Assignment 3

Network Security (UCS727)

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

Q1. Write a program to implement the autokey cipher taking user input for the plain text and key.

Answer:

Code –

```
# autokey cipher
#dictionary to store alphabets
dic = "abcdefghijklmnopqrstuvwxyz "

#modulo value to keep the values in the range of the alphabets
MAX_MOD = len(dic)

#function to get the input key
def getKey():
    print("\nEnter the key:")
    return input().lower()

#fucntion to get the input plain text
def getPlain():
    print("\nEnter the plain text:")
    #return after changing the string to lower case
    return input().lower()

#enciphering function
def enCode(plain, key):
    print("\n---Started enciphering---")

    cipher = ""

    for i in range(len(plain)):

        #append the plain kext after the key and add to the plain text
        if (i < len(key)):
            cipher += dic[( dic.find(plain[i]) + dic.find(key[i]) ) %
MAX_MOD]
        else:
            #plain text appended
            cipher += dic[( dic.find(plain[i]) + dic.find(plain[i-
len(key)]) ) % MAX_MOD]
    print("\n---Ended eniphering---\n")
    return cipher.upper()

#decipher fucntion
def deCode(cipher, key):
    print("\n---Started deciphering---\n")

    cipher = cipher.lower()
    decipher = ""

    for i in range(len(cipher)):

        #appends the cipher text to the key and subtracts the value
        #modulo keeps in the range of the dictionary
        if(i < len(key)):
            decipher += dic[( dic.find(cipher[i]) - dic.find(key[i]) ) %
MAX_MOD]
        else:
            decipher += dic[( dic.find(cipher[i]) - dic.find(decipher[i-
len(key)]) ) % MAX_MOD]
```

```
    print("\n---Ended deciphering---\n")
    return decipher

#gets user inputs for plain text and key
plain   = getPlain()
key     = getKey()

cipher      = enCode(plain, key)
print("The cipher text is:")
print(cipher)

decipher    = deCode(cipher, key)
print("The deciphered/plain text is:")
print(decipher,"\n")
```

Result –

```
PS C:\Users\sachl\Desktop\Network Security> & C:/Users/sachl/AppData/Local/Programs/Python/Python38-32/python.exe "c:/Users/sachl/Desk
top/Network Security/Assignemnt 3 (Autokey Cipher)/autokey.py"

Enter the plain text:
encode the message

Enter the key:
secret

---Started enciphering---

---Ended eniphering---

The cipher text is:
WREEHXDFJSCQDKZEFQ

---Started deciphering---


---Ended deciphering---

The deciphered/plain text is:
encode the message
```

Figure 1 Result for autokey cipher