Name: Jigar Siddhpura **SAPID:** 60004200155

DIV: C/C2 **Branch:** Computer Engineering

IS - Experiment 2 - VIGERENE CIPHER

Jigar Siddhpura
60004200155
C22

Exp 2: Vigerene cipher

Aim: To study & implement vigerene cipher

Theory: It is a polyalphabetic cipher. Here, set of polyalphabetic substitutions refers consists of 26 caeser cipher with shift of 0 through 25. Thus first letter of key is added to first letters of plaintext & then mod 26, same goes for 2nd, 3rd & so on. For next letters, key letters are repeated. This process continues until all plaintext sequence is encrypted.

A general eqn: $C_i = (p_i + k_i \cdot \text{mod } m) \text{ mod } 26$

where C → cipher text, P → plaintext, K → key

To encrypte msg a key is needed as long as msg, so key is usually a repeating keyword. During decryption, subtraction is used.

$P_i = (C_i - k_i \cdot \text{mod } m) \text{ mod } 26$.

Eg: P = we are discovered save yourself
Key = deceptive
as len(key) < len(P.T.) so key becomes
key: deceptive deceptive deceptive

So it will follow as :

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
P. T.	22	4	0	17	4	3	8	18	2	19	21	4	17	4
C. T.	25	8	2	21	19	22	16	13	6	17	25	6	21	17

So if we convert no.s into alphabets,

C. T = Z I C V T W Q N G K Z G V T W A V Z H C Q Y G L M G J

Decryption :

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
C. T.	25	8	2	21	19	22	16	13	6	17	25	6	21	19
P. T.	22	4	0	17	4	3	8	18	2	14	21	4	17	4

Conclusion :

Thus, we implemented & studied vigenere cipher in python & also tried with some plaintext, key example.

CODE

```
plain_txt = input("Enter plaintext : ").upper()
key = input("Enter Key : ").upper()
padd_key = key

if len(plain_txt) == len(key):
    padd_key = key
else:
    for i in range(len(plain_txt) - len(key)):
        padd_key += key[i % len(key)]

print(f"\nPlain Text : {plain_txt}\nKey : {key}\nPadded Key : {padd_key}\n")
print('Encryption : ')

encrypted = ""
for i in range(len(plain_txt)):
    encrypted += chr(((ord(plain_txt[i]) + ord(padd_key[i])) % 26) + 65)

print(f"After encryption, cipher text : {encrypted}")

print('Decryption : ')

decrypted = ""
for i in range(len(plain_txt)):
    decrypted += chr(((ord(encrypted[i]) - ord(padd_key[i])) % 26) + 65)

print(f"After decryption, decrypted text : {decrypted}")
```

OUTPUT

```
PS D:\SEM-6\IS\EXPERIMENTS> python -u "d:\SEM-6\IS\EXPERIMENTS\vigerene.py"
Enter plaintext : ELEPHANT
Enter Key : ZEBRA

Plain Text : ELEPHANT
Key : ZEBRA
Padded Key : ZEBRAZEB

Encryption :
After encryption, cipher text : DPFGHZRU
Decryption :
After decryption, decrypted text : ELEPHANT
PS D:\SEM-6\IS\EXPERIMENTS>
```