Roll No .....

MCIT - 201

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

Examination, December 2015

Information Security System

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Explain DES Encryption method. Write the strength of DES. 7

   b) What is the difference between linear and differential Cryptanalysis? 7

2. a) Write the principles of Block Cipher. Why do some block cipher modes of operation only use encryption while other use both encryption and decryption. 7

   b) What is the stream Cipher? Explain the stream ciphers based on linear feedback shift registers. 7

3. a) Write the properties of modulo operator. Explain Chinese remainder theorem. 7

   b) What basic arithmetical and logical functions are used in MD5? 7

4. a) Compare SHA-1 and MD5 techniques. Also write compression functions. 7

   b) What is the difference between little endian and big-endian format? 7

5. a) What is Diffie-Hellman problem? Explain any one algorithm to solve this problem. 7

   b) What are the principal elements of a public key cryptosystem? Write the role of public key and private key. 7

6. a) List four general categories of schemes for the distribution of public keys. 7

   b) Briefly explain Diffie-Hellman key exchange. 7

7. a) Draw a diagram and explain the term KERBEROS. 7

   b) Describe Digital Signature. What are the properties of a digital signature should have? 7

8. Write short notes on any two : 14

   a) Elliptic Curve Cryptography

   b) PKI

   c) Modular square root problem

   d) Integer factorization problem

******