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

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

# MCIT-201

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

Examination, December 2016

## Information Security System

***Time : Three Hours***

***Maximum Marks : 70***

*Note:* i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Explain one time pad method of Cryptography with a suitable example. What are two fundamental limitations? 7

b) List and briefly define types of Cryptanalytic attacks based on what is known to the attacker? 7

2. a) What is DES? Define Avalanche effect in DES. What are major strength of DES? 7

b) Describe stream Ciphers based on linear feedback shift registers. 7

3. a) What is Euclid's algorithm? With a suitable example explain the process of finding out GCD. 7

b) What type of attacks are addressed by message authentication? Name two approaches to provide message authentication. 7

4. a) Draw and explain MD5 Secure Hash Algorithm. What are its strengths. 7

b) What is Chinese Remainder theorem? Explain. 7

5. a) What do you mean by Intractable problems? Explain RSA problem. 7

b) Explain some known algorithms for solving the Intractable problems. 7

6. a) Describe Diffie-Hellman key exchange method in detail. 7

b) Write a short note on Digital Signatures. 7

7. a) Draw and explain KERBEROS. Differentiate version 4 and 5. 7

b) Explain Elliptic Curve method of Cryptography. 7

8. Write short notes on any two : 14

a) IP Security

b) SSL

c) Birthday Attack

******