**Name: Madhuri Ramakrishnan**

**PRN: 119A3032**

**TE-IT (E2)**

**EXPERIMENT-02**

**Aim:** *-* Design and Implement a product cipher using Substitution ciphers.

**Resources Required: -**

1. VS code IDE
2. Programming Language - Python

**Theory:**

1. Substitution Cipher:

* Hiding some data is known as encryption. When plain text is encrypted, it becomes unreadable and is known as cipher text.
* A **substitution cipher** is a method of [encrypting](https://en.wikipedia.org/wiki/Encrypting) in which units of [plaintext](https://en.wikipedia.org/wiki/Plaintext) are replaced with the [cipher text](https://en.wikipedia.org/wiki/Ciphertext), in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.
* The receiver deciphers the text by performing the inverse substitution process to extract the original message.

2. Transposition cipher:

* In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged.

3. Product Cipher:

* A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to [cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis).
* The product cipher combines a sequence of simple transformations such as [substitution](https://en.wikipedia.org/wiki/Substitution_cipher) (S-box), [permutation](https://en.wikipedia.org/wiki/Transposition_cipher) (P-box), and [modular arithmetic](https://en.wikipedia.org/wiki/Modular_arithmetic).

**Procedure:**

1. Mono alphabetic substitution (Ceaser cipher)

* Encryption :

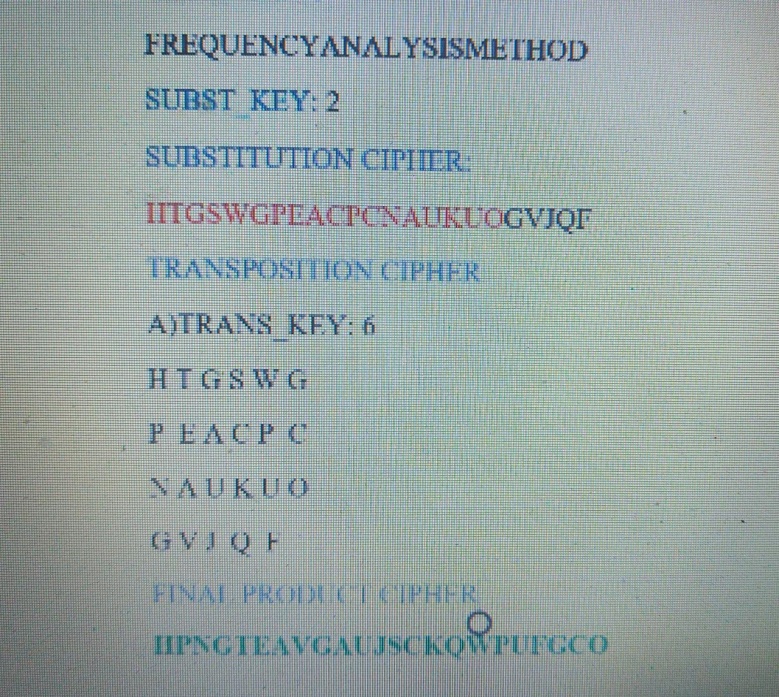
1. First we create the cipher text of the plain text by shifting the alphabets of the plain text to the left by the no. Of places given by the key(user input)
2. E.g. we must create a cipher text of "SHOBHANA". Thus a shift of 3 moves the plain text to “VKREKDQD".

2. Transposition Cipher:

* In a transposition cipher the order of alphabets is text to obtain the cipher text.
* The letters of the obtained ceaser cipher text are written alternating between rows. The columns are decided by the key provided by the user. Hence a matrix is formed.

3. Final Product Cipher:

* The final product cipher is obtained by transposing the above matrix. And reading it in a columnar format.

. 

**Code:**

# product cipher

def substitution(text,key):

  result = ""

  for i in range (len(text)):

    char = text[i]

    if (char.isupper()):

      result += chr((ord(char) + key-65) % 26 + 65)

    elif (char.islower()):

      result += chr((ord(char) + key - 97) % 26 + 97)

    else:

      result += "\*"

  return result

def encryptMessage(key, message):

   ciphertext = [''] \* key

   for col in range(key):

      position = col

      while position < len(message):

         ciphertext[col] += message[position]

         position += key

   return ''.join(ciphertext)

text = input("Enter a string to be encrypted: ")

key = int(input("Enter Substitution cipher key: "))

print ("Encrypted text:",substitution(text,key))

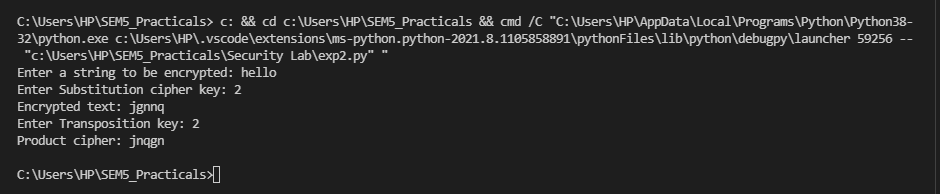
sub = substitution(text,key)

key = int(input("Enter Transposition key: "))

product = encryptMessage(key,sub)

print("Product cipher:", product)

**Results:**



**Conclusion:**

In this experiment we have learned about:

* Implementation of Substitution ceaser cipher with a shift key of 2
* Implementation of Transposition cipher with a key of 6
* Obtained a Final Product Cipher (Substitution + Transposition in this case) and verified the results.

Hence we have successfully completed the implementation of product ciphers using substitution ciphersand Transposition cipher.

Bottom of Form