ADVANCED SYSTEM SECURITY AND DIGITAL FORENSICS

MINI PROJECT

TOPIC: Caesar Cipher Encryption Technique

Class: BECMPN-1

Group Members

Name

Rahul Kalsariya

Index

- Introduction…… 3
- Algorithm…….. 4
- Diagrams…….. 5
- Code…… 9
- Output…….. 12

Introduction

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., 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. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus, to cipher a given text we need an integer value, known as shift which indicates the number of positions each letter of the text has been moved down.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communications security.

The encryption can 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 by a shift n can be described mathematically as.

$$E(x)=(x+n)mod\ 26$$

(Encryption Phase with shift n)

$$D(x)=(x-n)mod\ 26$$

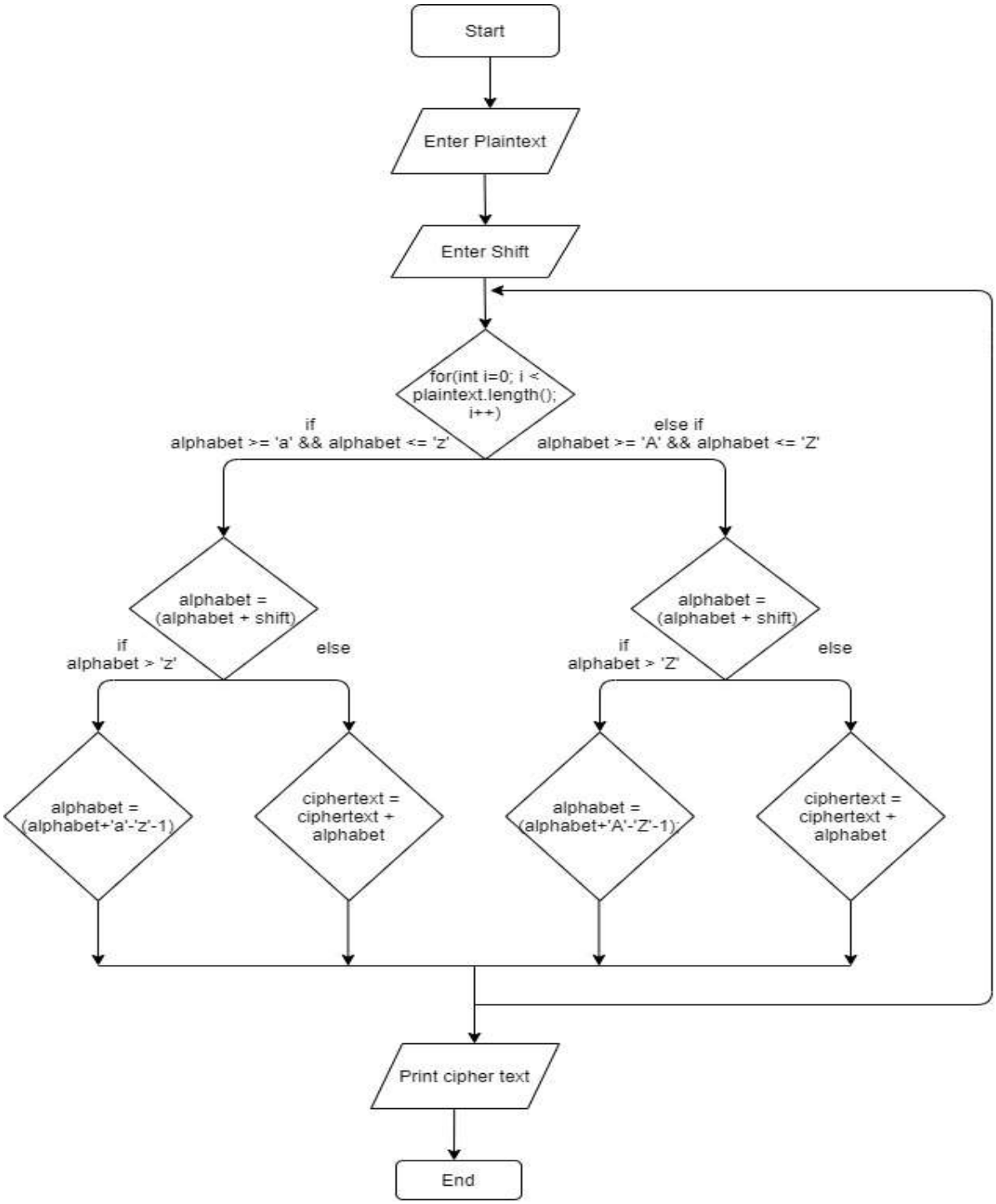
(Decryption Phase with shift n)

Algorithm

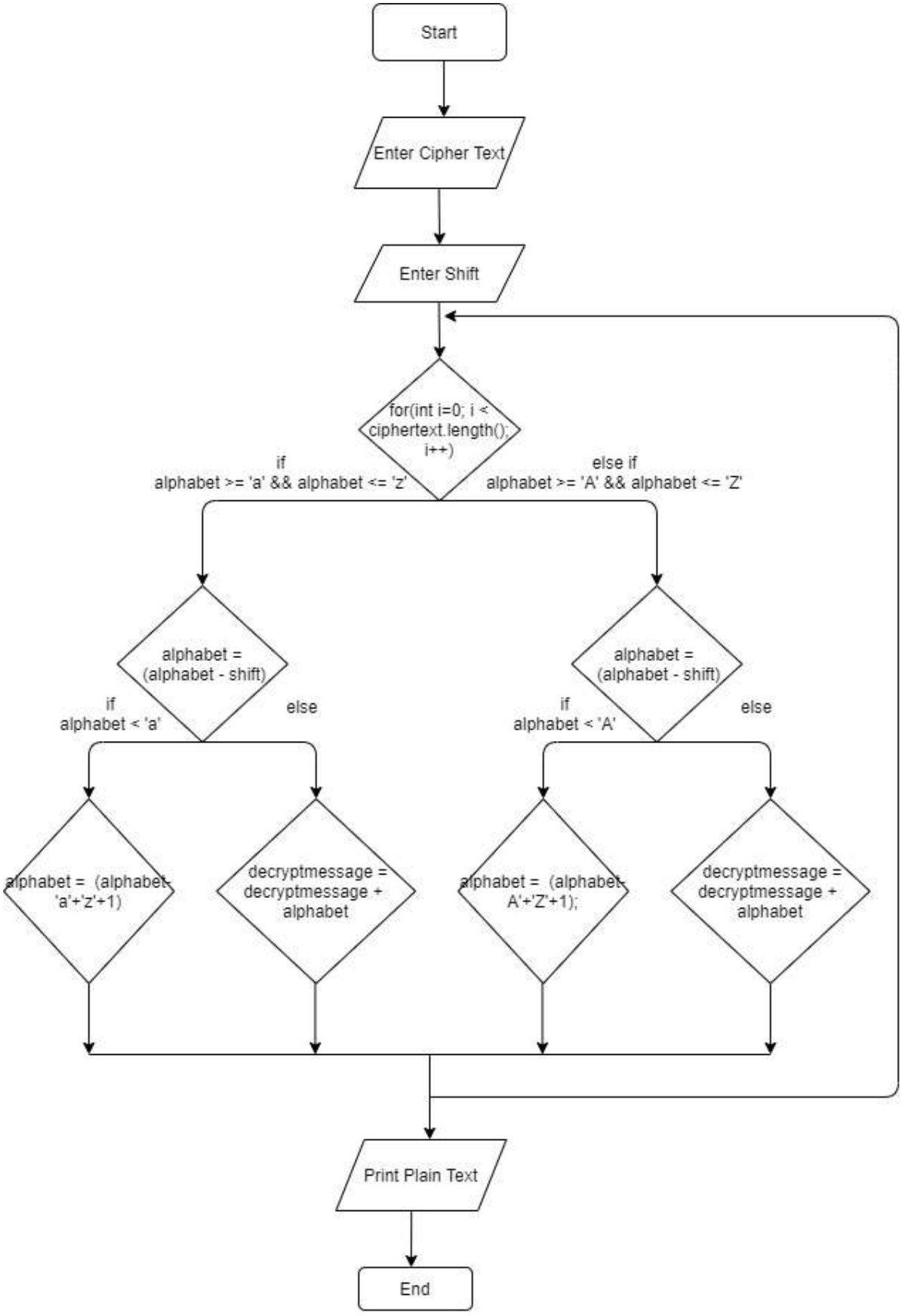
- Enter the plain text or cipher text as a input
- Enter an Integer between 0-25 denoting the required shift.
- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Return the new string generated.

Diagrams

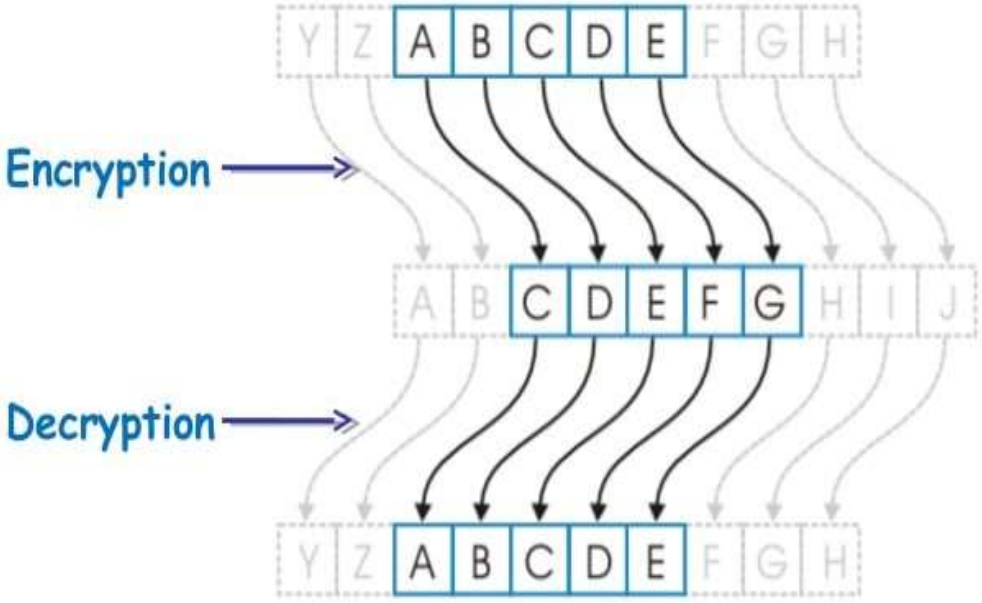
- Encryption Flow chart



- Decryption Flow Chart



- Caesar Cipher Shift Diagram


Y Z A B C D E F G H
Encryption
A B C D E F G H I J
Decryption
Y Z A B C D E F G H

Code

- Encryption Java Code

```
import java.util.*;
public class Encryption {
   public static void main(String args[]) {
      Scanner sc = new Scanner(System.in);
      System.out.println(" Input the plaintext message : ");
      String plaintext = sc.nextLine();
      System.out.println(" Enter the value by which each character in the plaintext message gets shifted : ");
      int shift = sc.nextInt();
      String ciphertext = "";
      char alphabet;
      for(int i=0; i < plaintext.length();i++)
      {
         alphabet = plaintext.charAt(i);
         if(alphabet >= 'a' && alphabet <= 'z')
         {
          alphabet = (char) (alphabet + shift);
          if(alphabet > 'z') {
             alphabet = (char) (alphabet+'a'-'z'-1);
          }
          ciphertext = ciphertext + alphabet;
         }
         else if(alphabet >= 'A' && alphabet <= 'Z') {
          alphabet = (char) (alphabet + shift);
          if(alphabet > 'Z') {
             alphabet = (char) (alphabet+'A'-'Z'-1);
```

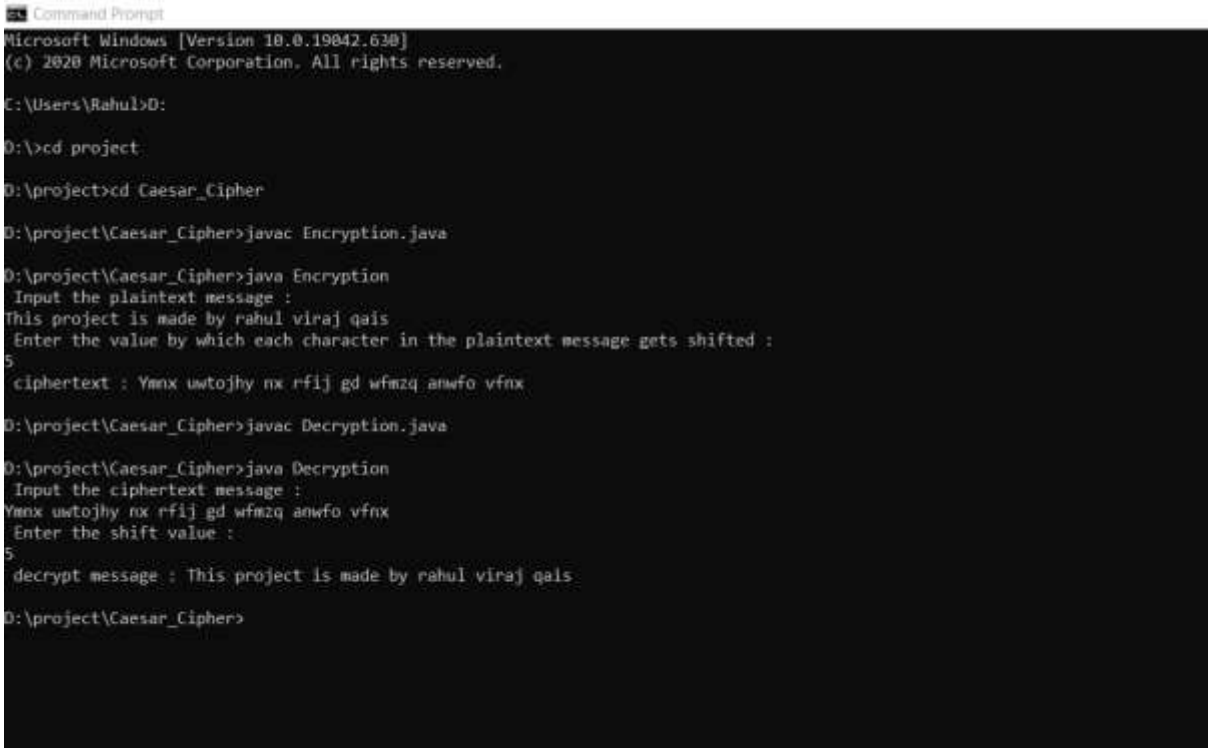
```
        }
        ciphertext = ciphertext + alphabet;
       }
       else {
        ciphertext = ciphertext + alphabet;
       }
```

- Decryption Java Code

```
import java.util.*;
public class Decryption {
    public static void main(String args[]) {
    Scanner sc = new Scanner(System.in);
    System.out.println(" Input the ciphertext message : ");
    String ciphertext = sc.nextLine();
    System.out.println(" Enter the shift value : ");
    int shift = sc.nextInt();
    String decryptMessage = "";
    for(int i=0; i < ciphertext.length();i++)
    {
       char alphabet = ciphertext.charAt(i);
       if(alphabet >= 'a' && alphabet <= 'z')
       {
          alphabet = (char) (alphabet - shift);
          if(alphabet < 'a') {
             alphabet = (char) (alphabet-'a'+'z'+1);
          }
          decryptMessage = decryptMessage + alphabet;
       }
```

```
        else if(alphabet >= 'A' && alphabet <= 'Z')
        {
           alphabet = (char) (alphabet - shift);
           if (alphabet < 'A') {
              alphabet = (char) (alphabet-'A'+'Z'+1);
           }
           decryptMessage = decryptMessage + alphabet;
        }
        else
        {
         decryptMessage = decryptMessage + alphabet;
        }
      }
      System.out.println(" decrypt message : " + decryptMessage);
   }
}
```

Output


Command Prompt
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\Rahul>D:
D:\>cd project
D:\project>cd Caesar_Cipher
D:\project\Caesar_Cipher>javac Encryption.java
D:\project\Caesar_Cipher>java Encryption
Input the plaintext message :
This project is made by rahul viraj qais
Enter the value by which each character in the plaintext message gets shifted :
5
ciphertext : Ymnx uwtojhy nx rfij gd wfmzq anwfo vfnx
D:\project\Caesar_Cipher>javac Decryption.java
D:\project\Caesar_Cipher>java Decryption
Input the ciphertext message :
Ymnx uwtojhy nx rfij gd wfmzq anwfo vfnx
Enter the shift value :
5
decrypt message : This project is made by rahul viraj qais
D:\project\Caesar_Cipher>