Total No. of Q

Roll No .....

MCIT-201

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

Examination, November 2019

Information Security System

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

iii) Assume suitable data if missing.

1. a) What are the key principles of information security? Differentiate conventional (symmetric) from public key (asymmetric) encryption. 7

   b) What are Cipher Feedback Block (CFB) and Output Feedback Block (OFB)? Explain both with neat diagram. 7

2. a) Explain the operation of double DES? Give some of the disadvantages of double DES? 7

   b) Describe the RC5 method used for encryption and decryption? 7

3. a) Compare MD5 and SHA algorithms. Also draw the working logic diagram for both methods. 7

   b) Analyse why Modular arithmetic and prime numbers are used in cryptography or information security? 7

4. a) Evaluate the security services provided by digital signature? Also list the requirement of hash function. 7

   b) Describe the Chinese remainder theorem with suitable example. 7

5. a) Explain the problem of integer factorization and modular square root problem with example. 7

   b) Describe the signature schemes with example. 7

6. a) Apply the mathematical foundations of RSA algorithm. Perform encryption and decryption for the following data. P = 17, q = 7, e = 5, n = 119, message = "6". Use Extended Euclid's algorithm to find the private key. 7

   b) Explain briefly about Diffie-Hellman key exchange algorithm with its pros and cons? 7

7. a) Illustrate a client C who wants to communicate with a server S using Kerberos protocol. How can it be achieved? 7

   b) What is Lattice? Give the applications of lattice in cryptography? 7

8. Write short notes on: 14

   i) Zero Knowledge Protocol

   ii) Elliptic Curve Cryptography

   iii) PKI

******