Roll No. ..... Total Pages : 2

48364

BT-8/D-23

INFORMATION SECURITY

Paper : OE-IT-410A

Time : Three Hours] [Maximum Marks : 75

Note : Attempt *five* questions in all, selecting at least *one* question from each unit.

UNIT–I

1. (a) Why is Confidentiality an important principle of security? Explain methods to ensure and maintain confidentiality. (8)

(b) Why are certain attacks labelled as passive, and why are others classified as active? Discuss active attacks. (7)

2. (a) What distinguishes a substitution cipher from a transposition cipher? Explore the concept of the Caesar cipher in detail. (8)

(b) What are Encryption and Decryption? Illustrate these processes with a block diagram depicting plaintext, ciphertext, encryption, and decryption. (7)

UNIT–II

3. (a) Differentiate between differential and linear cryptanalysis methods. (5)

(b) Discuss the idea of Block Cipher modes with detailed explanation. (10)

4. (a) Explain Diffie-Hellman key exchange algorithm using suitable example. (8)

(b) Discuss the principles of public key crypto systems. (7)

UNIT–III

5. (a) What is the important aspect that establishes trust in Digital Signature? Explain. (8)

(b) Discuss the idea of Secure Hash Algorithm. (7)

6. (a) How does Kerberos works? Explain. (8)

(b) Discuss the concept of Biometric authentication. (7)

UNIT–IV

7. Write short notes on :

(i) Pretty Good Privacy.

(ii) S/MIME. (15)

8. (a) List the characteristics of a good firewall implementation. How is a circuit gateway different from an application gateway? (8)

(b) What is Intrusion Detection System? Explain in detail. (7)