Question no. 1

As we studied in class, a substitution cipher uses a fixed system to replace the element.

Let us use the following example:

```
abcdefghijklmnopqrstuvwxyz
      maps to
efghijklmnopqrstuvwxyzabcd
```

means the Key is efghijklmnopqrstuvwxyzabcd.

our input is a plaintext: ilovesfbu

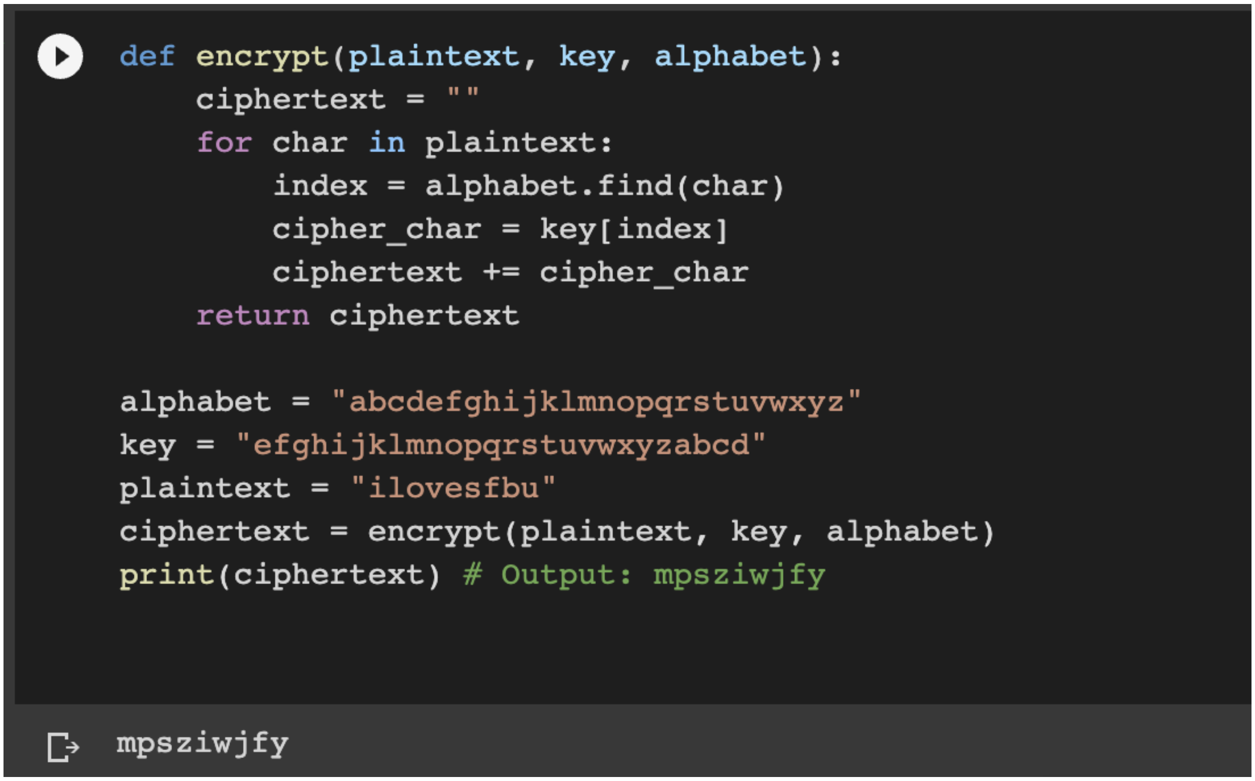
Please use Python language to generate a cipher text (output). You do need to decrypt the cipher text to check whether you can get the original plain text as well

```
alphabet = "abcdefghijklmnopqrstuvwxyz"
key = "efghijklmnopqrstuvwxyzabcd"
plaintext = "ilovesfbu"
output = "mpsziwjfy"
```

Note: You may use the .join() or/and .find() function in the program.

- ⇨ For encrypt: The function takes three arguments: plaintext: the text to be encrypted.

key: the substitution cipher key.
alphabet: the alphabet used in the substitution.
The function works as follows:It initializes an empty string ‘ciphertext’ to store the encrypted message. And then, for each character in the ‘plaintext’, the function finds its index in the alphabet using the .find() method. The function then looks up the corresponding character in the ‘key’ using the same index. This is the encrypted character for the original plaintext character. Then, the ‘encrypted’ character is added to the ciphertext string. After that, the function repeats the process for each character in the plaintext. Finally, the function returns the ‘ciphertext.’ The output is given.



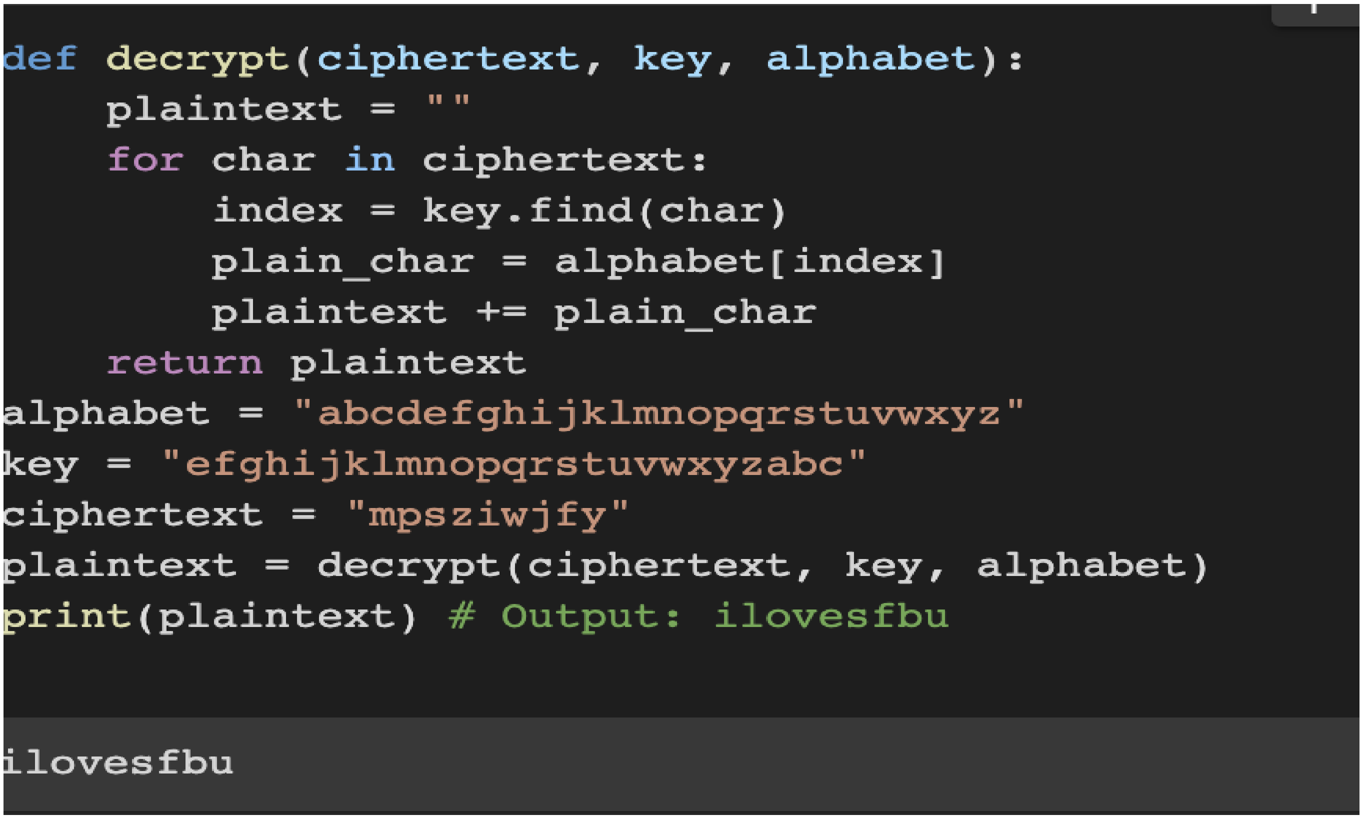
```python
def encrypt(plaintext, key, alphabet):
    ciphertext = ""
    for char in plaintext:
        index = alphabet.find(char)
        cipher_char = key[index]
        ciphertext += cipher_char
    return ciphertext

alphabet = "abcdefghijklmnopqrstuvwxyz"
key = "efghijklmnopqrstuvwxyzabcd"
plaintext = "ilovesfbu"
ciphertext = encrypt(plaintext, key, alphabet)
print(ciphertext) # Output: mpsziwjfy
```

```
mpsziwjfy
```

⇨ For decrypt: The function decrypt takes in 3 arguments - ciphertext, key, and alphabet. The ‘ciphertext’ is the encrypted message to be ‘decrypted’, the ‘key’ is the shared secret used for encryption, and the ‘alphabet’ is the mapping of characters to their corresponding indices.

The function creates an empty string ‘plaintext’ and initializes it as an empty string. It then iterates over each character in the ciphertext. For each character, it finds the index of that character in the key. This index is used to find the corresponding character in the alphabet, which is then added to the plaintext string. After iterating over all the characters in ciphertext, the function returns the decrypted message stored in ‘plaintext’.



```
def decrypt(ciphertext, key, alphabet):
    plaintext = ""
    for char in ciphertext:
        index = key.find(char)
        plain_char = alphabet[index]
        plaintext += plain_char
    return plaintext
alphabet = "abcdefghijklmnopqrstuvwxyz"
key = "efghijklmnopqrstuvwxyzabc"
ciphertext = "mpsziwjfy"
plaintext = decrypt(ciphertext, key, alphabet)
print(plaintext) # Output: ilovesfbu
```

```
ilovesfbu
```