Unit-1

1. Explain the following with Example
    - i. Confidentiality
    - ii. Authentication
    - iii. Integrity
    - iv. Non Repudiation
    - v. Access Control
2. List & Briefly define Security Attacks.
3. Define Cryptography and cryptanalysis
4. Draw and explain Conventional Cryptosystem.
5. Compare the following :
    - i. Active and Passive attack
    - ii. Worms , Virus , Trojan Horse
6. Construct Playfair matrix with the Key = ENGINEERING
   And Encrypt the message = TEST THIS PROCESS
7. Explain Monoalphabetic , Polyalphabetic ,One time pad cipher by giving an Example.
8. Encrypt the Message "Good morning" using the Hill Cipher with
   the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$.

9. Explain Transposition Techniques.
10. Explain Steganography Techniques.
11. Briefly describe attacks on Encrypted text.
12. Explain Security services and Security Mechanism.

Unit-2 & 3

1. Explain the following terms :
    - i. Block Cipher
    - ii. Stream Cipher
    - iii. Diffusion
    - iv. Confusion
2. The exact realization of feistel network depends on the choice of which Parameters?

3. Draw and explain the single round of DES encryption algorithm. Explain limitation of DES and also explain Avalanche effect in DES.
4. Explain triple DES with two keys and write about proposed attacks on 3DES.
5. Draw and explain the AES strcture.
6. List and explain various block cipher modes of operation with the help of diagram.

Unit-4

1. Write four possible approaches to attacking the RSA algorithm
2. What is primitive root? Write and explain the Deffie-Hellman key exchange algorithm. Is it vulnerable to man in the middle attack? Justify.
3. What is an elliptic curve? What is the zero point of an elliptic curve?
4. Give the steps of RSA algorithm.
5. Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5.
6. How key exchange using elliptic curves can be done?
7. In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?
8. Explain RSA algorithm and list the possible approaches to attacking it.

Unit-5 & 6

1. Illustrate the overall operation of HMAC. Define the terms.
2. Explain different characteristics of hash function
3. Explain the general structure of secure hash functions.
4. Explain briefly basic uses of CMAC, HMAC, DAA.
5. Explain briefly basic uses of MAC
6. Explain MD5 Hash Algorithm.
7. Illustrate variety of ways in which hash code can be used to provide message authentication.

8. What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is used.
9. Explain the following properties of hash function
   (i) One way property
   (ii) Weak collision resistance
   (iii) Compression function in hash algorithm.
10. What characteristics are needed in a secure hash function?
11. What is the difference between weak and strong collision resistance?
12. Explain SHA512 algorithm.
13. What is the need for message authentication? List various techniques used for authentication. Explain any one.
14. Explain the operation of secure hash algorithm on 512 bit block.
15. Is message authentication code same as encryption? How message authentication can be done by message authentication code?

Unit - 7 , 8, 9

1. Explain the one –way and two way authentication in X.509.
2. Explain the ticket granting server(TGS) scheme in Kerberos.
3. Explain X.509 authentication service.
4. Explain Kerberos in detail.
5. Explain digital signature algorithm in detail
6. What is dual signature and explain construction of dual signature
7. List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.
8. What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos.
9. Explain Kerberos Authentication System
10. Explain Public Key Infrastructure (PKIX) Architecture Model in detail.
11. Explain the key distribution scenario and write how does decentralized key control work?
12. Discus the ways in which public keys can be distributed to two communication parties.
13. Explain Key Distribution methods.
14. List and explain four general categories of schemes for the distribution of public keys.
15. What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center.

Unit - 10

1. What is a dual signature in reference to secure electronic transaction?
2. Write the key features of secure electronic transaction.
3. What is the difference between transport mode and tunnel mode?
4. Which parameters define session state and which parameters define connection state in SSL(secure socket Layer)?
5. Explain Secure electronic transaction protocol.
6. Explain Secure Socket Layer Protocol.