Caesar Cipher Program

Project - Report

Team members:

Areeba (CT-070)

Laiba Akram (CT-060)

Minahil Khan (CT-066)

WHAT WE BUILT:

We created a Caesar Cipher - a cyptogrphy tool in C language that can:

- Encrypt plain text into secret messages using a shift key
- Decrypt coded messages back to readable text using the correct key
- Brute Force attack to crack encrypted messages

What is Caesar Cipher?

It's one of the oldest encryption techniques where each letter in the message is shifted by a fixed number, i.e a secret key, of positions in the alphabet. Julius Caesar used it to protect his military messages. It is a crytography classic.

HOW IT WORKS:

The core formulas:

ENCRYPTION: (original message+key)%26

DECRYPTION: (encrypted message - key + 26) % 26

Program Handles:

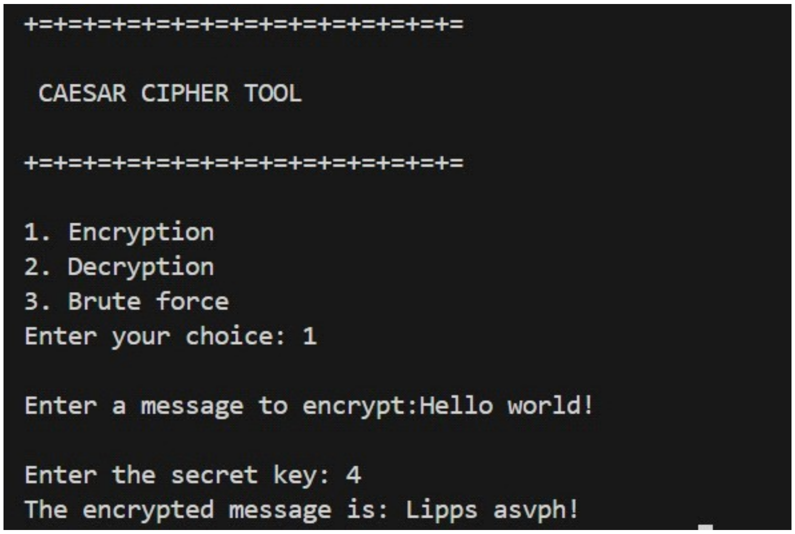
- Both uppercase (A-Z) and lowercase (a-z) letters
- Keeps spaces and symbols unchanged
- Works with any shift key from 1-25

CODE STRUCTURE:

```
switch(part) {
  case (1): encrypt(text, key); break;
  case (2): decrypt(text, key); break;
  case (3): bruteforce(text); break;
}
```

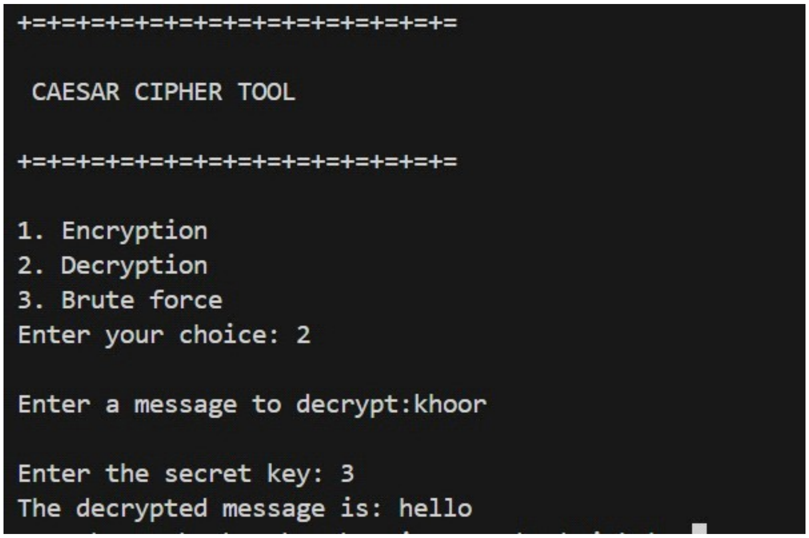
WORKING PROGRAM SCREENSHOTS:

Encryption:



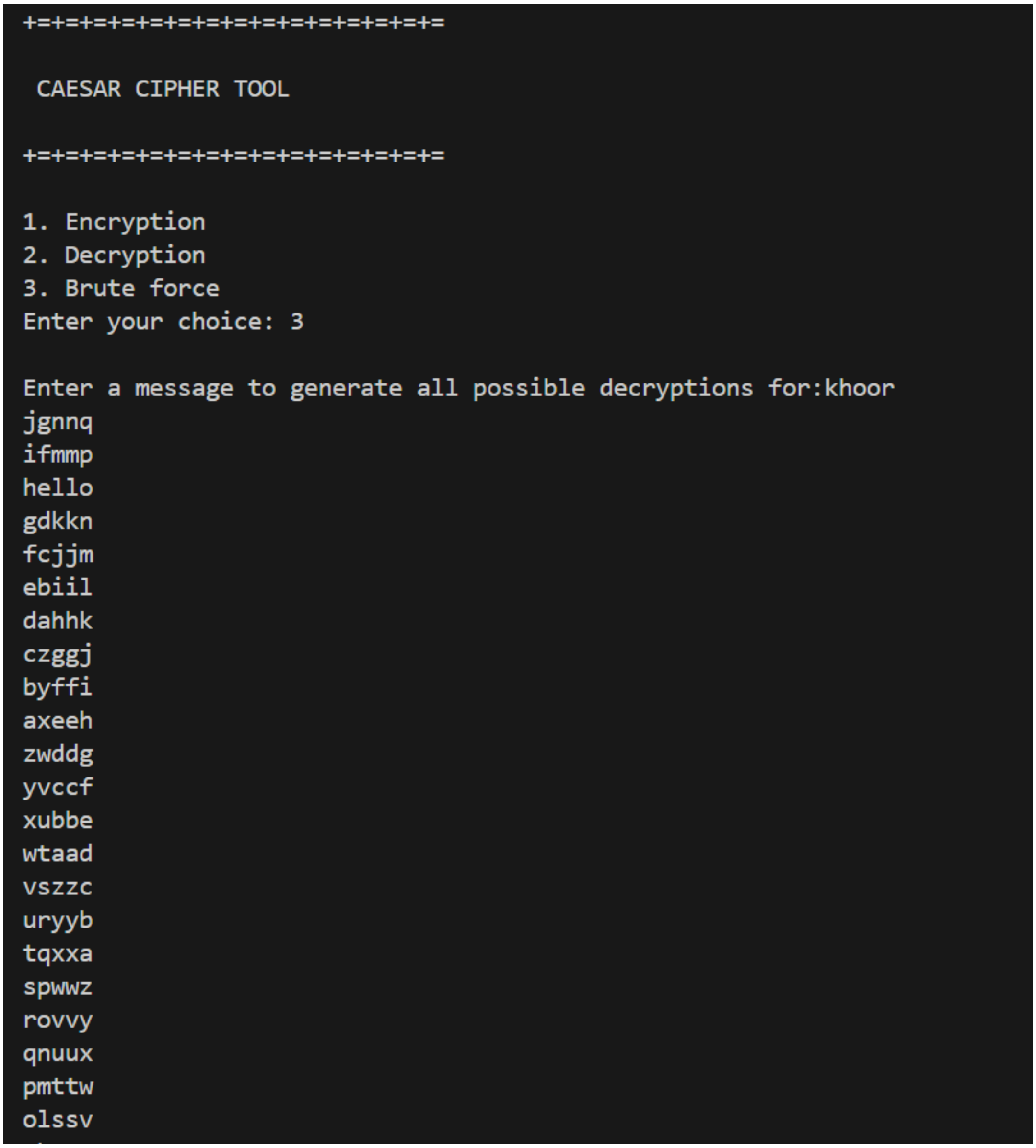
```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

 CAESAR CIPHER TOOL

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

1. Encryption
2. Decryption
3. Brute force
Enter your choice: 1

Enter a message to encrypt:Hello world!

Enter the secret key: 4
The encrypted message is: Lipps asvph!
```

Decryption:

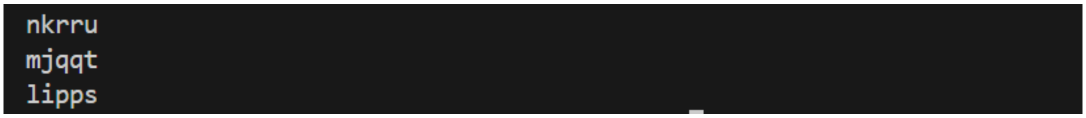


```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

 CAESAR CIPHER TOOL

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

1. Encryption
2. Decryption
3. Brute force
Enter your choice: 2

Enter a message to decrypt:khoor

Enter the secret key: 3
The decrypted message is: hello
```

Brute-force all possible decryptions:



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

 CAESAR CIPHER TOOL

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

1. Encryption
2. Decryption
3. Brute force
Enter your choice: 3

Enter a message to generate all possible decryptions for:khoor
jgnnq
ifmmp
hello
gdkkn
fcjjm
ebiil
dahhk
czggj
byffi
axeeh
zwddg
yvccf
xubbe
wtaad
vszzc
uryyb
tqxxa
spwwz
rovvy
qnuux
pmttw
olssv
```



```
nkrru
mjqqt
lipps
```

INSIGHTS:

In context of security, we grasped the basics of cryptography and also why ceasar cipher could be an unreliable choice for message encryption. It only contain 25 possible combinations which can easily be decrypted, even manually. It shows how attackers can easily break simple ciphers and also how important it is to keep the secret key hidden.

CONCLUSION:

The Caesar Cipher project successfully demonstrates fundamental cryptography and programming concepts while highlighting why simple encryption methods are inadequate for modern security needs.