Information Security
Lab 4
Aim: To Implement Vigenère Cipher

Name: - Shri Darandale
PRN: - 20210801066

1. Program definition –

   Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère table or it's formulas.

   The formula for encryption is:

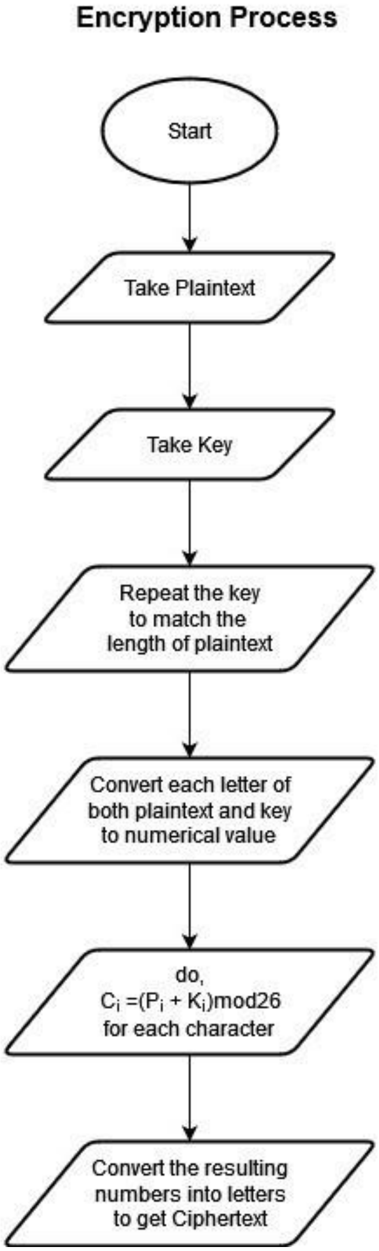
   $C=(P+K)\bmod 26$

   And the formula for decryption is:

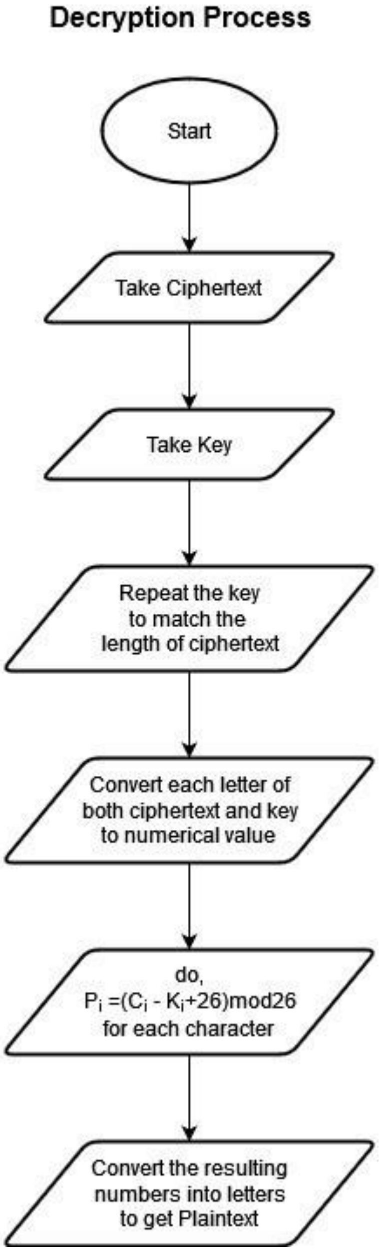
   $P=(C-K)\bmod 26$

   Flowchart: -

2.



Encryption Process
Start
Take Plaintext
Take Key
Repeat the key to match the length of plaintext
Convert each letter of both plaintext and key to numerical value
do, $C_i = (P_i + K_i) \bmod 26$ for each character
Convert the resulting numbers into letters to get Ciphertext



Decryption Process
Start
Take Ciphertext
Take Key
Repeat the key to match the length of ciphertext
Convert each letter of both ciphertext and key to numerical value
do, $P_i = (C_i - K_i + 26) \bmod 26$ for each character
Convert the resulting numbers into letters to get Plaintext

Algorithm: -

Encryption:

Step 1) Choose a keyword or phrase that both the sender and receiver know (e.g., "KEY").

Step 2) Repeat the keyword or phrase to match the length of the plaintext message (e.g., "KEYKEYKEY").

Step 3) Align the keyword above the plaintext.

Step 4) Convert each letter of the keyword and plaintext to a numerical value (e.g., A=0, B=1, C=2, etc.).

Step 5) Add the numerical values of the corresponding letters in the keyword and plaintext.

Step 6) Take the result modulo 26 (as there are 26 letters in the alphabet).

Step 7) Convert the resulting numbers back to letters using the same numerical mapping (A=0, B=1, C=2, etc.).

Decryption:

Step 1) Repeat the received keyword or phrase to match the length of the ciphertext message (e.g., "KEYKEYKEY").

Step 2) Align the keyword above the ciphertext.

Step 3) Convert each letter of the keyword and ciphertext to a numerical value (e.g., A=0, B=1, C=2, etc.).

Step 4) Subtract the corresponding numeric value of keyword letter from ciphertext letter.

Step 5) Add 26 if the result is negative.

Step 6) Convert the resulting numbers back to letters using the same numerical mapping (A=0, B=1, C=2, etc.).

Implementation: -

```
# Vigenère Cipher

def      vignere(text,key,mode="e"):
text,key=text.upper(),key.upper()
if mode=="d":
```

4.

```
       k = -1     elif
mode=="e":
k = 1     else:
       return
   output = [chr((ord(text[i])+(ord(key[i%len(key)])*k)+130)%26+65) for i in
range(len(text))]
   return "".join(output)

plaintext = input("Enter the Plain Text: ") key = input("Enter the
Key: ") encrypted_text =
vignere(text=plaintext,key=key,mode="e") print("Encrypted:",
encrypted_text) decrypted_text =
vignere(text=encrypted_text,key=key,mode="d")
print("Decrypted:", decrypted_text)
```

Input and Output: -

Case 1: -

Plaintext – GEEKSFORGEEKS
Key – AYUSH
Output –

```
Ciphertext: GCYCZFMLYLEIM
Plaintext: GEEKSFORGEEKS
```

Case 2: -

Plaintext – GETREADY
Key – TOWIN
Output –

```
Ciphertext: ZSPZRTRU
Plaintext: GETREADY
```

Case 3: -

Plaintext – HELLOWORLD
Key – GEEKSFORGEEKS
Output –

Ciphertext: NIPVGBCIRH

Plaintext: HELLOWORLD

Case 4: -

Plaintext – GOODBYE

Key – HELLO

Output –

Ciphertext: NSZOPFI

Plaintext: GOODBYE