Subject - Cryptography and Network Security
Question Bank
Semester-IV CE
UNIT -1 TO 4

1. Differentiate passive attack from active attack with example.
2. Discuss CIA model in cryptography.
3. Define Security attacks.
4. What are the 3 aspects of security?
5. Explain security mechanisms.
6. Explain Security service.
7. Define Steganography
8. Define:
    - Cryptography
    - Cryptology
    - Cryptanalysis
9. What are the two basic functions used in encryption algorithms/techniques?
10. Differentiate between threat, vulnerability and attack with example
11. What are the two approaches to attacking a cipher?
12. Define Brute-force attack
13. Explain about OSI Security architecture model with neat diagram.
14. What is Modification of messages
15. Define Denial of service with real case study of it
16. Classical cryptosystems and its types.
17. List out components of Encryption algorithms
18. Compare Substitution and Transposition techniques.
19. Specify the four categories of security threads?
20. Define integrity.

21. Define Non repudiation.
22. Differentiate symmetric and asymmetric encryption?
23. Compare stream cipher with block cipher with example.
24. Convert the Given Text “CRYPTOGRAPHY AND NETWORK SECURITY” into cipher text with DEPTH=3 using Rail fence Technique.
25. Encrypt the following using play fair cipher using the keyword MONARCHY .PT= CYBER SECURITY.
26. Write down the purpose of S-Boxes in DES? Explain each step in detail with one particular example of it for a particular s-box.
27. What is the difference between diffusion and confusion?(
28. What is an avalanche effect?
29. What are the operations used in AES?
30. What is a Substitute byte transformation in AES?
31. How can we achieve confusion and diffusion in DES, explain its steps in detail?
32. How can we achieve confusion and diffusion in AES, explain its steps in detail?
33. Discuss in detail a single round of DES.
34. Discuss in detail a single round of AES.
35. What is a Shift row in detail?
36. Write down the purpose of S-Box in AES? Explain each step in detail with one particular example of it for a s-box.
37. How the key is expanded in AES; explain it with a diagram.
38. Summarize OSI security architecture model with neat diagram.
39. Examples of all ciphers for encryption/decryption:
    a. Caesar
    b. Mono alphabetic
    c. Affine cipher
    d. Play fair cipher

e. Hill cipher
f. Vigenere cipher
g. Vernam Cipher
h. Auto key cipher
i. Rail Fence
j. Row transposition

40. Compare DES and AES.
41. List the parameters (block size, key size and no. of rounds) for the three AES versions.
42. Describe AES algorithm with a neat diagram and all its round functions in detail.
43. Describe DES algorithm with a neat diagram and explain the steps.
44. Explain the DES and General structure of DES with diagrams.
45. For each of the following elements of DES, indicate the comparable element in AES if available.
    i)XOR of sub key material with the input to the function
    ii) f function
    iii) Permutation p
    iv) Swapping of halves of the block.
46. What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in the AES encryption process with example.
47. Explain the working mechanism of a one-time pad.