Caesar Cipher Encryption Tool

A Mini Project In 'C' Programming Language

By: Minahil CT-66, Areeba CT-70, Laiba CT-60

Caesar Cipher

Classic Message Encryption

Introduction

The *Caesar Cipher* is a foundational encryption technique attributed to Julius Caesar. It shifts each letter in the plaintext by a fixed number, known as the key, creating coded messages. This method exemplifies early cryptographic principles and is widely used for educational purposes in understanding encryption basics and cipher mechanics.

❖ Introduction to Caesar Cipher

Historical Background

The Caesar Cipher was used by Julius Caesar to protect military communications. It is one of the earliest and simplest forms of substitution cipher, shifting letters within the alphabet. Despite its simplicity, it laid the groundwork for modern cryptography by introducing the concept of key-based message transformation.

Basic Concept Of Caesar Cipher

The cipher works by shifting every letter in the plaintext by a predetermined number of positions in the alphabet. This fixed *key* determines the encryption and decryption process. Only letters are shifted, while other characters remain unchanged. Its straightforward mechanism makes it easy to implement and understand.

Importance in cryptography

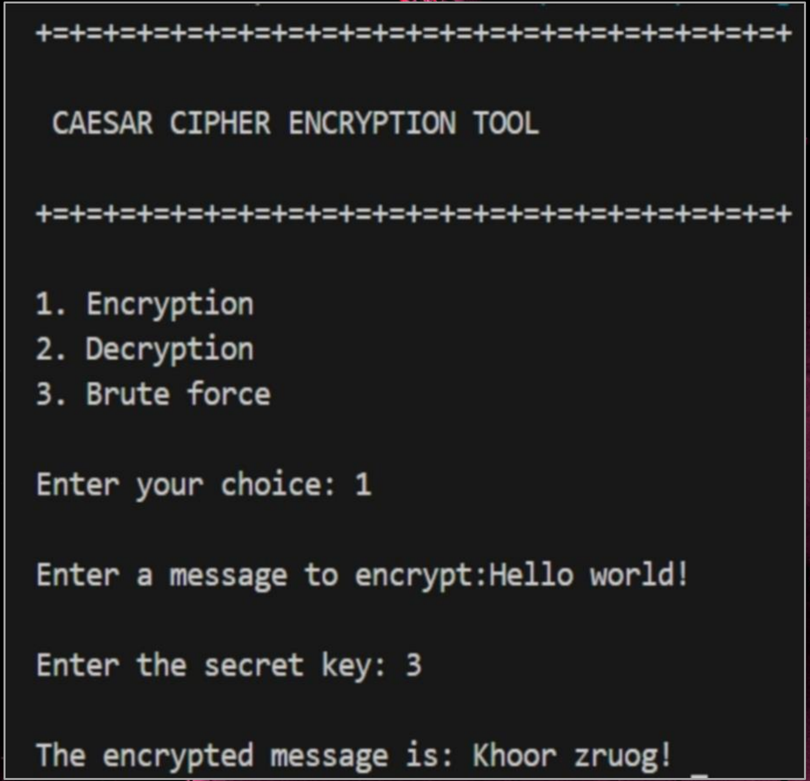
The Caesar Cipher serves as a fundamental example in the field of cryptography, illustrating basic encryption concepts. It highlights the significance of the *encryption key* in securing messages and introduces the idea of substitution ciphers. While simple, it forms the basis for understanding more complex cryptographic systems and the necessity of robust encryption in data protection.

❖ Implementation of Caesar Cipher in C

Encryption function logic

The encryption function shifts each letter in the message by a fixed *key* number. It processes uppercase and lowercase letters separately to maintain case sensitivity. The shift uses modular arithmetic to wrap around the alphabet, ensuring characters remain valid letters. Non-alphabet characters remain unchanged, preserving message structure during encryption.

Encryption Demo



```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

 CAESAR CIPHER ENCRYPTION TOOL

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

1. Encryption
2. Decryption
3. Brute force

Enter your choice: 1

Enter a message to encrypt:Hello world!

Enter the secret key: 3

The encrypted message is: Khoor zruog! _
```

This demonstrate the Caesar cipher, basic substitution encryption.

GOAL: To ecrypt a message.

METHOD CHOSEN: Encryption (choice 1).

PLAINTEXT MESSAGE: Hello world!

SECRET KEY(shift): 3

- **This means every letter is shifted 3 positions forward in alphabet.**

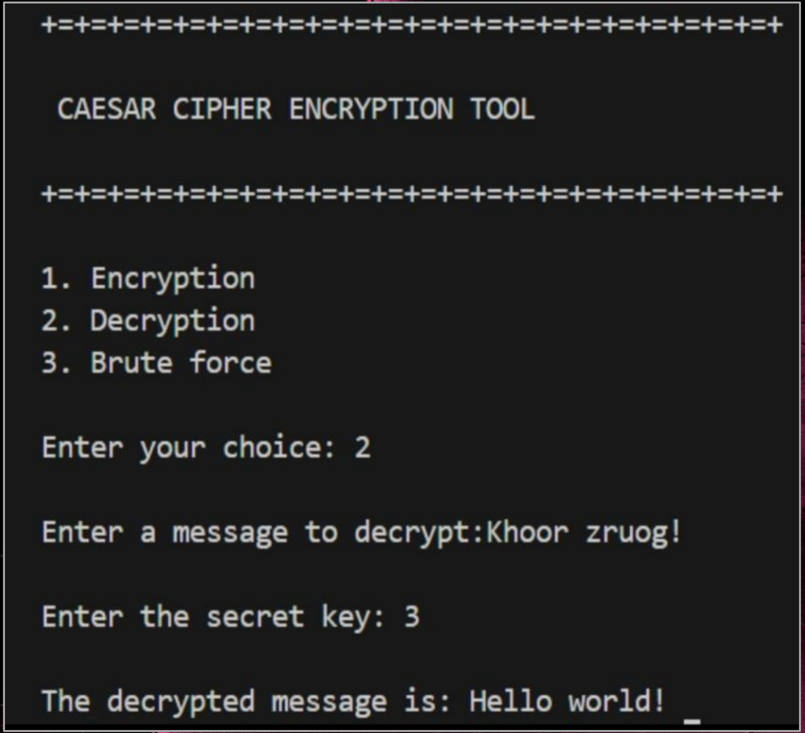
OUTPUT: Khoor zruog!

TAKEAWAY: This message is secured and unreadable without knowing the secret key (3).

Decryption function logic

The decryption function reverses the encryption process by shifting letters backward using the same key. It handles uppercase and lowercase letters distinctly, using modular arithmetic to correctly reposition characters in the alphabet. This function restores the original message from the encrypted text, ensuring accurate retrieval of the plaintext.

Decryption Demo



```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

 CAESAR CIPHER ENCRYPTION TOOL

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

1. Encryption
2. Decryption
3. Brute force

Enter your choice: 2

Enter a message to decrypt:Khoor zruog!

Enter the secret key: 3

The decrypted message is: Hello world! _
```

This demonstrate the Caesar cipher, basic substitution decryption.

GOAL: To convert an decrypted message back to its original form.

METHOD CHOSEN: Decryption (choice 2).

CIPHERTEXT MESSAGE(encrypted): Khoor zruog!

SECRET KEY(shift): 3
To decrypt, the key 3 is used to shift the letters 3 positions backword in the alpjhabet.

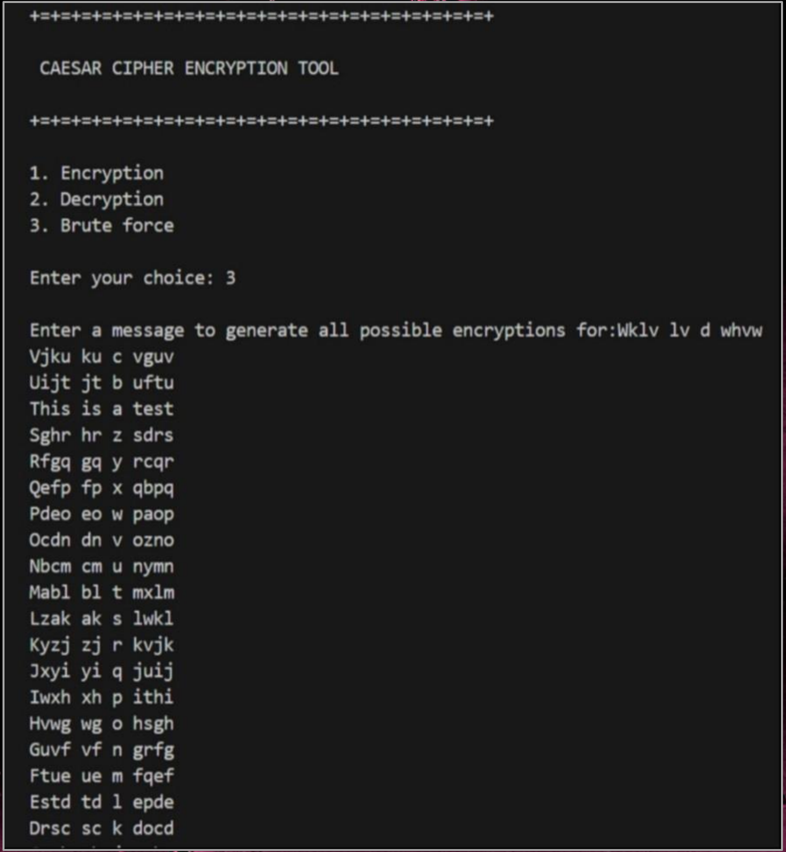
PLAINTEXT OUTPUT(decrypted): Hello world!

TAKEAWAY:Decryption successfully restores the original message only when the correct Secret key is provided.

Brute force approach for cryptanalysis

Brute force attempts all possible key shifts (1 to 25) to decode the message, generating every potential plaintext. This method works because the Caesar Cipher has a limited key space. It demonstrates how simple ciphers can be vulnerable without additional complexity, emphasizing the importance of more secure encryption techniques.

Brute Force Demo



```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

 CAESAR CIPHER ENCRYPTION TOOL

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

1. Encryption
2. Decryption
3. Brute force

Enter your choice: 3

Enter a message to generate all possible encryptions for:Wklv lv d whvw
Vjku ku c vguv
Uijt jt b uftu
This is a test
Sghr hr z sdrs
Rfgq gq y rcqr
Qefp fp x qbpq
Pdeo eo w paop
Ocdn dn v ozno
Nbcm cm u nymn
Mabl bl t mxlm
Lzak ak s lwkl
Kyzj zj r kvjk
Jxyi yi q juij
Iwxh xh p ithi
Hvwg wg o hsgh
Guvf vf n grfg
Ftue ue m fqef
Estd td l epde
Drsc sc k docd
```

This output demonstrates the Brute force attack method on a Caesar Cipher.

GOAL: To decrypt a message when the Secret Key is unknown.

METHOD CHOSEN: Brute force (Choice 3)

INPUT MESSAGE(cipher text): Wklv lv d whvw

PROCESS: The tool automatically generates all 25 possible shifts (Keys 1 through 25) for the English alphabet.

OUTPUT: A list of every possible plaintext message.

TAKEAWAY: The user must manually scan the output list to find the line that forms a readable, coherent message. In this list, the readable line is This is a test (which corresponds to a shift/key of 3).

INSIGHT

Working on this project gave us practical understanding of both the fundamental and the limitations of cryptographic systems. While implementing the Caesar cipher, it became clear why it's now considered a teaching tool rather than a secure method. The most glaring weakness is its extremely limited key space, with only 25 possible keys. A brute-force attack can break the cipher in seconds, as our own program demonstrates.

The experience highlighted a critical lesson in cybersecurity: Complexity does not equal security. A system can be logically sound, (and the Caesar cipher,s algorithm is) yet still be completely insecure due to a simple lack of possible combinations. It made an appreciate the immense importance of the large key space in method encryption, like that used in AES, where the number of possible keys is astronomically large.

Conclusion

The Caesar Cipher is an essential educational tool that demonstrates core principles of encryption and decryption. Its implementation in C showcases practical programming applications of cryptography. However, its simplicity also reveals vulnerabilities, underscoring the vital need for advanced security measures in modern communication systems.

Thank You!