CRYPTOGRAPHY AND NETWORK SECURITY

QUESTION BANK

UNIT 1

1. Discuss the taxonomy of attacks with related to security goals.
2. Explain the five common Security services
3. Explain security mechanism recommended by ITU-T (X.500).
4. Write the relationship between security services and security mechanism.
5. Write three properties used in binary operations for Z or Z_n.
6. Calculate using Euclidean Algorithm.

   GCD(831,366)

   GCD(1760, 2740)

   GCD(270, 192).
7. Write the Extended Euclidean algorithm to find the multiplicative inverse of a number and compute the multiplicative inverse of

   23 in Z_{100} gcd (100, 23)

   7 in Z_{180}

   11 in Z_{26}
8. Distinguish between the following with an example:

   i) Passive and Active attacks

   ii) Cryptography and Steganography

   iii) Repudiation and Replaying.

UNIT 2

1. Define Cryptanalyst. List the types of Common Attacks and explain them in brief.
2. What are the types of Polyalphabetic Ciphers and Explain in detail with an example.
3. Explain the Monoalphabetic Ciphers.
4. Use the additive cipher with key=15 to encrypt the message "HELLO" and decrypt the message "WTAAD".
5. Use the Multiplicative cipher with key=7 to encrypt the message "HELLO"
6. Using Affine cipher calculate the cipher text when the keys are given as K1 -21 K2- 7 and the plain text is "CSEMSRIT". Identify affine cipher is vulnerable for which attack.
7. Use an Affine Cipher to encrypt the message "MSRIT" with the key pairs (7,2)
8. Using play fair cipher find the cipher for the plain text "RIT CSE DEPRT " using the key word "Playfair "
9. Using playfair cipher encrypt message "MSRIT BANGALORE" using secret key "GUIDANCE".
10. Encrypt the message "Let us make it happen" using Vigenere cipher with the key "WORLD".
11. Use Hill cipher to encrypt the message "CRYPTOGRAPHY" and decrypt the cipher text to get the original plaintext.

    $$\text{Key} = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

12. Using Hill cipher encrypts the message "LIVE" and decrypts the cipher text to get the original plaintext.

    $$\text{key} = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

13. Solve the given problem using Hill Cipher with m=3 (block size =3) with key K shown below

    $$\begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$$

    i. What is the Cipher text corresponding to the plaintext = (V O W)?
    ii. What is the plaintext corresponding to the ciphertext = (T Q X)?

14. Explain the Tranposition Ciphers and its types with example.
15. Distinguish between the following with an example:
    i) Substitution and Transposition Cipher
    ii) Monoalphabetic and Polyalphabetic Cipher
    iii) Stream and Block Cipher.
16. Write and explain general structure of DES.
17. Explain with a neat diagram the process of Key generation in DES.
18. Explain the desired properties and weakness of DES.
19. Describe various possible attacks on DES in brief.
20. With an example explain key expansion in AES-128.
21. Identify four types of transformations used by AES.