Subject: Security Lab-Assignment 2

Aim: **Shift cipher and mono alphabet substitution cipher**

Theory:

Shift Cipher (Caesar Cipher)

Theory:

1. **Definition**: The shift cipher, also known as the Caesar cipher, is a type of substitution cipher where each letter in the plaintext is 'shifted' a certain number of places down or up the alphabet.
2. **Encryption**:
    - **Key**: The key in a shift cipher is a number that represents the number of positions each letter in the plaintext is shifted.
    - **Formula**: If the key is kkk, then the encryption of a letter xxx is given by E(x)=(x+k)mod 26E(x) = (x + k) \mod 26E(x)=(x+k)mod26, where xxx is the position of the letter in the alphabet (0 for 'A', 1 for 'B', ..., 25 for 'Z').
    - **Example**: With a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.
3. **Decryption**:
    - **Formula**: To decrypt, you shift in the opposite direction: D(x)=(x−k)mod 26D(x) = (x - k) \mod 26D(x)=(x−k)mod26.
    - **Example**: If the encrypted letter is 'D' and the shift is 3, then 'D' is decrypted back to 'A'.
4. **Usage**: This cipher is simple and historically significant but provides minimal security due to its predictability. With only 25 possible shifts (excluding the trivial shift of 0), it is vulnerable to brute-force attacks.

Monoalphabetic Substitution Cipher

Theory:

1. **Definition**: In a monoalphabetic substitution cipher, each letter in the plaintext is replaced with a fixed letter in the ciphertext. This replacement is consistent throughout the message.
2. **Encryption**:
    - **Key**: The key is a permutation of the alphabet. Each letter in the plaintext is substituted by a corresponding letter from the key.
    - **Example**: If the key is a permutation of the alphabet, say ZEBRASCDFGHIJKLMNOPQTUVWXYA, then 'A' might be replaced by 'Z', 'B' by 'E', etc. The mapping is fixed for the entire message.
3. **Decryption**:
    - **Formula**: To decrypt, you reverse the substitution using the inverse of the key. If 'Z' was mapped to 'A', then 'A' maps back to 'Z'.

- **Example**: Using the above key, if the encrypted letter is 'Z', you would look up the key to find that it maps to 'A'.

4. **Usage**: While monoalphabetic substitution ciphers are more complex than shift ciphers, they are still vulnerable to frequency analysis. Each letter in the ciphertext is consistently replaced, making it possible for an attacker to analyze the frequency of letters and guess the substitutions.

Implementation: