Roll No. .... Total Pages : 2

BT-8/M-20 38195

INFORMATION SECURITY

Paper–IT-406-N

Time Allowed : 3 Hours] [Maximum Marks : 75

Note : Attempt five questions in all, selecting at least one question from each Unit. All questions carry equal marks.

UNIT–I

1. What are the various types of security attacks? Why is the security needed in Computers? 15

2. Discuss in detail about symmetric and asymmetric key cryptography techniques. 15

UNIT–II

3. What is the principle of Block Cipher? What is the working of encryption function? 15

4. Discuss in detail about Diffie-Hellman and ECC algorithms. 15

UNIT–III

5. What do mean by secure hashing technique? Compare SHA-1 and SHA-256 algorithms. 15

38195/K/1034 P. T. O.

6. What is hash function? How do digital signature provide more authenatication to the data? 15

UNIT–IV

7. What are the Intruders? How is an Intrusion detected? What are the related threats due to Intrusion? 15

8. What do mean by E-mail security? Write short notes on Pretty Good Privacy and S/MIME. 15