**QUESTION BANK**

1. Explain data confidentiality, data authentication and data integrity.
2. Explain generation of encryption matrix in play fair cipher.
3. Explain Caesar cipher.
4. Apply brute force on Caesar cipher “PHHWPHDIWHUWKHWRJDSDUWB.
5. Explain one time pad cipher with an example.
6. Explain rail fence Cipher technique
7. Explain transposition technique with multiple round
8. Apply brute force on Caesar cipher “FOBIQYYN”
9. Define the term – confusion, diffusion
10. Use Hill cipher to encrypt the text DEF. The key to be used is

2 4 5

9 2 1

3 8 7

1. Using playfair cipher encrypt the plaintext “Why, don’t you?”. Use the key “keyword”.
2. Use hill cipher to encrypt text pay. The key to be used is

17  17  5

21  18  21

2    2   19

1. Using playfair cipher encrypt the plaintext “balloon” use the key “Monarchy”.
2. Using playfair cipher encrypt the plaintext “mynameisatul” use the key “playfair example”
3. Use hill cipher to encrypt the text cat. The key to be used is

6     29     1

13   16    10

20   17    15

1. Using playfair cipher encrypt the plaintext “mynameisatul” use the key “harsh”.
2. What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.
3. Define the term cryptanalysis. Explain various types of cryptanalytic attacks.
4. Give examples of replay attacks. List three general approaches for dealing with replay attacks.

1. Encrypt the message “Exam” using the Hill cipher with the key

2 4 5

9 2 1

3 8 7

1. When an encryption scheme is said to be unconditionally secure and  computationally secure?
2. Which type of substitution is called monoalphabetic substitution cipher?
3. Which two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext?
4. Use playfair algorithm with key “monarchy” and encrypt the text “jazz”.
5. What is security Services? Explain any three types of security services
6. Explain Vegenere Cipher.
7. What is security mechanism? List and explain various security mechanism.
8. Explain the conventional security model used for information security.
9. Explain cryptanalysis. Discuss any one technique for it
10. What attacks can be done on encrypted text? Explain them.
11. Explain play fair cipher with suitable example.
12. Define the terms threat and attack. List and briefly define categories of security attacks.
13. List and briefly define the security services.
14. Construct a playfair matrix with the key “occurrence”. Generate the cipher text for the plaintext “Tall trees”
15. Define the terms diffusion and confusion. What is the purpose of S-box in DES?
16. Explain the avalanche effect in DES.
17. Explain monoalphabetic cipher and polyalphabetic cipher by giving an example.
18. What  is  cryptography?
19. With example explain function of s-box in DES.
20. Explain various steps of AES in short.
21. Explain AES in detail
22. Explain key generation in AES.
23. Explain S-box generation in AES.
24. Explain single round of DES algorithm.
25. Explain the steps involved in International data encryption standard algorithm
26. Explain scheme for DES encryption.
27. Define Block Cipher. Explain Design Principles of block cipher.
28. Explain DES algorithm with Figure.
29. Explain Sub key generation Process in Simplified DES algorithm with Example.
30. Explain limitation of DES in detail.
31. Explain linear and differentical cryptanalysis?
32. What is SAC and BIC?
33. Explain double DES.
34. Explain triple DES with two and three keys.
35. What is meet in the middle attack?
36. Explain cipher feedback mode of operation
37. Explain Modes of Operations.
38. Why mode of operation is defined? Explain the block cipher modes of operation?
39. Explain Diffie - Hellman key exchange algorithm with example.
40. What is man in the middle attack explain with example.
41. Explain RSA algorithm with example.
42. 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.
43. Perform encryption using the RSA algorithm.

p=3,q=11(two random numbers).

e(encryption key)=7

M(plaintext message)=5

1. What  is  primitive  root? Explain Diffi-Hellmen key exchange  algorithm with proper example.
2. Elaborate various kinds of attacks on RSA algorithm.
3. Explain computational aspects of RSA.
4. Compare public key and private key cryptography. Also list various algorithms for each
5. Briefly explain  the  model  of  Asymmetric Cryptosystem.
6. Explain RSA algorithm and list the possible approaches to attacking it.
7. Perform  encryption  and  decryption  using  the  RSA  algorithm  for p=3,q=11, e=7, M=5.
8. Compare conventional encryption with public key encryption.
9. What  is  a trap-door  one-way function? What  is  its importance in public key cryptography?
10. Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.
11. What   is   the   difference   between   weak   and   strong   collision resistance?
12. What characteristics are needed in a secure hash function?
13. Write the properties of hash functions.
14. Explain hash function requirement and security.
15. What characteristics are needed in a secure hash function?
16. What is MAC? Explain HMAC.
17. How  following  can  be  achieved  with  message  authentication: Message authentication, Message authentication and confidentiality
18. How message authentication code can be used to achieve message authentication and confidentiality
19. Explain MAC based on Block cipher.
20. What are the advantages of HMAC.
21. Explain MAC function requirement and security.
22. Explain authentication mechanism of Kerberos.
23. What four requirements were defined for Kerberos?
24. Explain Kerberos Authentication System
25. What problem was Kerberos designed to address?
26. Briefly explain how session key is distributed in Kerberos.
27. Which techniques are used for the distribution of public keys?
28. Explain Key Distribution methods.
29. List and Explain various key management techniques.
30. Discus  the  ways  in  which  public  keys  can  be  distributed  to  two communication parties.
31. What is digital signature? Explain its use with the help of example.
32. List  the  security  services  provided  by  digital  signature.  Write  and explain the Digital Signature Algorithm.