CS 131 : Discrete Structures Project

Cryptography: Caesar Cipher

By. Sujin Kim

Overview

What is Caesar Cipher?

- Introduction to Cryptography
- Caesar Cipher: How does it work?
- Mathematical Description

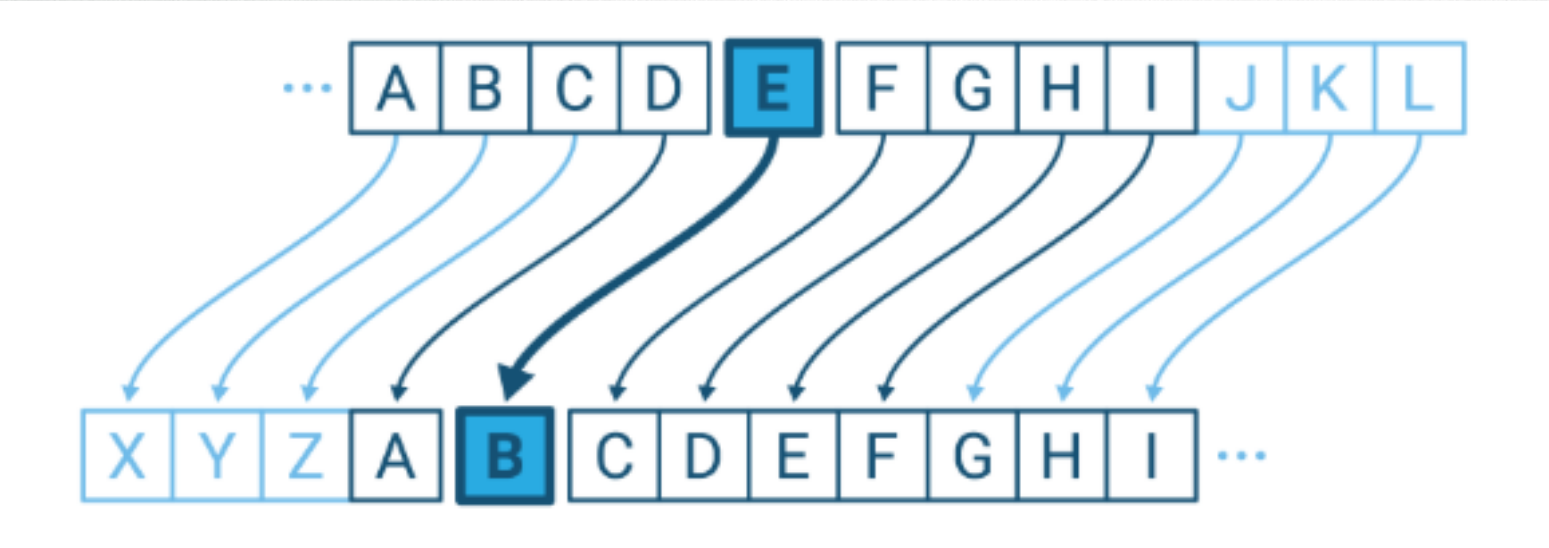
Java Project: Sujin's Secret Message Translator

- Purpose / Introduction
- Implementation of Caesar Cipher
- Program Demo / Test Case
- Github Link / Youtube Link / Work Cited

What is Cryptography?

- A method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

- **“Hidden Writing”**
  - The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."



Caesar cipher (or **Caesar** code) is a shift **cipher**, one of the easiest, earliest and most famous encryption systems.

Caesar Cipher

- Named after Julius Caesar, who used it in his private correspondence with officers
- A type of substitution cipher
- Each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.
- For example with a shift of 1, A would be replaced by B, B would become C, and so on

ABCD → BCDE

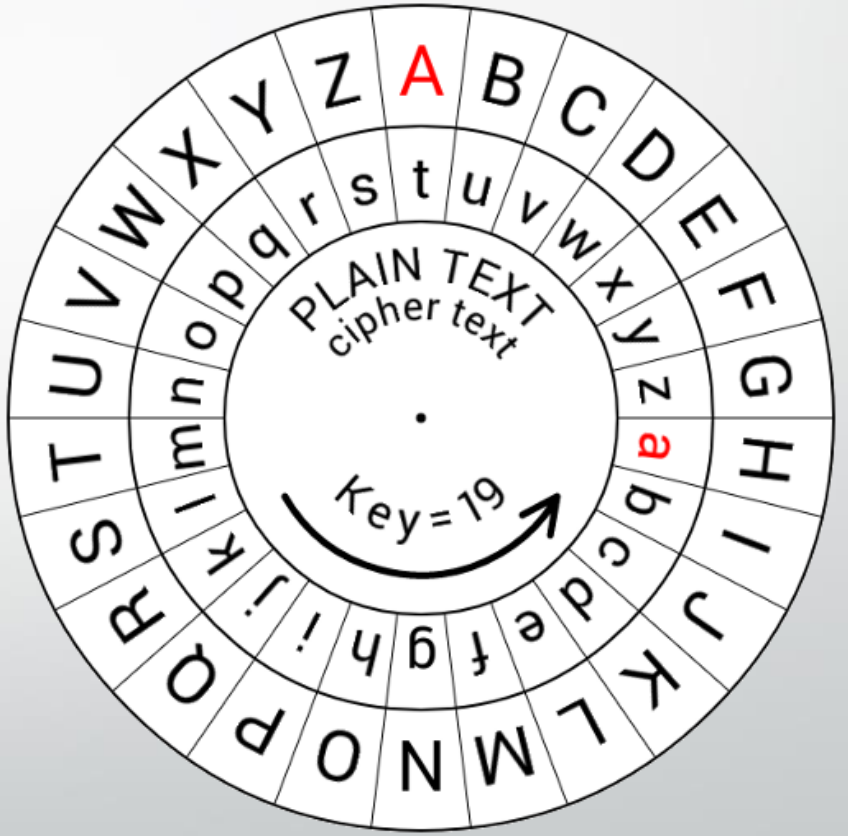
Caesar Cipher : Mathematical Description

- Encryption Phase with shift n

$$e(x) = (x+n)(\mathrm{mod}\ 26)$$

- Decryption Phase with shift n

$$d(x) = (x-n)(\mathrm{mod}\ 26)$$



Java Project
<Sujin's Secret Message Translator>

Step 1- Planning

1) Introduction Message
2) Menu Driven – Encrypt, Decrypt, Quit
3) Encryption- 3 steps (ask user input + encryption method + show output)
4) Decryption- 3 steps (ask user input + decryption method + show output)
5) Quit- allow user to exit the program

Step 2- Implementation

1) Extract one character at a time from the user input text

```
for (int i=0; i<text.length(); i++)
{
    if (Character.isUpperCase(text.charAt(i)))
    {
        char ch = (char)(((int)text.charAt(i) +
                          s - 65) % 26 + 65);
        result.append(ch);
    }
    else if (Character.isLowerCase(text.charAt(i)))
    {
        char ch = (char)(((int)text.charAt(i) +
                          s - 97) % 26 + 97);
        result.append(ch);
    }
```

2)For each character, transform the extracted character as per rule by the shift value of 3

```
final int SHIFT = 3;
String encryptedMsg = encryptMessage(text,SHIFT).toString();
String decryptedMsg =decryptMessage(cipher,26-SHIFT).toString();
```

3)Return the new string generated

```
System.out.println("Secrect Message: " + encryptedMsg);
System.out.println("Decrypted Mssage: " + decryptedMsg);
```

Test Case

1. Encryption

```
================================================================================
|Sujin's Secret Message Translator|
-This Program will encrypt and decrypt message by using Caesar Cipher technique-
1. Encrypt Message
2. Decrypt Message
3. Exit the Program
Press 1,2 or 3 to Exit the Program: 1

Enter The Message to EnCrypt: Discrete Math is Awesome!
Secrect Message: Glvfuhwh Pdwk lv Dzhvrph!
```

2. Decryption

```
================================================================================
|Sujin's Secret Message Translator|
-This Program will encrypt and decrypt message by using Caesar Cipher technique-
1. Encrypt Message
2. Decrypt Message
3. Exit the Program
Press 1,2 or 3 to Exit the Program: 2

Enter The Message to Decrypt:
Glvfuhwh Pdwk lv Dzhvrph!
Decrypted Mssage: Discrete Math is Awesome!
```

GitHub Link

- https://github.com/ShaggyBox/CS131_2021_WEST/tree/Sujin_Kim_Project

YouTube Link

- https://www.youtube.com/watch?v=FT5VhuTSx10

Work Cited

- https://searchsecurity.techtarget.com/definition/cryptography
- https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/