LAB MID

SUBMITTED BY:

Aliza Faisal SP24-BSE-048

SUBMITTED TO: MA’AM AMBREEN GUL

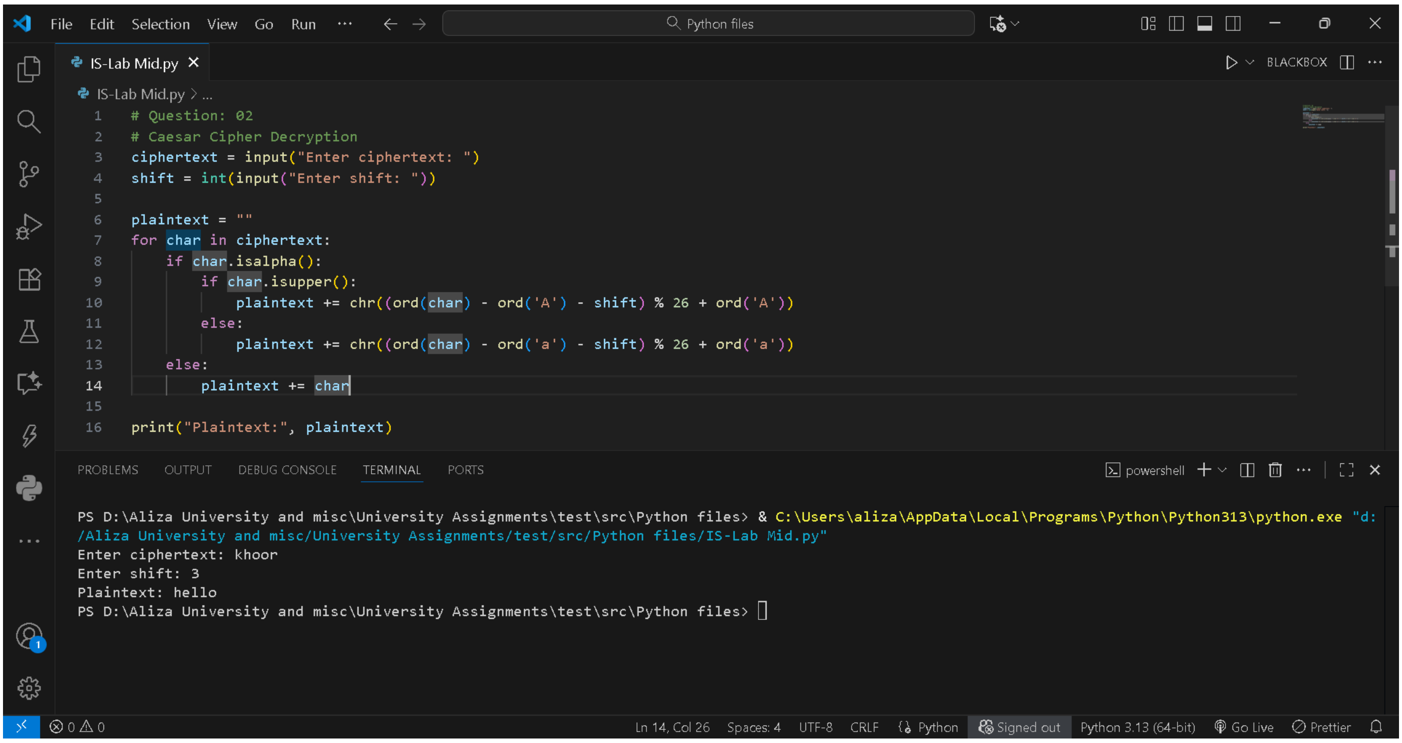
DATE: 21ST OCTOBER, 2025

COURSE: Information Security

Q2. Caesar Cipher (Decryption)

Write a Python program to decrypt a message that was encrypted using the Caesar Cipher.

```
ciphertext = input("Enter ciphertext: ")

shift = int(input("Enter shift: "))

plaintext = ""

for char in ciphertext:

    if char.isalpha():

        if char.isupper():

            plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        else:

            plaintext += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))

    else:

        plaintext += char

print("Plaintext:", plaintext)
```



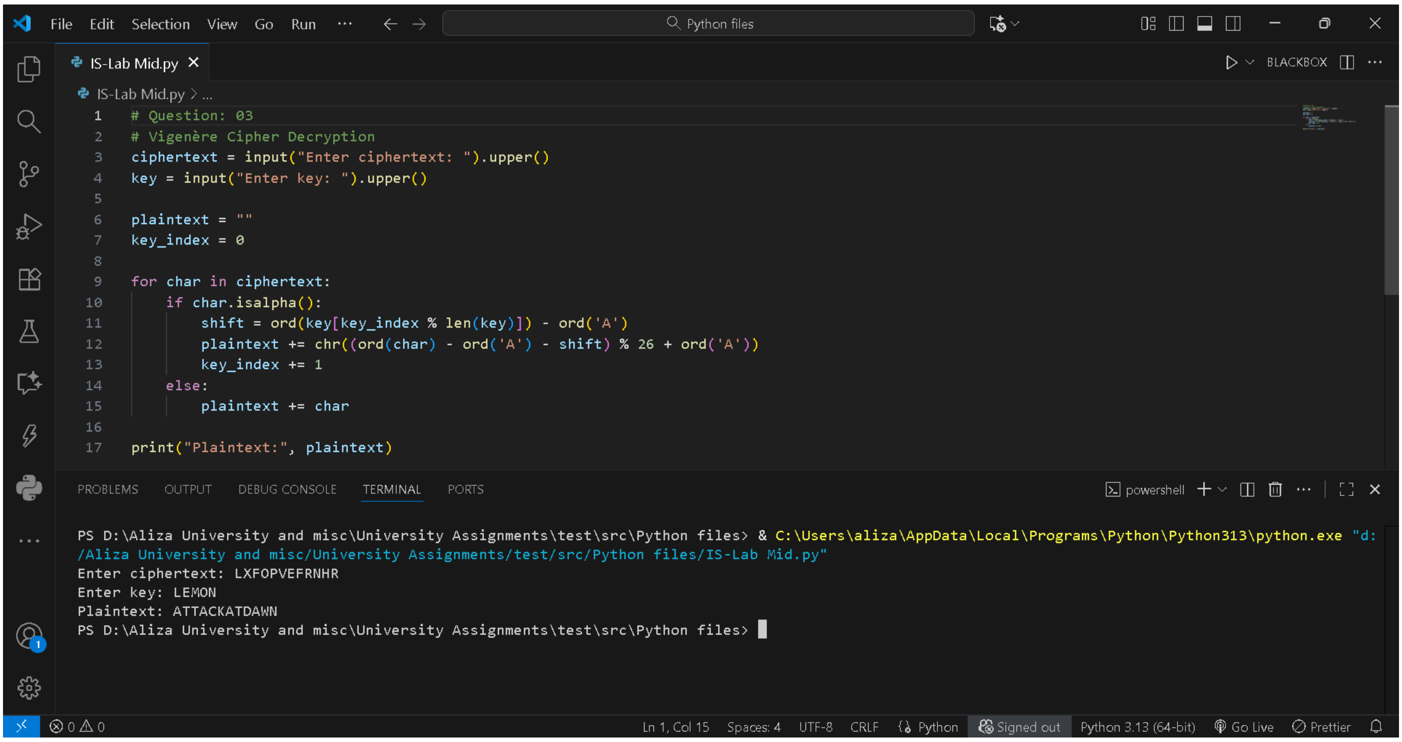
```
# Question: 02
# Caesar Cipher Decryption
ciphertext = input("Enter ciphertext: ")
shift = int(input("Enter shift: "))

plaintext = ""
for char in ciphertext:
    if char.isalpha():
        if char.isupper():
            plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))
        else:
            plaintext += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))
    else:
        plaintext += char

print("Plaintext:", plaintext)
```

```
PS D:\Aliza University and misc\University Assignments\test\src\Python files> & C:\Users\aliza\AppData\Local\Programs\Python\Python313\python.exe "d:
/Aliza University and misc/University Assignments/test/src/Python files/IS-Lab Mid.py"
Enter ciphertext: khoor
Enter shift: 3
Plaintext: hello
PS D:\Aliza University and misc\University Assignments\test\src\Python files> 
```

Q3. **Vigenère Cipher (Decryption Only)**

Write a Python program to decrypt a ciphertext using the Vigenère Cipher. Ask the user for ciphertext and key, and display the decrypted plaintext.

```
ciphertext = input("Enter ciphertext: ").upper()

key = input("Enter key: ").upper()

plaintext = ""

key_index = 0

for char in ciphertext:

    if char.isalpha():

        shift = ord(key[key_index % len(key)]) - ord('A')

        plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        key_index += 1

    else:

        plaintext += char

print("Plaintext:", plaintext)
```



File Edit Selection View Go Run ···
Python files
IS-Lab Mid.py
BLACKBOX
IS-Lab Mid.py > ...
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
powershell
Ln 1, Col 15 Spaces: 4 UTF-8 CRLF Python Signed out Python 3.13 (64-bit) Go Live Prettier

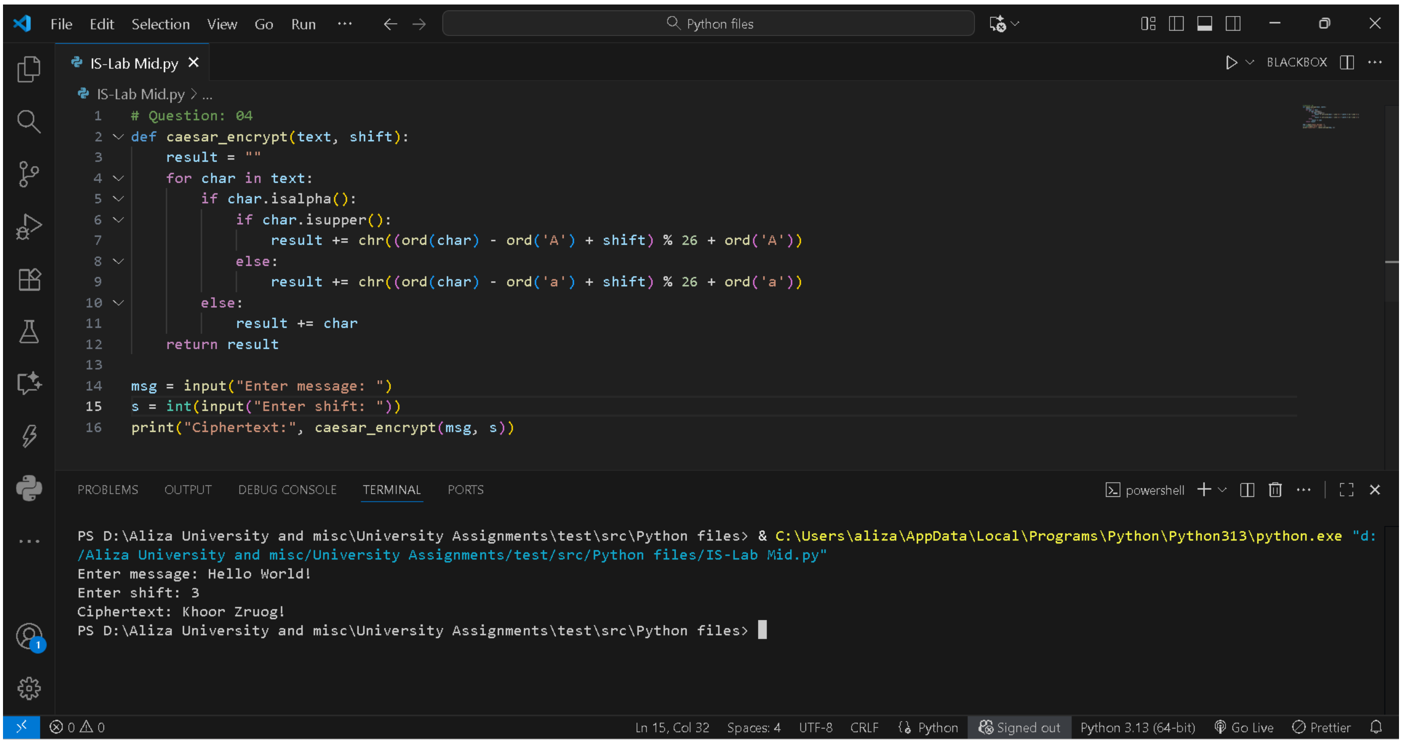
```python
# Question: 03
# Vigenère Cipher Decryption
ciphertext = input("Enter ciphertext: ").upper()
key = input("Enter key: ").upper()

plaintext = ""
key_index = 0

for char in ciphertext:
    if char.isalpha():
        shift = ord(key[key_index % len(key)]) - ord('A')
        plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))
        key_index += 1
    else:
        plaintext += char

print("Plaintext:", plaintext)
```

```
PS D:\Aliza University and misc\University Assignments\test\src\Python files> & C:\Users\aliza\AppData\Local\Programs\Python\Python313\python.exe "d:/Aliza University and misc/University Assignments/test/src/Python files/IS-Lab Mid.py"
Enter ciphertext: LXFOPVEFRNHR
Enter key: LEMON
Plaintext: ATTACKATDAWN
PS D:\Aliza University and misc\University Assignments\test\src\Python files>
```

Q4. **Debugging Task (Caesar Cipher Code)**

The following program is intended to encrypt text using the Caesar Cipher, but it contains an error. Fix the mistake so that it runs correctly and gives the right output.

```
def caesar_encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            if char.isupper():
                result += chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
            else:
                result += chr((ord(char) - ord('a') + shift) % 26 + ord('a'))
        else:
            result += char
    return result
msg = input("Enter message: ")
s = int(input("Enter shift: "))
print("Ciphertext:", caesar_encrypt(msg, s))
```



```python
# Question: 04
def caesar_encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            if char.isupper():
                result += chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
            else:
                result += chr((ord(char) - ord('a') + shift) % 26 + ord('a'))
        else:
            result += char
    return result

msg = input("Enter message: ")
s = int(input("Enter shift: "))
print("Ciphertext:", caesar_encrypt(msg, s))
```

```
PS D:\Aliza University and misc\University Assignments\test\src\Python files> & C:\Users\aliza\AppData\Local\Programs\Python\Python313\python.exe "d:/Aliza University and misc/University Assignments/test/src/Python files/IS-Lab Mid.py"
Enter message: Hello World!
Enter shift: 3
Ciphertext: Khoor Zruog!
PS D:\Aliza University and misc\University Assignments\test\src\Python files> 
```

Q4. Conceptual: DES and AES

a) Write one similarity between DES and AES.

Both are symmetric key block ciphers that use the same key for both encryption and decryption.

b) What does CBC mode stand for in block ciphers?

Cipher Block Chaining mode - where each block is XORed with the previous ciphertext block before encryption.

c) Why is AES faster than DES?

AES uses simpler mathematical operations and can be efficiently implemented in both software and hardware.