Assignment 2

Network Security (UCS727)

Name:	Sachleen Singh Chani
Roll No.:	101506143
Date:	April 2021

Q1. Write a program to implement a simple substitution cipher (Monoalphabetic cipher). Take the plain text as input from the user.

Answer:

Code –

```
# dictionary to store the letters
LETTERS = "ABCDEFGHIJKLMNOPQRSTUVWXYZ "

# their substitution mapping
key = "QWERTYUIOP ZXCVBNMASDFGHJKL"

def getPlain():
    print("\nEnter the plain text:")
    return input()

# encrypt function
def encText(text):

    cipher = ""
    # looping though plain text
    for char in text:
        # changing the lower case to upper case
        # keeping encrypted text in upper and plain/decrypted text in lower
        char = char.upper()
        # finding the character in the key string which maps to the plain text
        cipher += key[LETTERS.find(char)]

    return cipher


def decText(cipher):

    dcipher = ""
    # looping through the cipher text single char at a time
    for char in cipher:
        # finding the character in the Letters string which maps to the key string
        dcipher += LETTERS[key.find(char)]
    # changing the deciphered text back to lower case
    return dcipher.lower()

# user input plain text
plain = getPlain()

# calling the encryption function
cipher = encText(plain)
print("\nCipher text is:")
print(cipher)

# calling the decryption function
dcipher = decText(cipher)
print("\nThe original plain text is:")
print(dcipher)
```

Result –

The substitution mapping is done by using a key string which contains all the letters but in a random order. A space character has also been added to the string to encipher and decipher space character as well.

The screenshot in fig. 1 shows the result of the above code. The code goes through the plain text string character by character and simply substitute it with the corresponding position of the character in the ‘Letters’ string to the ‘key’ string

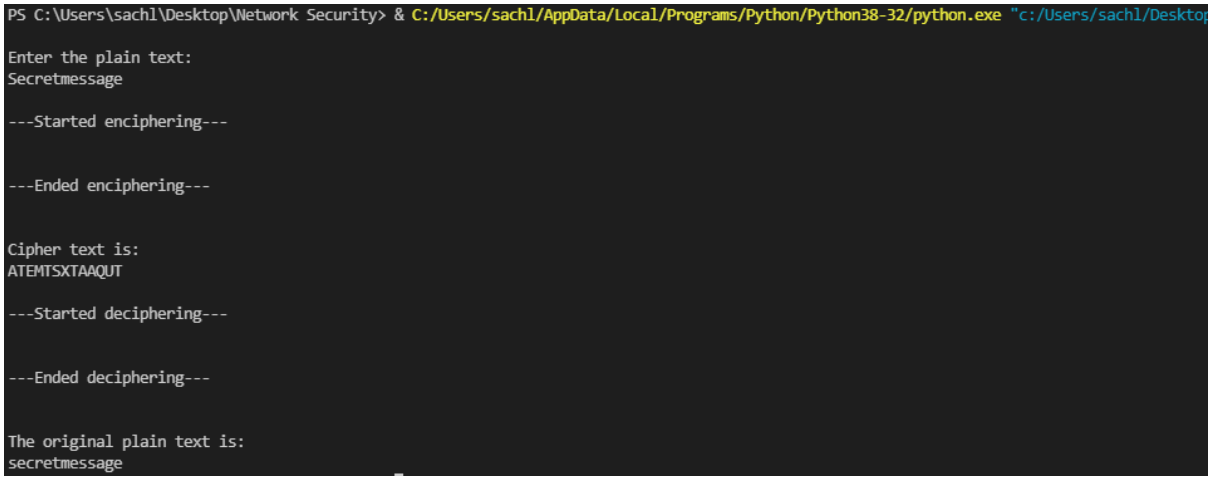

Figure 1 User input plain text

Q2. Write a program to implement the substitution cipher by reading the plain text from a file.

Answer:

Code –

```
# dictionary to store the letters
LETTERS = "ABCDEFGHIJKLMNOPQRSTUVWXYZ "

# their substitution mapping
key = "QWERTYUIOP ZXCVBNMASDFGHJKL"


# encrypt function
def encText(text):

    cipher = ""
    # looping though plain text
    for char in text:
        # changing the lower case to upper case
        # keeping encrypted text in upper and plain/decrypted text in lower
        char = char.upper()
        # finding the character in the key string which maps to the plain text
        cipher += key[LETTERS.find(char)]

    return cipher


def decText(cipher):

    dcipher = ""
    # looping through the cipher text single char at a time
    for char in cipher:
        # finding the character in the Letters string which maps to the key string
        dcipher += LETTERS[key.find(char)]
    # changing the deciphered text back to lower case
    return dcipher.lower()

# open a file in read mode with the plain text
while True:
# repeat until the try statement succeeds
    try:
```

```
        file = open("C:\\Users\\sachl\\Desktop\\plaintext_assignment2.ssc", "r")
        print("\nFile open successfully!")
        break
        # exit the loop
    except IOError:
        input("Could not open file!")
        # restart the loop

print("\nPlain text read from file:")
# reading the whole file
plain = file.read()
print(plain)

# calling encryption function
cipher = encText(plain)
print("\nCipher text is:")
print(cipher)

# calling the decryption function
dcipher = decText(cipher)
print("\nThe original plain text is:")
print(dcipher,"\n")

# closing the file
file.close()
```

Result –

The plain text is read from the file using the read() function.

The text file ‘plaintext_assignment2_q2.ssc’ contains a single line text, ‘Monoalphabetic Cipher’. A check is performed to make sure the file is opened successfully.

The result of the above code could be seen in the screenshot in fig. 2.

```
PS C:\Users\sachl\Desktop\Network Security> & C:/Users/sachl/AppData/Local/Programs/Python/Python38-32/python.exe "c:/Users/sachl/Desktop/Network Security/Assig

File open successfully!

Plain text read from file:
EncodeTheText

---Started enciphering---


---Ended enciphering---


Cipher text is:
TCEVRTSITSTHS

---Started deciphering---


---Ended deciphering---


The original plain text is:
encodethetext
```

Figure 2 Plain text read from a file