KARNATAK LAW SOCIETY’S

GOGTE INSTITUTE OF TECHNOLOGY

UDYAMBAG, BELAGAVI-590008

(An Autonomous Institution under Visvesvaraya Technological University, Belagavi)

**(APPROVED BY AICTE, NEW DELHI)**

Department of Electronics and Communication Engineering



*Course Project Report on*

**Encryption and Decryption using Substitution Cipher**

*Submitted in partial fulfillment of the requirement for the award of the degree of*

**Bachelor of Engineering**

**in**

***Computer Organization and Architecture***

*Submitted by*

SHIVANI PATIL 2GI17EC121

SHREYA SARAF 2GI17EC126

SURAJ VIBAYKUMAR 2GI17EC146

**Guide**

Proff. MS Chougle

**2018–2019**

**ENCRYPTION AND DECRYPTION**

**OF A PLAIN TEXT USING SUBSTITUTION CIPHER**

**Objective of the Project:**

To Encrypt and Decrypt a plain text using Substitution Cipher.

**Code:**

1**. Encryption:**

#include<stdio.h>

int main()

{

printf("\*\*\*\*\*\*\*\*\*\* SUBSTITUTION CIPHER ENCRYPTION \*\*\*\*\*\*\*\*\*\*\n");

printf("Working flow of the program\nExample\n");

printf("\nEnter the plain text\nbat\n");

printf("Enter the number of alphabets to be replaced\n2\n");

printf("Enter the alphabets to be replaced without space\nab\n");

printf("Enter the replacement alphabets\ncd\n");

printf("Cipher text is\ndct\n");

printf("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\n\n\n");

//main program

int alphanum;//to read number alphabets to be replaced

char plaintext[100],ciphertext[100];//strings to store plain text and cipher text

//input plain text

printf("\nEnter the plain text\n");

gets(plaintext);

//input number of alphabets to be replaced

printf("Enter the number of alphabets to be replaced\n");

scanf("%d",&alphanum);

//input the replacement table in form of two strings

char letter[alphanum],replacewith[alphanum];

printf("Enter the alphabets to be replaced without space\n");

getchar();

gets(letter);//input characters to be replaced

printf("Enter the replacement alphabets\n");

gets(replacewith);//input characters to be replaced as

int i,j;

//loop to travel through plain text

for(i=0;plaintext[i]!='\0';i++)

{

//loop to find presence of plain text character in the replacement table

//if yes then replace it

for(j=0;letter[j]!='\0';j++)

{

//find the occurance if found then replace else keep as it is

if(plaintext[i]==letter[j])

{

ciphertext[i]=replacewith[j];

break;//replace and go to next plain text character

}

else

ciphertext[i]=plaintext[i];

}

}

ciphertext[i]='\0';//end the cipher text string

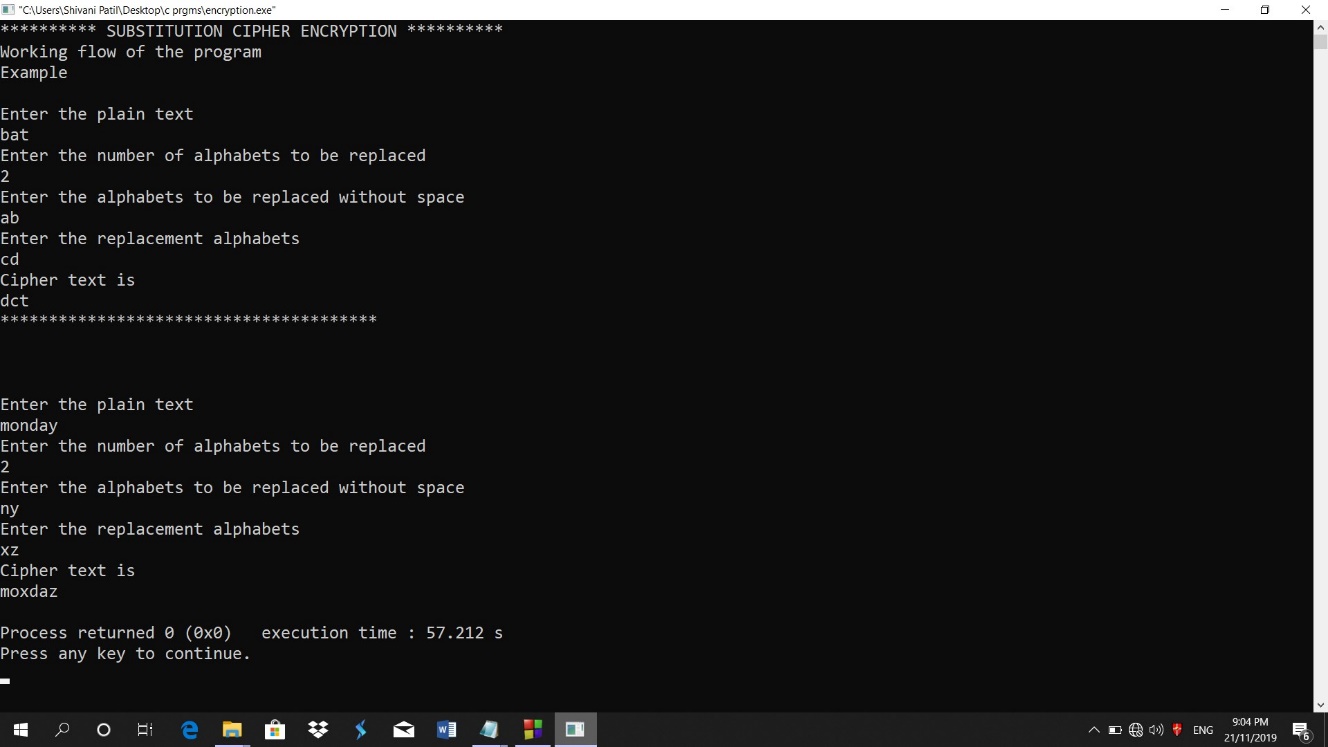
printf("Cipher text is\n");

puts(ciphertext);//output ciphered text

return 0;

}

**Sample Input and Output for Encryption**



**2. Decryption:**

#include<stdio.h>

int main()

{

printf("\*\*\*\*\*\*\*\*\*\* SUBSTITUTION CIPHER DECRYPTION \*\*\*\*\*\*\*\*\*\*\n");

printf("Working flow of the program\nExample\n");

printf("\nEnter the Cipher text\nbat\n");

printf("Enter the number of alphabets to be replaced\n2\n");

printf("Enter the alphabets to be replaced without space\nab\n");

printf("Enter the replacement alphabets\ncd\n");

printf("Plain text is\ndct\n");

printf("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\n\n\n");

//main program

char ciphertext[100],plaintext[100];//strings to store plain text and cipher text

//input plain text

printf("\nEnter the Cipher text\n");

gets(ciphertext);

int alphanum;//to read number alphabets to be replaced

//input number of alphabets to be replaced

printf("Enter the number of alphabets to be replaced\n");

scanf("%d",&alphanum);

//input the replacement table in form of two strings

char letter[alphanum],replacewith[alphanum];

printf("Enter the alphabets to be replaced without space\n");

getchar();

gets(letter);//input characters to be replaced

printf("Enter the replacement alphabets\n");

gets(replacewith);//input characters to be replaced as

int i,j;

//loop to travel through cipher text

for(i=0;ciphertext[i]!='\0';i++)

{

//loop to find presence of cipher text character in the replacement table

//if yes then replace it

for(j=0;letter[j]!='\0';j++)

{

//find the occurrence if found then replace else keep as it is

if(ciphertext[i]==letter[j])

{

plaintext[i]=replacewith[j];

break;//replace and go to next cipher text character

}

else

plaintext[i]=ciphertext[i];

}

}

plaintext[i]='\0';//end the plain text string

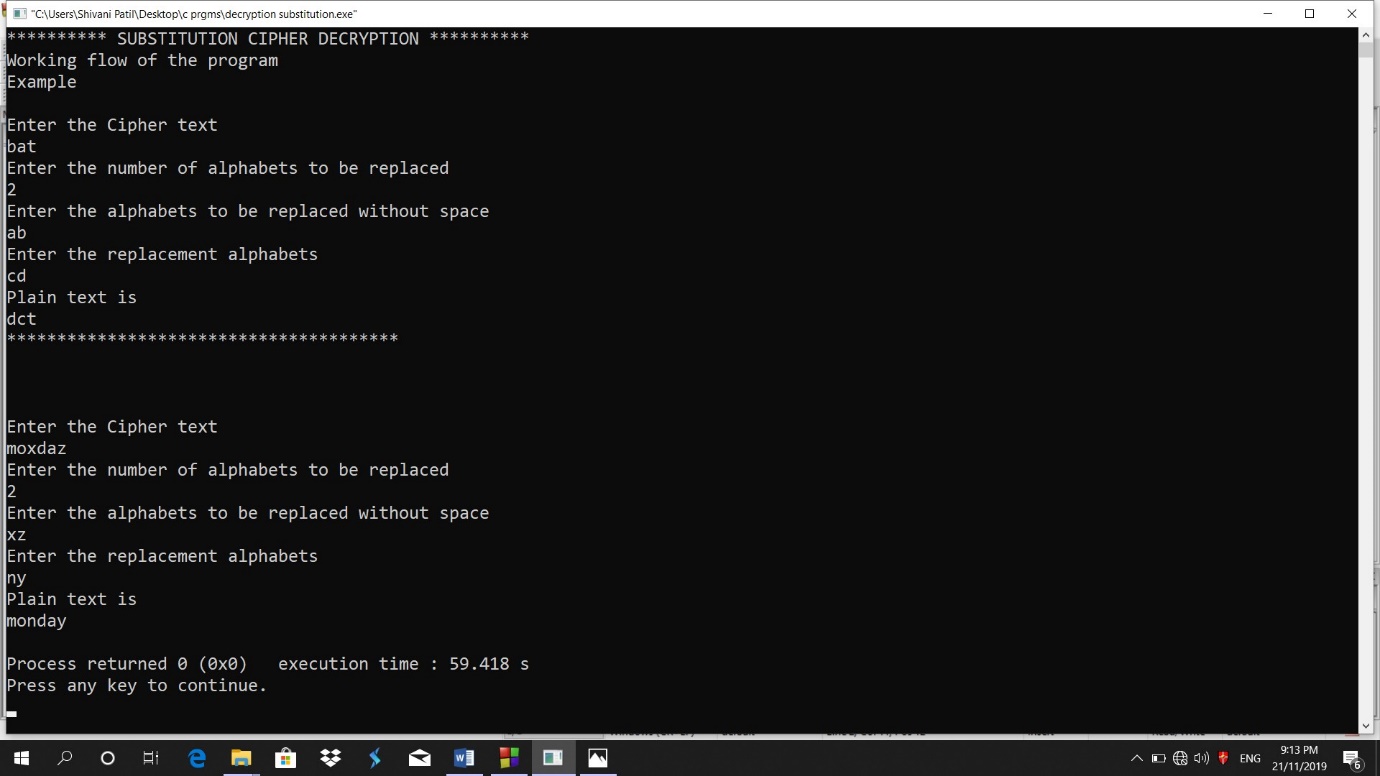
printf("Plain text is\n");

puts(plaintext);//output ciphered text

return 0;

}

**Sample Input and Output for Decryption**



**Limitations:**

* Program fails when same letters/symbols/numbers are present multiple times in plaintext as it provides different output after decryption.
* These ciphers are easy to break because they reflect the frequency data of the original alphabet
* Practical problem of encrypting large files is that it requires millons of random characters on a regular basis and supplying truly random characters in this volume is a significant task.

**Improvements:**

* Data can be more efficiently encrypted and decrypted using block cipher techniques like DES, AES.
* Permutation and combination techniques can be added in program for efficient encryption.