UNIT I

1. Discuss the various security attacks, mechanisms, services
2. Summarize OSI security architecture model with neat diagram.
3. Illustrate the Classical Encryption Technique with an example(substitution Techniques Transposition Techniques)
4. Explain the network security model and its important parameters with a neat block diagram
5. Define Steganography? Describe various techniques used in Steganography.

UNIT II

6. Describe Modulo Arithmetic operations and properties in detail.
7. Describe AES algorithm with all its round functions in detail.
8. Describe DES algorithm with neat diagram and explain the steps.
9. Solve gcd(98, 56) using Extended Euclidean algorithm. Write the algorithm also
10. Explain about Block cipher design principles – Block cipher mode of operation.
11. Discuss about RC4 Symmetric-Key Distribution

UNIT III

12. Explain Chinese Remainder theorem and find X for the given set of congruent equation using CRT
13. State and Prove Fermat's theorem.
    Discuss the Diffie-Hellman key exchange algorithm with its merits and demerits.
14. Describe RSA algorithm
15. Discuss the ElGamal cryptosystem and elliptic curve cryptosystem

UNIT IV

16. What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end .differentiate digital signature from digital certificate.
17. Describe SHA2 in detail with neat diagram.
18. Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers?
19. Explain in detail about X.509 authentication services.

UNIT V

20. Describe PGP cryptographic functions in detail with suitable block diagrams.
21. Describe in detail about S/MIME.
22. Describe in detail about SSL/TLS.
23. Explain the architecture of IPsec in detail in detail with a neat block diagram.
24. Illustrate the various types of firewalls with neat diagrams.
25. Explain intrusion detection system (IDS) in detail with suitable diagrams.(also study about Honey pot)
26. Elaborate how secure electronic transaction (SET) protocol enables e- transactions. Explain the components involved.