PRE LAB:-

1. What is the Caesar cipher, and how does it work?

A substitution cipher that shifts each letter in the plaintext by a fixed number of positions in the alphabet. Encryption involves shifting letters forward, while decryption involves shifting them backward by the same number.

2. Explain the process of encrypting and decrypting using the Caesar cipher.

Encryption: Shift each letter in the plaintext by a fixed number of positions in the alphabet to obtain the ciphertext.

Decryption: Shift each letter in the ciphertext backward by the same number of positions to retrieve the original plaintext.

3. What is the significance of the "shift" value in the Caesar cipher?

The shift value determines the number of positions each letter is moved, defining the encryption and decryption transformations.

4. How does the Caesar cipher handle spaces and punctuation in the plaintext?

The Caesar cipher typically ignores spaces and punctuation, only applying shifts to alphabetic characters.

5. Discuss the security implications of using the Caesar cipher for encryption?

The Caesar cipher is very insecure due to its simplicity; it can be easily broken with brute-force attacks, as there are only 25 possible shifts.

VIVA :-

1. **What is the key space of the Caesar cipher, and why is it important?**

The key space of the Caesar cipher is 25 possible shifts (1 through 25), as a shift of 0 or 26 would leave the plaintext unchanged, making it small and vulnerable to brute-force attacks.

2. **Describe the process of breaking the Caesar cipher using brute-force attacks.**

Try all 25 possible shifts to decrypt the ciphertext and check which one yields readable plaintext.

3. **How can frequency analysis be used to attack the Caesar cipher?**

Analyze the frequency of letters in the ciphertext and compare them to the typical frequency distribution of letters in the language to deduce the shift value .

4. **Explain the relationship between the Caesar cipher and modular arithmetic.**

The Caesar cipher uses modular arithmetic to wrap around the end of the alphabet when shifting letters, effectively using modulo 26 operations.

5. **What are some practical applications of the Caesar cipher in today's world, if any?**

The Caesar cipher is primarily of historical interest and used in educational contexts; it is not secure for modern applications but can be seen in simple puzzles and games.