Kartik Padave

A022

70362019039

Experiment 2

Aim

To implement Monoalphabetic Cipher.

Theory

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

Code

```
def decrypt(char):
    for i in cipher:
        if cipher[i] == char:
            return i

cipher = {
    'a': 'm',
   'b': 'n',
   'c': 'b',
   'd': 'v',
   'e': 'c',
   'f': 'x',
   'g': 'z',
   'h': 'a',
   'i': 's',
   'j': 'd',
   'k': 'f',
   'l': 'g',
   'm': 'h',
   'n': 'j',
   'o': 'k',
   'p': 'l',
   'q': 'p',
```

```
    'r': 'o',
    's': 'i',
    't': 'u',
    'u': 'y',
    'v': 't',
    'w': 'r',
    'x': 'e',
    'y': 'w',
    'z': 'q',
    ' ': ' '
}
plain_text = input("Enter plain text: ")
cipher_text = ""

for i in range(len(plain_text)):
    char = plain_text[i]
    if char.isupper():
        char = char.lower()
        cipher_word = cipher[char].upper()
    else:
        cipher_word = cipher[char]

    cipher_text += cipher_word

print("\nEncryption:\n")
print(f"Plain Text: {plain_text}")
print(f"Cipher text: {cipher_text}")

plain_text = ""

for i in range(len(cipher_text)):
    char = cipher_text[i]
    if char.isupper():
        char = char.lower()
        plain_word = decrypt(char).upper()
    else:
        plain_word = decrypt(char)

    plain_text += plain_word

print("\nDecryption:\n")
print(f"Cipher text: {cipher_text}")
print(f"Plain Text: {plain_text}")
```

Output

```
E:\Programs\College-Labs\CRYPTO-Lab>python Monoalphabetic.py
Enter plain text: my name is kartik

Encryption:

Plain Text: my name is kartik
Cipher text: hw jmhc si fmousf

Decryption:

Cipher text: hw jmhc si fmousf
Plain Text: my name is kartik
```

Conclusion

Hence, we were able to perform Monoalphabetic Cipher.