA depends on the difficulty of factoring large numbers. 7

   b) Explain Diffie-Hellman key exchange algorithm. Calculate secret shared key if h = 17, g = 13, x = 3 and y = 7. 7

4. a) What are the various requirements for a hash function to be used for message Authentication? 7

   b) Describe modulo arithmetic with its properties. 7

5. What are Kerberos? Write the working principle of Kerberos. 14

6. Explain the following term: 14

   a) Digital signatures

   b) Entity Authentications

7. a) Briefly explain elliptic curve encryption/decryption using suitable example. 7

   b) Discuss discrete logarithm problem with example. 7

8. Write a short notes on any two : 14

   a) SHA -1

   b) Modular square root

   c) Zero knowledge protocol

******