IMPLEMENTATION OF CAESER CIPHER

MINIPROJECT

SUBMITTED BY:

NAME: CHAITANYA P

CANDIDATE ID: 104967

SEPTEMBER 26, 2020

L&T TECHNOLOGY SERVICES

Table of Contents

LIST OF FIGURES ii

LIST OF TABLES ii

CHAPTER 1: INTRODUCTION 1

HISTORY: 1

REQUIREMENTS GATHERING: 1

PROJECT DESCRIPTION: 2

CHAPTER 2: IMPLEMENTATION 4

DESIGN: 4

ALGORITHM 5

Caesar cipher algorithm: encryption 5

Caesar cipher algorithm: decryption 5

FLOWCHART 6

UML DIAGRAM 6

CHAPTER 3: TEST PLAN: 7

CHAPTER 4: TEST CASES: 7

CHAPTER 5: EXPECTED RESULTS: 8

ENCRYPTION: 8

DECRYPTION: 8

CHAPTER 6: ADVANTAGES AND DISADVANTAGES 9

ADVANTAGES: 9

DISADVANTAGES: 9

CHAPTER 7: CONCLUSION AND FUTURE WORK 10

CONCLUSION 10

FUTURE WORK 10

CHAPTER 8: REFERENCES AND BIBILOGRAPHY 11

LIST OF FIGURES

Figure 1: CIPHER WHEEL 1
Figure 2: REPRESENTATION OF CAESER SHIFT 2
Figure 3: ENCRYPTION WITH CAESER SHIFT 3 4
Figure 4: FLOWCHART OF IMPLEMENTATION OF CAESER CIPHER 6
Figure 5: UML DIAGRAM FOR CAESER CIPHER 6
Figure 6: EXPECTED RESULT FOR ENCRYPTION 8
Figure 7: EXPECTED RESULT FOR DECRYPTION 8
Figure 8: RELATIVE FREQUENCY OF LETTERS IN ENGLISH TEXT 9

LIST OF TABLES

Table 1: NUMERIC TRANSFORMATION FOR ENCRYPTION BY MODULAR ARITHMETIC 3
Table 2: TEST CASES 7

CHAPTER 1: INTRODUCTION

HISTORY:

The Caesar cipher is named after Julius Caesar, who used it with a shift of three (A becoming D when encrypting, and D becoming A when decrypting) to protect messages of military significance. While Caesar's was the first recorded use of this scheme, other substitution ciphers are known to have been used earlier.

If he had anything confidential to say, he would write it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, they must substitute the fourth letter of the alphabet, namely D, for A [3].

Figure 1: CIPHER WHEEL

PROBLEM STATEMENT:

To keep important information unknown to third parties but allow interception by required parties, Caeser cipher is one of the techniques used.

REQUIREMENTS GATHERING:

- Plaintext: this is the original intelligible message or data that is fed into the algorithm as input.
- Encryption algorithm: the algorithm performs substitution on the plaintext.
- Secret key: this is the input to the encryption algorithm. Its value is independent of the plaintext and the algorithm. The algorithm produces output depending on the value of this key.
- Ciphertext: this is the scrambled message produced as the output. It’s a random stream of data and is unintelligible [4].
- Decryption algorithm: this is essentially the encryption algorithm run in reverse. The output of the algorithm is the original plaintext.

PROJECT DESCRIPTION:

In cryptography, Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

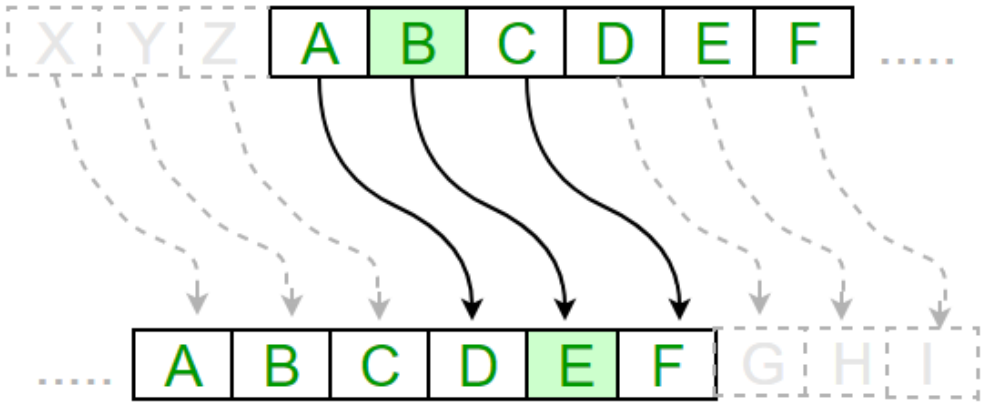

Figure 2: REPRESENTATION OF CAESER SHIFT

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

```
Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:  XYZABCDEFGHIJKLMNOPQRSTUVW
```

When **encrypting**, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

```
Plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD
```

Deciphering is done in reverse, with a right shift of 3.

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A → 0, B → 1, ..., Z → 25. Encryption of a letter *x* by a shift *n* can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

(There are different definitions for the modulo operation. In the above, the result is in the range 0 to 25; i.e., if $x + n$ or $x - n$ are not in the range 0 to 25, we have to subtract or add 26.)

The replacement remains the same throughout the message, so the cipher is classed as a type of monoalphabetic substitution, as opposed to polyalphabetic solution.

Table 1: NUMERIC TRANSFORMATION FOR ENCRYPTION BY MODULAR ARITHMETIC

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

CHAPTER 2: IMPLEMENTATION

DESIGN:

One simple and basic method to encrypt a message is using Caesar's cipher. It is a very simple form of encryption, where we take letters one by one from the original message and translate it into an encrypted text. A C program design that will encrypt and decrypt the text using Caesars cipher. On a high-level, will do the following [5]:

- The source text that needs to be encrypted is given in lower case. But if we need to decrypt the text, it should be given in upper case.
- When it is encrypted, each letter will have its ANSII code increased for three places. When it is decrypted, it will have its code moved toward left.
- The letter 'x' will be translated into 'A', the letter 'y' is transformed into the letter 'B', and the 'z' will change into 'C'.
- The program will handle only English letters and each input text will not be longer that one sentence. At the end of the input sentence it should have the marker for end '.'.
- The longest sentence is 1024 letters long. This prevents the user to input the sentence that would over populate the size of the program.
- The numbers in the input will not be changed.
- The blank symbol or any non-letter symbol will not be changed.
- The decryption is reverse. If we input the encrypted text, we should get decrypted text as the output.

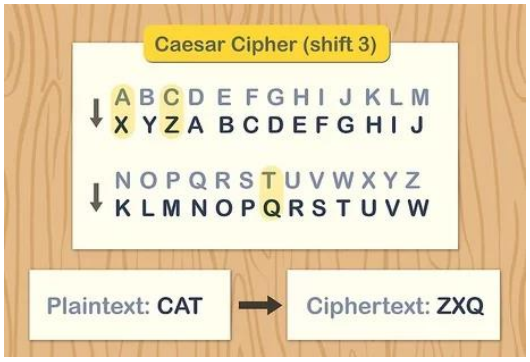

Figure 3: ENCRYPTION WITH CAESER SHIFT 3

ALGORITHM

Caesar cipher algorithm: encryption

Store letters as numbers: A=1, B=2, C=3 etc.

START

- INPUT message
    - take first letter (only lower case letters will be encrypted)
    - change letter to number
    - add 3 to number
    - change number back to letter
    - display letter
- Repeat until end of message

STOP

Caesar cipher algorithm: decryption

Store letters as numbers: A=1, B=2, C=3 etc.

START

- IF receive message
    - take first letter (only upper case letters will be decrypted)
    - change letter to number
    - subtract 3 to number
    - change number back to letter
    - display letter
- Repeat until end of message

STOP

FLOWCHART

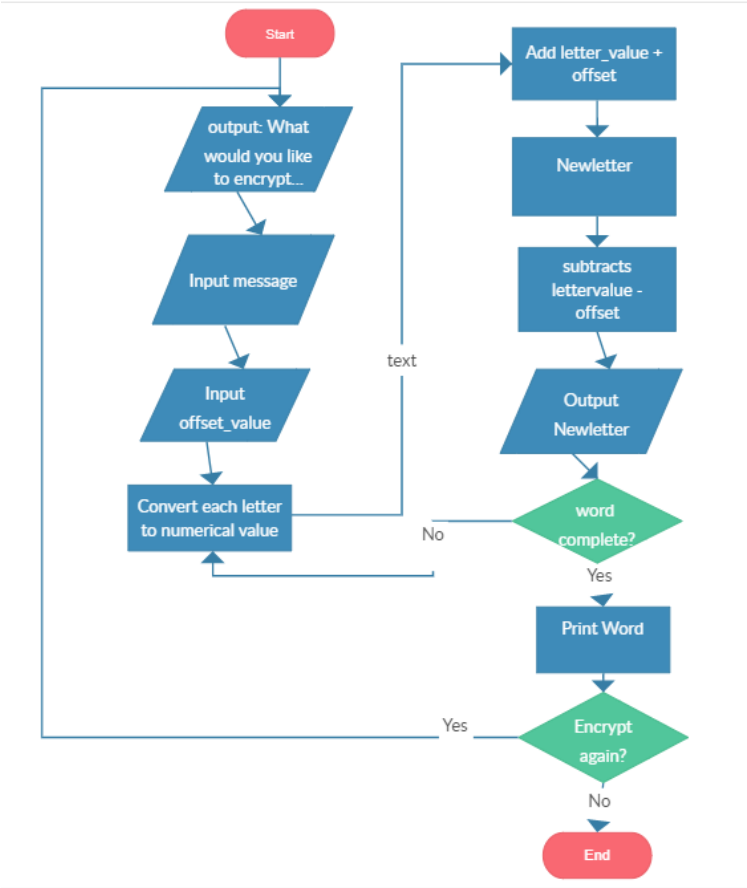

Figure 4: FLOWCHART OF IMPLEMENTATION OF CAESER CIPHER

UML DIAGRAM

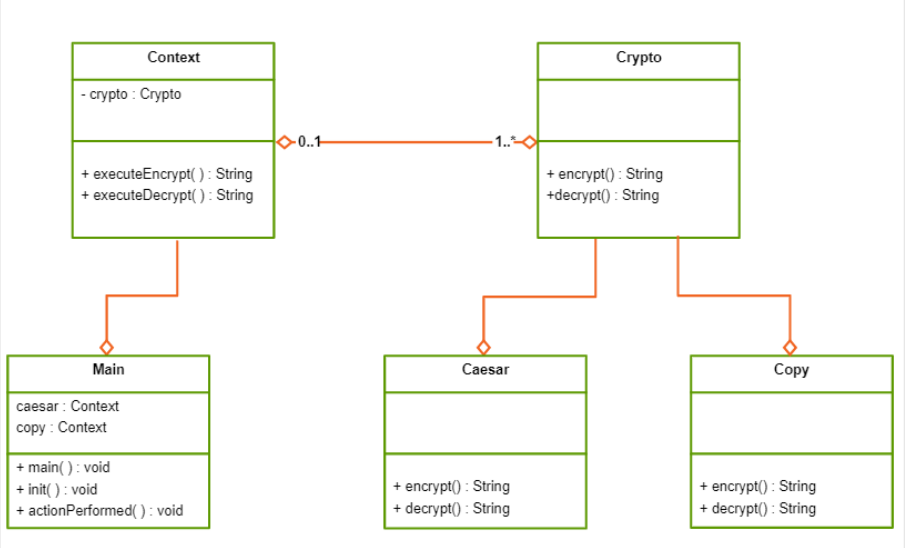

Figure 5: UML DIAGRAM FOR CAESER CIPHER

CHAPTER 3: TEST PLAN:

1. Encrypt a message using Caeser cipher encryption algorithm.
2. Decrypt the encrypted message using Caeser cipher decryption algorithm.
3. Compare initial message and the decrypted message.
4. Pass the test case when initial and decrypted messages are same.
5. Fail the test case when initial and decrypted messages are not same.

CHAPTER 4: TEST CASES:

Table 2: TEST CASES

SL. No	PLAIN TEXT (INPUT)	CIPHER TEXT (ENCRYPTED OUTPUT)	PLAIN TEXT (DECRYPTED OUTPUT)
1	hello	KHOOR	hello
2	chaitanya	FKDLWDQBD	chaitanya
3	l&t technology services	O&W WHFKQRORJB VHUYLFHV	l&t technology services
4	embedded123	HPEHGGHG123	embedded123
5	Life_long_learning	LLIH_ORQJ_OHDUQLQJ	Life_long_learning

CHAPTER 5: EXPECTED RESULTS:

The choice of encryption on decryption to be performed on the given text can be selected by the user. User has to enter E (in uppercase or lower case) for encryption, and D ((in uppercase or lower case) for decryption. Once the choice is selected the text can be entered for encryption or decryption.

ENCRYPTION:

```
To encrypt, input e or E

To decrypt, input d or D

To exit, input any other letter

Your choice:->

e
Input text to encrypt->
chaitanya p
FKDLWDQBD S
```

Figure 6: EXPECTED RESULT FOR ENCRYPTION

DECRYPTION:

```
To decrypt, input d or D

To exit, input any other letter

Your choice:->

D
Input text to decrypt->
FKDLWDQBD S
chaitanya p
```

Figure 7: EXPECTED RESULT FOR DECRYPTION

CHAPTER 6: ADVANTAGES AND DISADVANTAGES

Most ciphers and especially the early ones had to easy to perform in the field. In particular it was dangerous to have the cryptosystem algorithms written down for the soldiers or spies to follow. Any cipher that was so complicated that its algorithm had to be written out was at risk of being revealed if the interceptor caught a sender with the written instructions. Then the interceptor could readily decode any cipher text messages intercepted. Following are some of the advantages and disadvantages of Caeser cipher.

ADVANTAGES:

- Use of only a short key in the entire process
- One of the best methods to use if the system cannot use any complicated coding techniques
- Requires few computing resources
- In terms of speed of execution Caesar cipher algorithm is still the fastest owing to its simplicity.
- Simple structure usage

DISADVANTAGES:

- Can only provide minimum security to the information
- Frequency of the letter pattern provides a big clue in deciphering the entire message

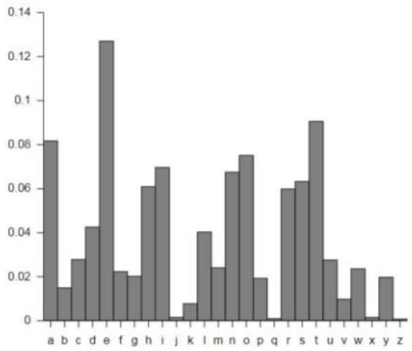

Figure 8: RELATIVE FREQUENCY OF LETTERS IN ENGLISH TEXT

CHAPTER 7: CONCLUSION AND FUTURE WORK

CONCLUSION

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique [2].

FUTURE WORK

Caeser cipher is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So, it becomes very important to augment this algorithm by adding new levels of security to make it applicable. One way to make Caeser cipher a bit harder to break is to use different shifts at different positions in the message which is Vignere cipher [1].

CHAPTER 8: REFERENCES AND BIBILOGRAPHY

[1]http://www.math.stonybrook.edu/~scott/Book331/Improved_Caesar_like_cipher.html

[2]https://www.techopedia.com/definition/6311/caesar-cipher

[3]https://www.google.com/search?q=caesar+cipher+wikipedia&rlz=1C1CHBD_enIN804IN804&oq=CAesar+cipher+WIKI&aqs=chrome.1.69i57j0l2j69i60l3.10184j0j7&sourceid=chrome&ie=UTF-8

[4] W. STALLINGS, CRYPTOGRAPHY AND NETWORK SECURITY, PEARSON.

[5]https://brilliant.org/wiki/caesar-cipher/

BIBILOGRAPHY

[1] [Online]. Available: http://www.math.stonybrook.edu/~scott/Book331/Improved_Caesar_like_cipher.html.

[2] [Online]. Available: https://www.techopedia.com/definition/6311/caesar-cipher.

[3] [Online]. Available: https://www.google.com/search?q=caesar+cipher+wikipedia&rlz=1C1CHBD_enIN804IN804&oq=CAesar+cipher+WIKI&aqs=chrome.1.69i57j0l2j69i60l3.10184j0j7&sourceid=chrome&ie=UTF-8.

[4] W. STALLINGS, CRYPTOGRAPHY AND NETWORK SECURITY, PEARSON.

[5] [Online]. Available: https://brilliant.org/wiki/caesar-cipher/.