R19IT303 - CRYPTOGRAPHY AND CYBER SECURITY

QUESTION BANK

UNIT – I

PART-A

1. Specify the four categories of security threats.
2. Explain active and passive attack with example.
3. Define integrity and non-repudiation.
4. Differentiate symmetric and asymmetric encryption?
5. Define cryptanalysis.
6. Define security mechanism.
7. Define steganography.
8. Why does a network need security?
9. Define confidentiality and authentication.
10. Define cryptography.
11. Compare Substitution and Transposition techniques.
12. Define Diffusion & Confusion.
13. Define Multiple Encryption.
14. Specify the design criteria of a block cipher.
15. Define Reversible mapping.
16. Specify the basic task for defining a security service.
17. Define network security.
18. Define computer security.
19. What are Hill cipher merits and demerits?

PART-B

1. Explain the following: (a) Playfair cipher. (8) (b) Vernam cipher in detail. (8)
2. Explain simplified DES with example. (16)
3. Write short notes on: (i) Steganography (16)
4. Explain classical encryption techniques in detail. (16)
5. Write short notes on: (a) Security services (8) (b) Feistel cipher structure (8)
6. Explain the OSI security architecture. (16)
7. (a) Explain various transposition ciphers in detail. (8) (b) Explain the basic principle of rotor machine. (8)
8. Explain in detail about Feistel cipher with diagram. (16)
9. (a) Explain classical encryption techniques with symmetric cipher model. (12) (b) Explain steganography in detail. (4)
10. Convert “MEET ME” using Hill cipher with the key matrix. Convert the cipher text back to plaintext.
11. Write short notes on block cipher modes of operation.
12. (i) Discuss any four substitution techniques and list their merits and demerits. (16)
13. Explain in detail about various types of attacks.
14. Explain in detail about various services provided by X.800.
15. Explain in detail about various mechanisms provided by X.800.
16. Briefly explain the design principles of block cipher. (8)
17. Write short notes on: (i) Fermat and Euler’s theorem (8) (ii) Chinese Remainder theorem (8)
18. Discuss with neat sketch a network security model. (8)