Name: Nikita Shivchandra Khot

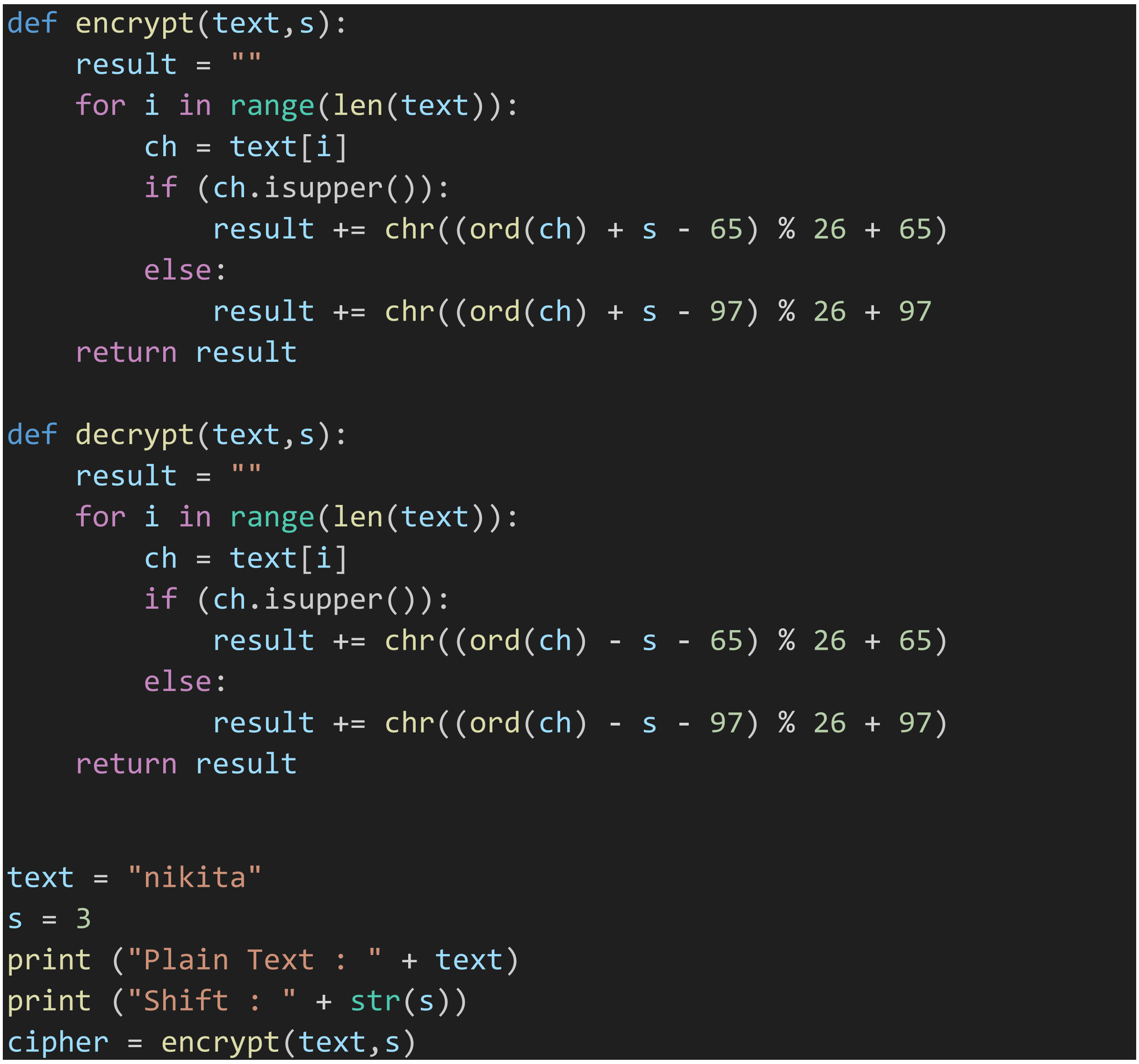
PRN No: 2020BTECS00041

Assignment No 1

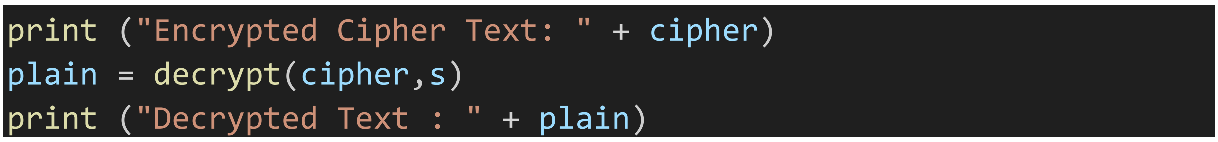
Aim: To Study and implementation of Caesar Cipher Technique

Theory:
Caesar cipher works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.
It is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Code:

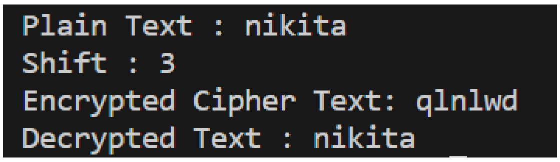


```
def encrypt(text,s):
    result = ""
    for i in range(len(text)):
        ch = text[i]
        if (ch.isupper()):
            result += chr((ord(ch) + s - 65) % 26 + 65)
        else:
            result += chr((ord(ch) + s - 97) % 26 + 97
    return result

def decrypt(text,s):
    result = ""
    for i in range(len(text)):
        ch = text[i]
        if (ch.isupper()):
            result += chr((ord(ch) - s - 65) % 26 + 65)
        else:
            result += chr((ord(ch) - s - 97) % 26 + 97)
    return result


text = "nikita"
s = 3
print ("Plain Text : " + text)
print ("Shift : " + str(s))
cipher = encrypt(text,s)
```



```
print ("Encrypted Cipher Text: " + cipher)
plain = decrypt(cipher,s)
print ("Decrypted Text : " + plain)
```

Output:



```
Plain Text : nikita
Shift : 3
Encrypted Cipher Text: qlnlwd
Decrypted Text : nikita
```

Caesar Cipher:

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Example:

Caesar cipher to encrypt the message “nikita” with a shift of 3:
Write down the plaintext message: nikita
Choose a shift value. In this case, we will use a shift of 3.
Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

n	i	k	i	t	a
q	l	n	l	w	d

The encrypted message is now “qlnlwd”.

To decrypt the message, we simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “qlnlwd” back by 3 positions to get the original message, “nikita”.

Limitations:

It is not secure against modern decryption methods.
Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
Small number of possible keys means that an attacker can easily try all possible keys until correct one is found, making it vulnerable to a brute force attack.
It is not suitable for long text encryption as it would be easy to crack.
It is not suitable for secure communication as it is easily broken.
Does not provide confidentiality, integrity, and authenticity in a message.