Total No. of Questions :10] [Total No. of Printed Pages :2

Roll No ....

MCIT - 201

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

Examination, June 2014

Information Security System

Time : Three Hours

Maximum Marks : 70

Note : i) Attempt all questions.

ii) All questions carries equal marks.

UNIT - I

1. a) Explain the terms Logic Bomb, Trojan Horses and Trap doors. 7

b) Discuss the various code-breaking methodologies. 7

Or

2. a) With suitable diagrams explain the concept of public-key cryptography. 7

b) Describe in detail RC 5 algorithm. 7

UNIT - II

3. a) Discuss the working principle of hash function. 7

b) Enlist the attacks on hash function. Explain Birthday attack. 7

Or

4. a) Explain SHA-1 algorithm with basic arithmetic and logic functions used. 7

b) Explain primality testing and chinese remainder theorem used in modular arithmetic. 7

UNIT - III

5. a) Explain the different Intractable problems in short. 7

b) Enlist the features of IFP and DLP. 7

Or

6. a) Explain RSA problem and Diffie-Hellman problem. 7

b) Describe the different algorithms known for solving intractable problems. 7

UNIT - IV

7. a) Discuss the Diffie-Hellman algorithm of key exchange. 7

b) What is digital signature? Describe Elgamal digital signature scheme. 7

Or

8. a) Write and explain RSA algorithm with the help of a suitable example. 7

b) Explain the terms Entity authentication. 7

UNIT - V

9. a) What is Secure Socket Layer? Explain its architecture. 7

b) Explain Kerberos with its working principle. 7

Or

10. Write short notes: 14

i) Hyper-elliptic curve cryptography.

ii) Hidden monomial cryptosystems.

******