Task one

Implement Caesar Cipher

Report

Introduction

The Caesar Cipher is one of the earliest and simplest forms of encryption, attributed to Julius Caesar who used it to secure military communications. This method involves shifting the letters of the plaintext by a fixed number (called the "key") to produce the ciphertext. It provides a foundational understanding of substitution ciphers in the field of cryptography.

Understanding the Caesar Cipher

The Caesar Cipher is one of the oldest and simplest encryption methods, named after Julius Caesar who used it to encode military messages. It works by shifting each letter in the plaintext a fixed number of positions forward in the alphabet, defined by a key. For example, with a key of 3, "HELLO" becomes "KHOOR".

Decryption involves shifting the letters backward by the same key. This cipher is a basic form of substitution encryption and introduces key concepts like plaintext, ciphertext, and the use of encryption keys.

Although easy to understand, the Caesar Cipher is not secure by modern standards. It can be broken quickly using brute-force attacks or frequency analysis due to its limited key space (25 options).

Despite its weaknesses, the Caesar Cipher remains valuable in education as a foundation for learning more advanced cryptographic methods such as AES and RSA.

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.

Programming a creaser cypher

Algorithm

EncryptedChar = (OriginalChar + Key) % 26

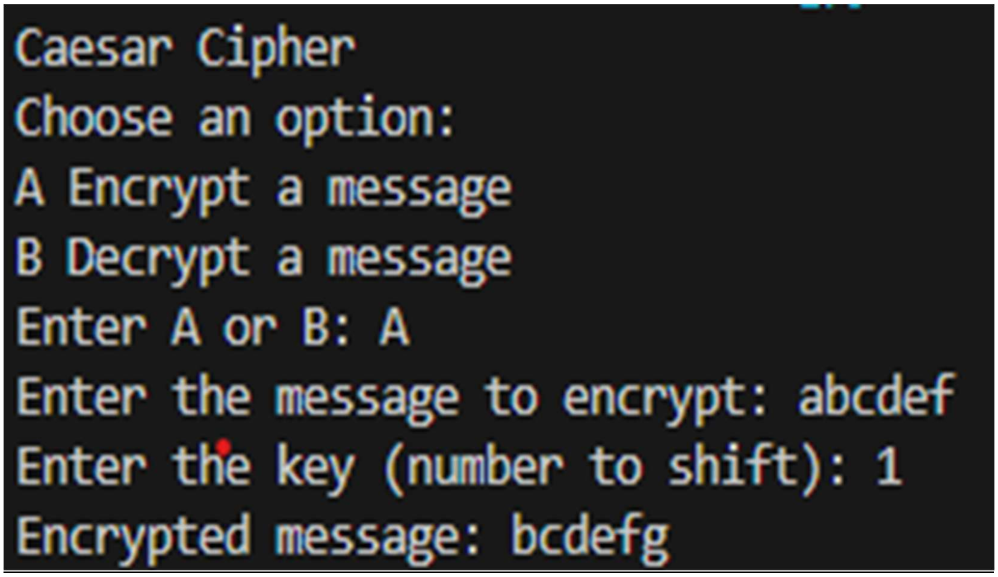
Program

```
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.")
```

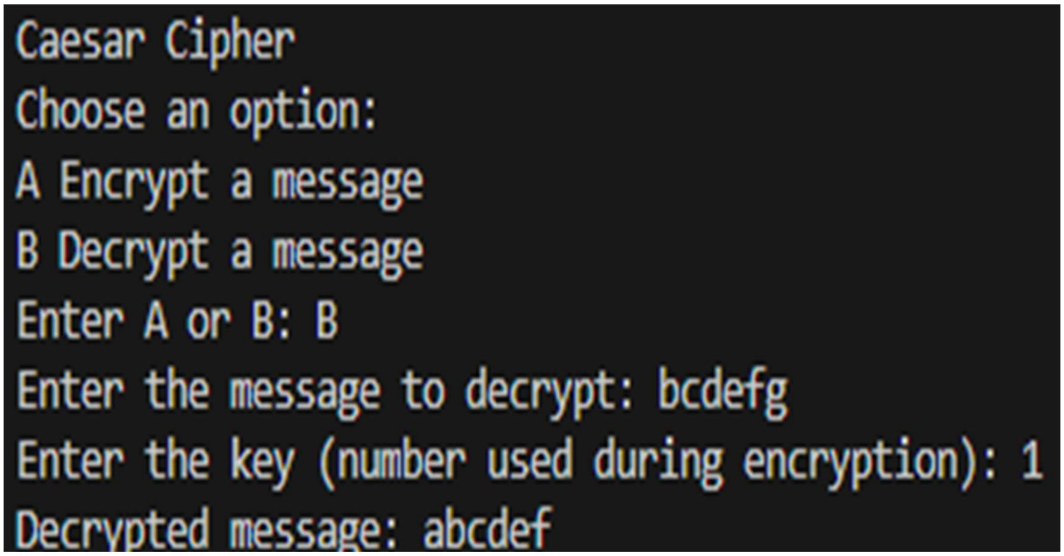
OUTPUT

1) *Encryption*



```
Caesar Cipher
Choose an option:
A Encrypt a message
B Decrypt a message
Enter A or B: A
Enter the message to encrypt: abcdef
Enter the key (number to shift): 1
Encrypted message: bcdefg
```

2) *Decryption*



```
Caesar Cipher
Choose an option:
A Encrypt a message
B Decrypt a message
Enter A or B: B
Enter the message to decrypt: bcdefg
Enter the key (number used during encryption): 1
Decrypted message: abcdef
```

Conclusion

The Caesar Cipher, while no longer suitable for modern data protection, remains a vital teaching tool in cybersecurity education. It introduces essential encryption principles and forms a gateway to more complex systems. Understanding its strengths and limitations provides insight into the development of modern cryptographic techniques.