**Task 1**

***Implement Caesar Cipher***

**Report**

***STEP 1: understand and learn about Caesar Cipher***

***Caesar Cipher***

The **Caesar Cipher** is one of the earliest and simplest encryption techniques in history. Named after **Julius Caesar**, who reportedly used it to protect military messages, this cipher works by replacing each letter in the original message (called the **plaintext**) with another letter a fixed number of positions forward in the alphabet. The number of positions used for the shift is known as the **key**.

For example, if we use a key of 3, the letter A becomes D, B becomes E, C becomes F, and so on. After Z, the shift wraps around to the beginning of the alphabet. This means X becomes A, Y becomes B, and Z becomes C. So, the word **HELLO** becomes **KHOOR** using a Caesar Cipher with a key of 3.

To **decrypt** a Caesar Cipher message, the process is reversed. Each letter in the ciphertext is shifted **backward** by the same number of positions. Using the same example, if we receive the message KHOOR, we shift each letter back by 3 to get the original message HELLO.

The Caesar Cipher belongs to a group of techniques known as **substitution ciphers**, where letters are substituted with others according to a fixed system. It is one of the simplest ways to conceal information, which is why it is often used as a first step in learning about encryption in cybersecurity.

Despite its simplicity, the Caesar Cipher is important for **teaching basic encryption principles**. It introduces key concepts such as the use of an **encryption key**, the idea of **plaintext vs. ciphertext**, and how information can be **encoded and decoded**. It also highlights a critical concept in cybersecurity: **the strength of an encryption method** is often based on how difficult it is to reverse the process without knowing the key.

However, the Caesar Cipher is **not secure by modern standards**. It can be easily broken using a brute-force attack because there are only **25 possible keys** (since a shift of 0 means no encryption). An attacker could try all possible shifts and see which one results in readable text. Furthermore, the Caesar Cipher does not disguise the frequency of letters, which means someone could use **frequency analysis** (e.g., recognizing that 'E' is the most common letter in English) to break the code even faster.

In today's world of cybersecurity, the Caesar Cipher has no real application for **protecting sensitive data**, but its educational value remains significant. It is an excellent starting point for those new to the field, providing insight into how encryption has evolved from simple manual methods to complex algorithms like **AES** (Advanced Encryption Standard) and **RSA** (a public key cryptosystem used for secure data transmission).

**Conclusion**

The Caesar Cipher is a historically important encryption method that illustrates how letters can be shifted to create secret messages. While it offers no real security today, it plays a key role in helping cybersecurity students understand basic encryption concepts and paves the way for learning more advanced cryptographic systems.

**Summary of Steps**

1. Write down your message (plaintext).
2. Choose a key (number of positions to shift).
3. Shift each letter forward in the alphabet by the key.
4. Wrap around the alphabet if needed (Z → A).
5. Write down the new letters as the ciphertext.
6. To decrypt, shift letters backward using the same key.

***STEP 2: Programming a creaser cypher***

*Algorithm*

**EncryptedChar = (OriginalChar + Key) % 26**

*Program*

def caesar\_cipher(text, key, mode):

    result = ""

    for char in text:

        if char.isalpha():

            base = ord('A') if char.isupper() else ord('a')

            if mode == "encrypt":

                shifted = chr((ord(char) - base + key) % 26 + base)

            elif mode == "decrypt":

                shifted = chr((ord(char) - base - key) % 26 + base)

            result += shifted

        else:

            result += char

    return result

print("Caesar Cipher")

print("Choose an option:")

print("A Encrypt a message")

print("B Decrypt a message")

choice = input("Enter A or B: ")

if choice == "A":

    message = input("Enter the message to encrypt: ")

    key = int(input("Enter the key (number to shift): "))

    encrypted = caesar\_cipher(message, key, "encrypt")

    print("Encrypted message:", encrypted)

elif choice == "B":

    message = input("Enter the message to decrypt: ")

    key = int(input("Enter the key (number used during encryption): "))

    decrypted = caesar\_cipher(message, key, "decrypt")

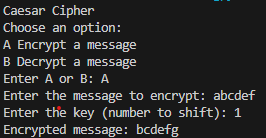
    print("Decrypted message:", decrypted)

else:

    print("Invalid choice.")

*OUTPUT*

1. *Encryption*

**

1. *Decryption*

