

Question Paper consists of FIVE units, each carrying 14 marks
 Each unit has TWO questions; either of them should be answered
 All parts of a question must be answered at one place.

UNIT-I

Marks

1. a) Explain the primary goals of network security and classify different types of cryptographic attacks. 7M
 - b) Describe the structure and working of the Data Encryption Standard (DES) algorithm. 7M
- (OR)

2. a) Define symmetric key cryptography. Explain the mathematical principles behind symmetric key algorithms. 7M
- b) Explain the Advanced Encryption Standard (AES) architecture and its transformation functions. 7M

UNIT-II

3. a) Explain the mathematical foundations of asymmetric key cryptography including prime numbers and modular arithmetic. 7M
 - b) Describe the working principle and algorithmic steps of the RSA Cryptosystem with an example. 7M
- (OR)

4. a) Compare and contrast RSA, ElGamal, and Elliptic Curve Cryptosystems. 7M
- b) Discuss the process of primality testing and its importance in public key cryptography. 7M

UNIT-III

5. a) Define a cryptographic hash function. Explain the desirable properties of a secure hash function. 7M
 - b) Describe the working of the SHA-3 algorithm with its key design principles. 7M
- (OR)

6. a) Explain the concept and working of the ElGamal Digital Signature scheme. 7M
- b) Write short notes on Schnorr Digital Signature and NIST Digital Signature Algorithm (DSA). 7M

UNIT-IV

7. a) Explain symmetric key distribution using asymmetric encryption with a neat diagram. 7M
 - b) Discuss the role of X.509 certificates in public key infrastructure (PKI). 7M
- (OR)

8. a) Explain the architecture and working of the Kerberos authentication protocol. 7M
- b) Describe the principles of Remote User Authentication using asymmetric key encryption. 7M

UNIT-V

9. a) Explain the architecture of Secure/Multipurpose Internet Mail Extensions (S/MIME) and its security features. 7M
 - b) Discuss the various security threats in electronic mail communication and their countermeasures. 7M
- (OR)

10. a) Describe the IP Security (IPSec) architecture and explain the Encapsulating Security Payload (ESP) protocol. 7M
- b) Explain the Internet Key Exchange (IKE) mechanism used for establishing Security Associations (SA). 7M