Unit I

1. Explain data confidentiality,data authentication and data integrity.
2. Explain generation of encryption matrix in play fair cipher.
3. Explain one time pad cipher with example.
4. Explain rail fence Cipher technique
5. Define the term – confusion, diffusion
6. Use Hill cipher to encrypt the text DEF. The key to be used is

   2 4 5

   9 2 1

   3 8 7

7. Using playfair cipher encrypt the plaintext "Why, don't you?". Use the key "keyword".
8. What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.
9. Define the term cryptanalysis. Explain various types of cryptanalytic attacks.
10. Give examples of replay attacks. List three general approaches for dealing with replay attacks.
11. Encrypt the message "Exam" using the Hill cipher with the key
    2 4 5
    9 2 1
    3 8 7

12. When an encryption scheme is said to be unconditionally secure and computationally secure?
13. Which type of substitution is called monoalphabetic substitution cipher?
14. Which two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext?
15. Use playfair algorithm with key "monarchy" and encrypt the text "jazz".
16. What is security Services? Explain any three types of security services
17. Explain Vegenere Cipher.
18. Explain various types of attack on computer system.
19. What is security mechanism? List and explain various security mechanism.
20. Explain the conventional security model used for information security.
21. Explain cryptanalysis. Discuss any one technique for it
22. What attacks can be done on encrypted text? Explain them.
23. Explain play fair cipher with suitable example.
24. Define the terms threat and attack. List and briefly define categories of security attacks.
25. List and briefly define the security services.

26. Construct a playfair matrix with the key “occurrence”. Generate the cipher text for the plaintext “Tall trees”
27. Define the terms diffusion and confusion. What is the purpose of S-box in DES?
28. Explain the avalanche effect in DES.
29. Explain monoalphabetic cipher and polyalphabetic cipher by giving an example.
30. What is cryptography?

Unit-II

1. With example explain function of s-box in DES.

2. Explain various steps of AES in short.

3. Explain single round of DES algorithm.

4. Explain the steps involved in International data encryption standard algorithm

5. Explain scheme for DES encryption.

6. Define Block Cipher. Explain Design Principles of block cipher.

7. Explain DES algorithm with Figure.

8. Explain Sub key generation Process in Simplified DES algorithm with Example.

9. Explain limitation of DES in detail.

Unit 3

1. Explain cipher feedback mode of operation
2. Explain Modes of Operations.
3. Why mode of operation is defined? Explain the block cipher modes of operation?

Unit -4

1. Explain Diffie - Hellman key exchange algorithm.
2. Explain RSA algorithm with example.

3. The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and calculate the ciphertext if the given plaintext is 7.
4. Perform encryption using the RSA algorithm.
   p=3,q=11(two random numbers).
   e(encryption key)=7
   M(plaintext message)=5
5. What is primitive root? Explain Diffi-Hellmen key exchange algorithm with proper example.
6. Elaborate various kinds of attacks on RSA algorithm.
7. Compare public key and private key cryptography. Also list various algorithms for each
8. Briefly explain the model of Asymmetric Cryptosystem.
9. Explain RSA algorithm and list the possible approaches to attacking it.
10. Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5.
11. Compare conventional encryption with public key encryption.
12. What is a trap-door one-way function? What is its importance in public key cryptography?
13. Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.
14. What is the difference between weak and strong collision resistance?

Unit 5

1. Describe MD5 message digest algorithm.
2. What characteristics are needed in a secure hash function?
3. Write the properties of hash functions.
4. Explain SHA512 Algorithm.
5. What characteristics are needed in a secure hash function?

Unit 6

1. What is MAC? Explain HMAC.
2. How following can be achieved with message authentication: Message authentication, Message authentication and confidentiality
3. How message authentication code can be used to achieve message authentication and confidentiality

Unit 7

1. What is digital signature? Explain its use with the help of example.
2. List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.

Unit 8

1. Explain key distribution using KDC. [
2. In symmetric encryption, Describe the ways in which key distribution can be achieved between two parties A and B?
3. What is the purpose of X.509 standard?
4. Which techniques are used for the distribution of public keys?
5. Explain Key Distribution methods.
6. List and Explain various key management techniques.
7. Discus the ways in which public keys can be distributed to two communication parties.

Unit 9

1. Explain authentication mechanism of Kerberos.
2. What four requirements were defined for Kerberos?
3. Explain Kerberos Authentication System
4. What problem was Kerberos designed to address?
5. Briefly explain how session key is distributed in Kerberos.