UNIT -1

SUBSTITUTION CIPHER

1. Apply Product cipher to encrypt the phrase 'ENGINEERING GRADUATE' through the application of the Caesar cipher. Alice and Bob have established the key as the fifth character of the plaintext, adhering to the agreed-upon mapping where A=0 to Z=25. What is the resulting ciphertext?

2. Encrypt the message "this is an exercise" using additive cipher with key = 20. ignore the space between words. Decrypt the message to get the original plaintext.

3. Plaintext Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ

  Key   : QWERTYUIOPASDFGHJKLZXCVBNM

Plaintext: "cryptography and network security" ,Find cipher text?

4. Encrypt the message 'WE WILL SCORE GOOD' with key 'HARDWORKING' using play fair cipher technique.

5. Encrypt the message 'MY BALLOON' with key 'MONACHRY' using play fair cipher technique.

6. Given the Playfair key square:

$$
\begin{array}{ccccc}
P & L & A & Y & F \\
I & R & E & B & C \\
D & G & H & K & M \\
N & O & Q & S & T \\
U & V & W & X & Z
\end{array}
$$

      Encrypt the message "HELLO". Use the rule that if two identical letters appear together, insert an "X" between them (e.g., "LL" becomes "LX").

7. Let message = "graduate", Key = "word", find ciphertext using playfair cipher

8. Demonstrate encryption and decryption process in hill cipher. Consider m = "sh" and key = hill

9. Perform encryption using hill cipher for the following message "PEN" key "ACTIVATED"

10.Calculate the result of (869 mod 26).

11. Compute the multiplicative inverse of 21

12. Calculate the K^{-1} using the key K = VIEW through the application of the Hill cipher.

13. Encrypt the message "HELLO TO EVERYONE" using the keyword "KEY" with the Vigenère Cipher.

14. Encrypt the message "DATA" using the Vernam Cipher with the key "KEY". Explain the encryption process

15. Encrypt the message "SECURITY IS KEY" using the Rail Fence Cipher with 3 rails.

16. encrypt the plaintext **"MEET ME AFTER THE TOGA PARTY"** using the **Rail Fence Cipher** with a depth of **2**.

16. Encrypt the message **"CRYPTOGRAPHY IS FUN"** using the **Columnar Transposition Cipher** with the key **"SECRET"**

17. To encrypt the plaintext **"ATTACK P O S T P O N E D U N T I L T W O A M"** using the **two Columnar Transposition Cipher** with the key **4312567**