Vivekanand Education Society's Institute of Technology

Department of Computer Engineering

Subject: CSS Lab.

Class :- D12 Semester:- V Div :- A

Roll No: 14	Name: Soham Das		
Exp No: 01	Title: Product Cipher.		
DOP: 11/01/22		DOS:	**23/01/22**
GRADE:	LAB OUTCOMES: LO1	SIGNATURE:	

SOHAM. DAS

D12A

14

CSS Experiment No 1

Aim: Design & implement product cipher using substitution and transposition ciphers.

Theory :-

I) Substitution Cipher :-

In this cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key.

For eg :- with shift of 1, A would be B, so on

Mathematically :-

The encryption can be represented using modular arithmetic by first transforming the letter into numbers, according to scheme, A=0, B=1, Z=25. Encryption of a letter by a shift

$$En(x) = (x+n) \bmod 26$$

For decoding

$$Dn(x) = (x-n) \bmod 26$$

II) Transposition cipher :

It is a form of cipher which involves writing the plain text out in rows, and then reading ciphertext off in columns one by one.

Message is written in rows with fixed length and then read it column by column

Conclusion :-

In this experiment we learnt about substitute and transposition cipher how to encode it and decode it. This program was written in python and done successfully.

Code:

```
pltext = input("Enter the text: ")
key = int(input("Enter the key: "))
outputtext = []
for i in range(len(pltext)):
    if pltext[i].isupper():
        t = pltext[i].lower()
        if t.isalpha():
            outputtext.append(chr(((ord(t)-96 + key)%26)+96).upper())
        else:
            outputtext.append(t)
    else:
        if pltext[i].isalpha():
            outputtext.append(chr(((ord(pltext[i]) - 96 + key)%26) + 96))
        else:
            outputtext.append(pltext[i])

transtext = ''.join(outputtext)
col = len(transtext)//3

arr = []
c = 0
```

```
for j in range(col):
    text = ['0']*col
    for i in range(col):
        if c < len(transtext):
            text[i] = transtext[c]
            c += 1
    arr.append(text)

part = ''
for i in range(col):
    for j in range(col):
        if arr[j][i] != '0':
            part += arr[j][i]
print(f"Encoded product cipher string is {part}")



# decoding

part = ''
for i in range(col):
    for j in range(col):
        if arr[i][j] != '0':
            part += arr[i][j]

decode = []
```

```
for i in range(len(part)):
    if part[i].isupper():
        t = part[i].lower()
        if t.isalpha():
            decode.append(chr(((ord(t)-96 - key)%26)+96).upper())
        else:
            decode.append(t)
    else:
        if part[i].isalpha():
            decode.append(chr(((ord(part[i]) - 96 - key)%26) + 96))
        else:
            decode.append(part[i])
print(f"Decoded product cipher string is {''.join(decode)}")
```

Output:

```
C:\Windows\System32\cmd.exe

D:\sem6\CSS>python cipher.py
Enter the text: I am shubham
Enter the key: 4
Encoded product cipher string is M f wleleqyq
Decoded product cipher string is I am shubham

D:\sem6\CSS>
```