

**Time: 3 Hours****Max. Marks: 60****Note:** This question paper contains two parts A and B.

Part A is compulsory which carries 20 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 8 marks and may have a, b, c as sub questions.

PART - A**5 × 4 Marks = 20**

- 1.a) What is cryptanalysis and cryptography? [4]
- b) What are roles of public and private key? Specify the applications of the public key cryptosystem. [4]
- c) What are the requirements for message authentication? [4]
- d) Why does PGP generate a signature before applying compression? [4]
- e) What is IP address spoofing? [4]

PART - B**5 × 8 Marks = 40**

- 2.a) Explain Active attacks and Passive Attacks.
 - b) What is mono alphabetic cipher? How it is different from Caesar cipher? [4+4]
- OR**
3. Discuss the following:
 - a) A model for internetwork security.
 - b) Steganography. [4+4]
 4. Explain Blowfish in detail. [8]
- OR**
5. Discuss the following:
 - a) Public-key Cryptography Principles
 - b) RC4 Algorithm [4+4]
 6. Describe the authentication dialog used by Kerberos for obtaining services from another realm. [8]
- OR**
7. Explain the X.509 authentication service. [8]
 - 8.a) How can the signed data entity of S/MIME be prepared?
 - b) Explain the general format of PGP message. [4+4]
- OR**
- 9.a) What do you mean by Security Association? Illustrate the parameters that identify the Security Association.
 - b) Describe IP security Architecture. [4+4]
 10. What is the importance of web security? Explain how secure socket layer provides the reliable service. [8]
- OR**
11. Explain statistical anomaly detection and rule based intrusion detection system. [8]

