



LAB MID

SUBMITTED BY:

Aliza Faisal

SP24-BSE-048

**SUBMITTED TO: MA'AM AMBREEN
GUL**

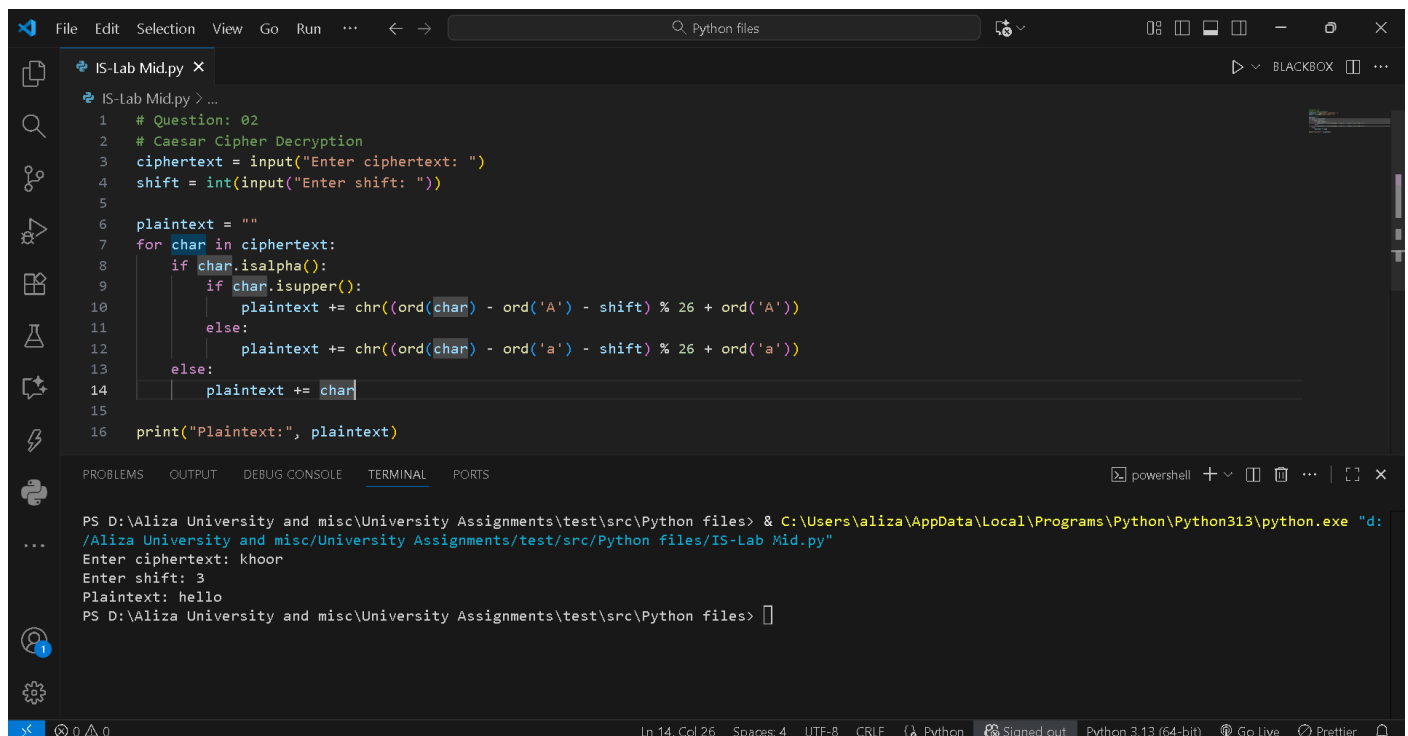
DATE: 21ST OCTOBER, 2025

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)
```



The screenshot shows a Visual Studio Code editor window with a Python file named 'IS-Lab Mid.py'. The code implements a Caesar Cipher decryption program. The terminal output shows the program being executed, with the ciphertext 'khoor' and shift '3' resulting in the plaintext 'hello'.

```
1 # Question: 02
2 # Caesar Cipher Decryption
3 ciphertext = input("Enter ciphertext: ")
4 shift = int(input("Enter shift: "))
5
6 plaintext = ""
7 for char in ciphertext:
8     if char.isalpha():
9         if char.isupper():
10            plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))
11        else:
12            plaintext += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))
13    else:
14        plaintext += char
15
16 print("Plaintext:", plaintext)
```

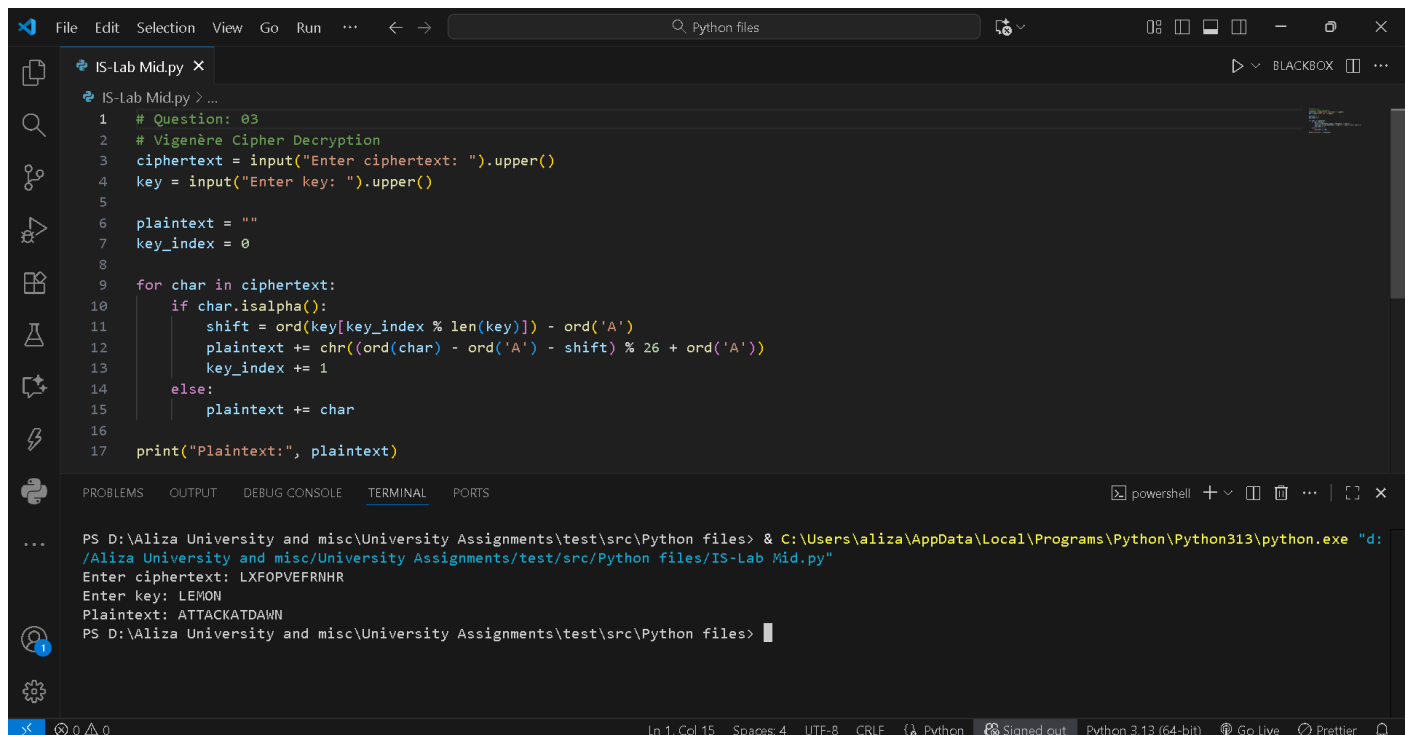
Terminal Output:

```
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)
```



The screenshot shows a Visual Studio Code editor window with a Python file named 'IS-Lab Mid.py'. The code implements a Vigenère Cipher decryption algorithm. Below the editor, a terminal window shows the execution of the script. The user enters the ciphertext 'LXFOPVEFRNHR' and the key 'LEMON'. The program outputs the decrypted plaintext 'ATTACKATDAWN'.

```
1 # Question: 03
2 # Vigenère Cipher Decryption
3 ciphertext = input("Enter ciphertext: ").upper()
4 key = input("Enter key: ").upper()
5
6 plaintext = ""
7 key_index = 0
8
9 for char in ciphertext:
10     if char.isalpha():
11         shift = ord(key[key_index % len(key)]) - ord('A')
12         plaintext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))
13         key_index += 1
14     else:
15         plaintext += char
16
17 print("Plaintext:", plaintext)
```

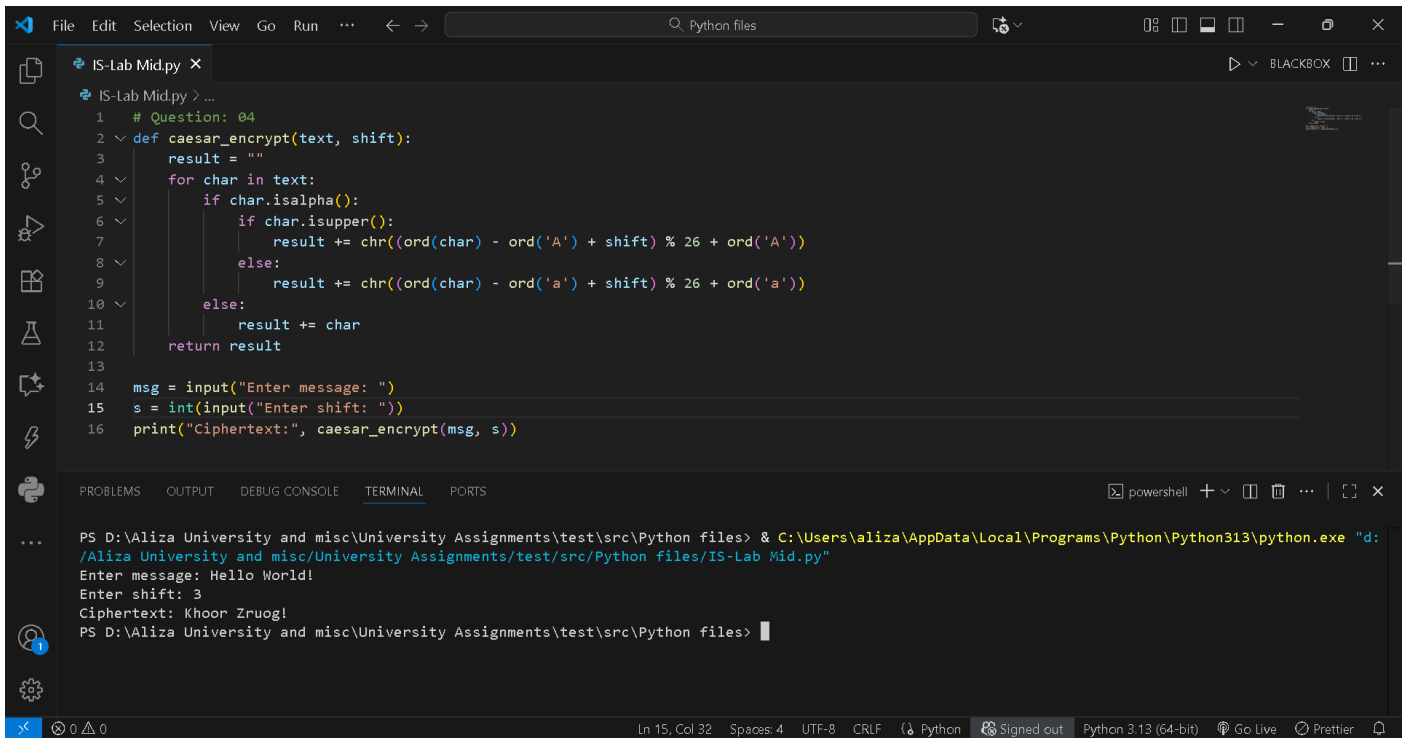
Terminal Output:

```
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))
```



The screenshot shows a Visual Studio Code editor with a Python file named 'IS-Lab Mid.py'. The code implements a Caesar cipher encryption function. The terminal window at the bottom shows the command to run the script, followed by user input for a message and a shift value, resulting in the encrypted output.

```
1 # Question: Q4
2 def caesar_encrypt(text, shift):
3     result = ""
4     for char in text:
5         if char.isalpha():
6             if char.isupper():
7                 result += chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
8             else:
9                 result += chr((ord(char) - ord('a') + shift) % 26 + ord('a'))
10        else:
11            result += char
12    return result
13
14 msg = input("Enter message: ")
15 s = int(input("Enter shift: "))
16 print("Ciphertext:", caesar_encrypt(msg, s))
```

Terminal Output:

```
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.