PRACTICAL-1

AIM:

Implement the cipher in any programming language of your choice. Perform encryption, decryption.

Discuss and try some possible attacks on traditional Caesar cipher.

THEORY:

- Caesar Cipher Technique is the simple and easy method of encryption technique.
- It is simple type of substitution cipher.
- Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.
- The plain text character is traversed one at a time.
- For each character in the given plain text, transform the given character as per the rule depending on the procedure of encryption and decryption of text.
- After the steps is followed, a new string is generated which is referred as cipher text.

BRUTE FORCE:

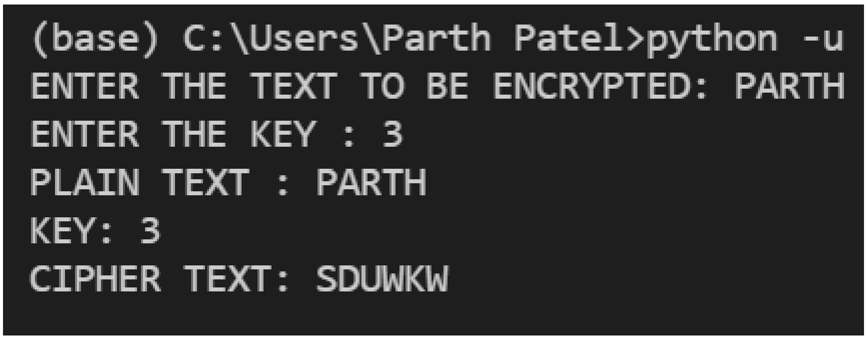
- The cipher text can be hacked with various possibilities.
- One of such possibility is **Brute Force Technique,** which involves trying every possible decryption key.
- This technique does not demand much effort and is relatively simple for a hacker.

PROGRAM CODE:

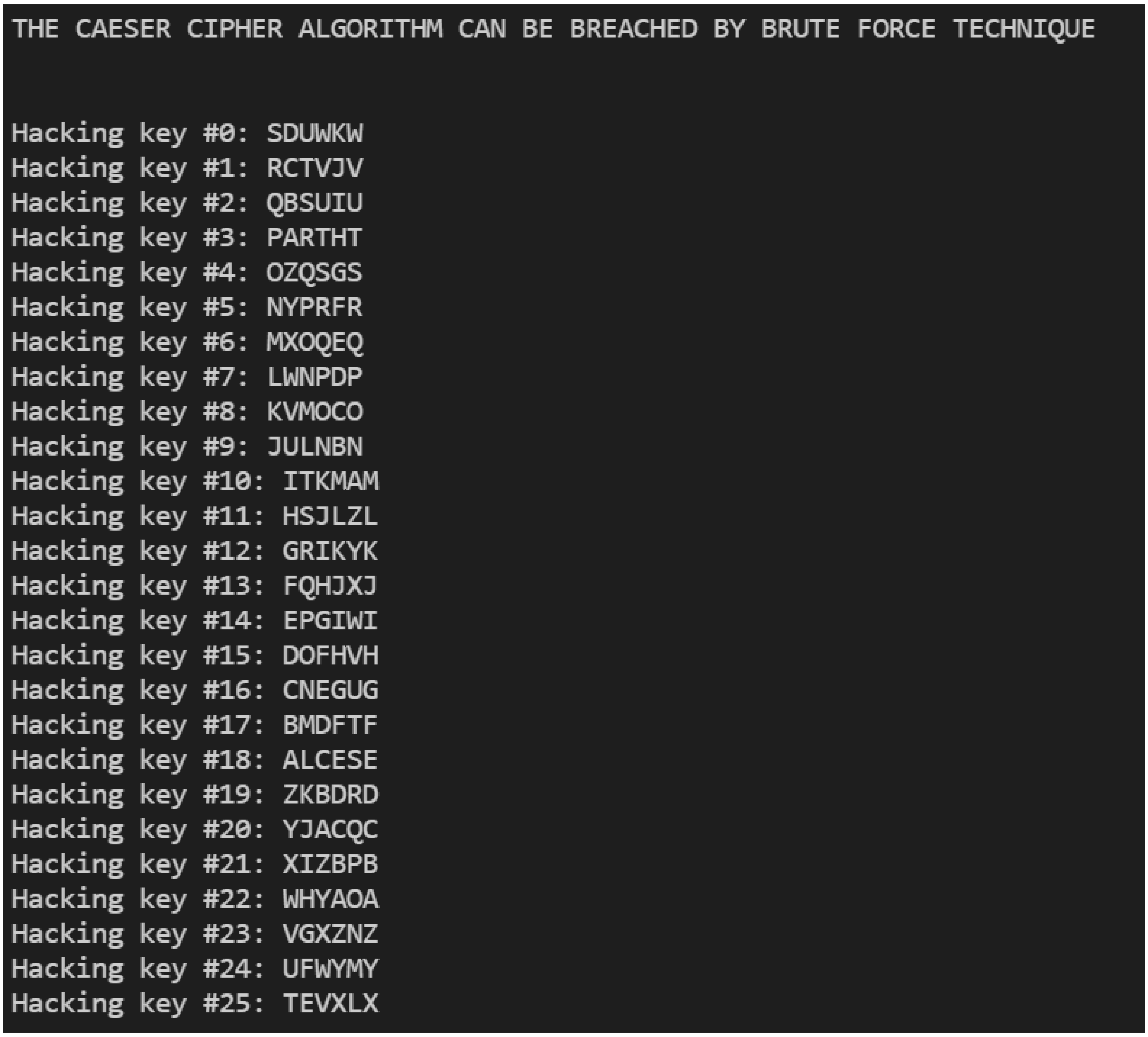
```
#PYTHON CODE FOR CAESER CIPHER

def encrypt(text,key):

    encrpytedString = ""


    #SEPERATING THE ALPHABETS FROM THE STRING

    for i in range(len(text)):

        char = text[i]


    #ENCRYPTING THE ALPHABETS WITH THE HELP OF KEY


        encrpytedString += chr((ord(char) + key-65) % 26 + 65)


    return encrpytedString


#check the above function

text = input("ENTER THE TEXT TO BE ENCRYPTED: ")

key = input("ENTER THE KEY : ")

print("PLAIN TEXT : " + text)

print("KEY: " + key)

encrpytedMessage=""

encryptedMessage=encrypt(text,int(key))
```

```
print("CIPHER TEXT: " +encryptedMessage)



print("\n\nTHE CAESER CIPHER ALGORITHM CAN BE BREACHED BY BRUTE FORCE TECHNIQUE\n\n")
message =encrypt(text,int(key)) #encrypted message
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

for key in range(len(LETTERS)):
    translated = ''
    for symbol in message:
        if symbol in LETTERS:
            num = LETTERS.find(symbol)
            num = num - key
            if num < 0:
                num = num + len(LETTERS)
            translated = translated + LETTERS[num]
        else:
            translated = translated + symbol
    print('Hacking key #%s: %s' % (key, translated))
print("\nPARTH PATEL\n19DCS098")
```

OUTPUT:



```
(base) C:\Users\Parth Patel>python -u
ENTER THE TEXT TO BE ENCRYPTED: PARTH
ENTER THE KEY : 3
PLAIN TEXT : PARTH
KEY: 3
CIPHER TEXT: SDUWKW
```



```
THE CAESER CIPHER ALGORITHM CAN BE BREACHED BY BRUTE FORCE TECHNIQUE


Hacking key #0: SDUWKW
Hacking key #1: RCTVJV
Hacking key #2: QBSUIU
Hacking key #3: PARTHT
Hacking key #4: OZQSGS
Hacking key #5: NYPRFR
Hacking key #6: MXOQEQ
Hacking key #7: LWNPDP
Hacking key #8: KVMOCO
Hacking key #9: JULNBN
Hacking key #10: ITKMAM
Hacking key #11: HSJLZL
Hacking key #12: GRIKYK
Hacking key #13: FQHJXJ
Hacking key #14: EPGIWI
Hacking key #15: DOFHVH
Hacking key #16: CNEGUG
Hacking key #17: BMDFTF
Hacking key #18: ALCESE
Hacking key #19: ZKBDRD
Hacking key #20: YJACQC
Hacking key #21: XIZBPB
Hacking key #22: WHYAOA
Hacking key #23: VGXZNZ
Hacking key #24: UFWYMY
Hacking key #25: TEVXLX
```

```
PARTH PATEL
19DCS098
```

CONCLUSION:

- By performing the above practical, I learned the basic concept of Caesar Cipher Algorithm and how