**Comsats University Islamabad**

**(Attock Campus)**



**Department of Computer Science**

|  |  |
| --- | --- |
| NAME | WALID SHAHZEB |
| REG NO | SP24-BSE-032 |
| SUBMITTED TO | MS AMBREEN GUL |
| LAB | MID TERM |
| COURSE | INFORMATION SECURITY |
| DATE | 20-OCT-2025 |

**Question 1**

**Caesar Cipher**

Write a Python program that encrypts a message using the Caesar Cipher with a user-given shift value.  
  
Example:  
Enter message: hello  
Enter shift: 3  
Ciphertext: khoor  
  
Hint: Use ord() and chr() for shifting letters.

CODE:

message = input("Enter message: ")

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

ciphertext = ""

for char in message:

if char.isalpha():

base = ord('a') if char.islower() else ord('A')

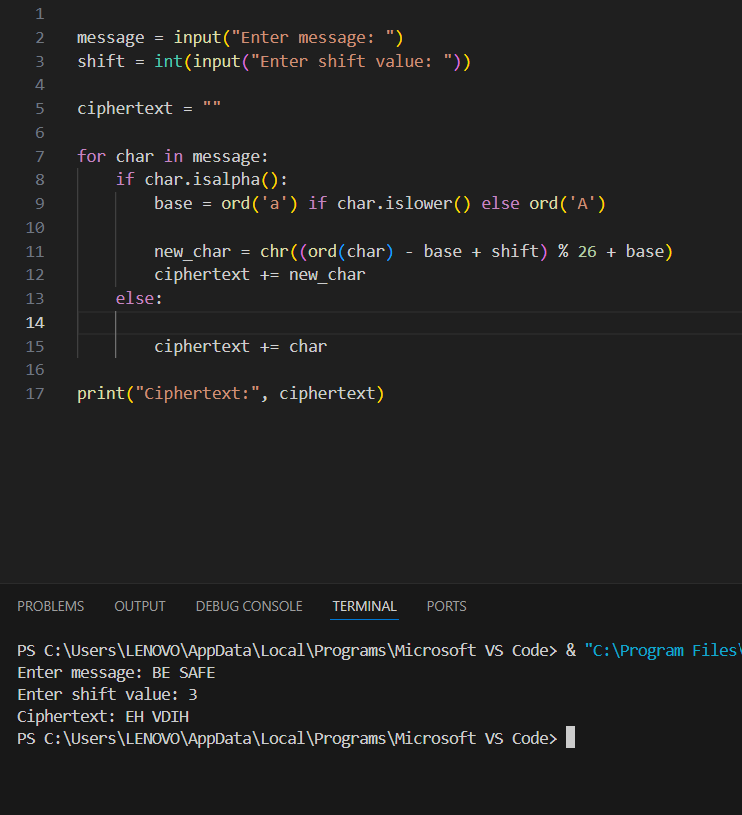
new\_char = chr((ord(char) - base + shift) % 26 + base)

ciphertext += new\_char

else:

ciphertext += char

print("Ciphertext:", ciphertext)



**Question 2**

**Vigenère Cipher (Encryption Only)**

Write a Python program to encrypt a plaintext message using the Vigenère Cipher. Ask the user for plaintext and keyword. Display the ciphertext only.  
  
Example:  
Enter plaintext: ATTACKATDAWN  
Enter key: LEMON  
Ciphertext: LXFOPVEFRNHR

CODE:

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

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

ciphertext = ""

key\_index = 0

for char in plaintext:

    if char.isalpha():

        p = ord(char) - ord('A')

        k = ord(key[key\_index % len(key)]) - ord('A')

        c = (p + k) % 26

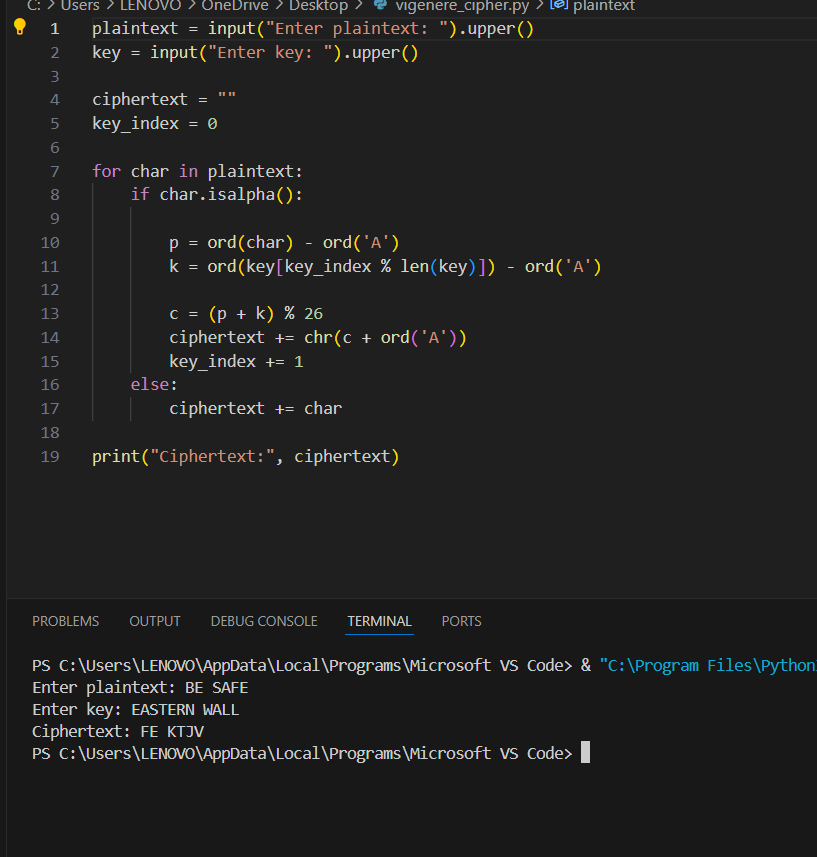
        ciphertext += chr(c + ord('A'))

        key\_index += 1

    else:

        ciphertext += char

print("Ciphertext:", ciphertext)



**Question: 4**

**Caesar Cipher Decryption (Simple Brute Force)**

You are given a Caesar Cipher ciphertext. Write a Python program to try all 25 possible shift values and print each possible plaintext.  
  
Example Input:  
Ciphertext: khoor  
  
Expected Output:  
Shift 1: jgnnq  
Shift 2: ifmmp  
Shift 3: hello <-- correct plaintext

**CODE:**

ciphertext = input("Enter ciphertext: ")

for shift in range(1, 26):

plaintext = ""

for char in ciphertext:

if char.isalpha():

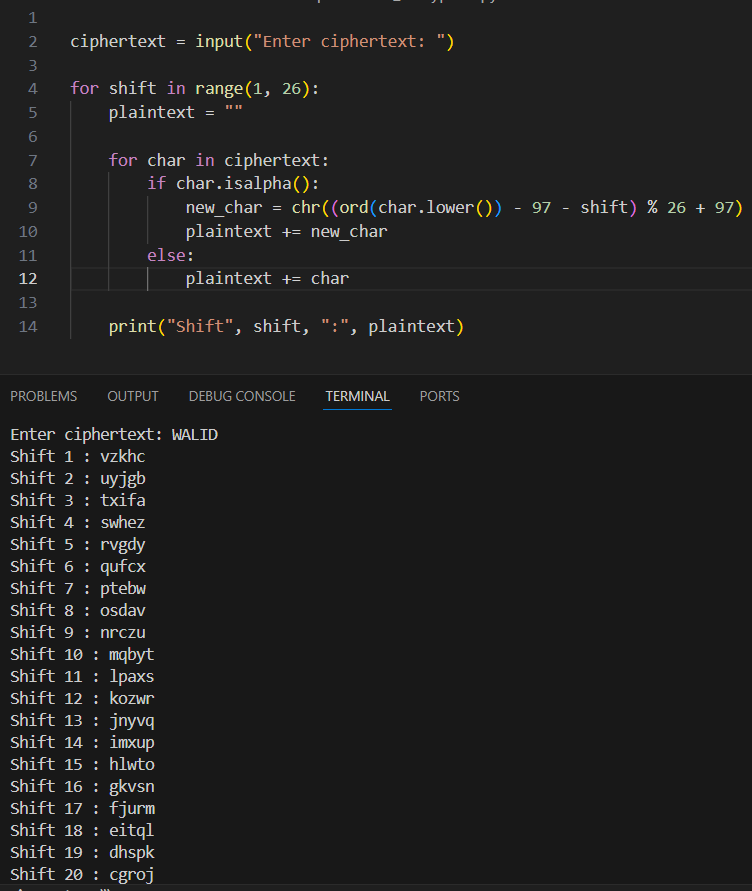
new\_char = chr((ord(char.lower()) - 97 - shift) % 26 + 97)

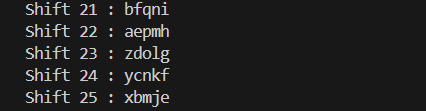
plaintext += new\_char

else:

plaintext += char

print("Shift", shift, ":", plaintext)

**



**Question 5**

**DES and AES**

Answer briefly:  
  
a) One difference between DES and AES.   
b) AES block size and one key size.   
c) One reason why AES is more secure than DES.

ANSWER:

**One difference between DES and AES**

DES (Data Encryption Standard) is an older encryption algorithm that uses a 56‑bitkey and a Feistel structure, making it less secure by modern standards.  
AES (Advanced Encryption Standard) is a newer algorithm that uses 128‑, 192‑, or256‑bit keys and a substitution–permutation network, providingfaster and strongerencryption.

**AES block size and one key size**

AES operates on fixed data blocks of 128 bits.  
It supports multiple key sizes: 128, 192, or 256 bits.  
For example, AES‑128 uses a 128‑bit block size with a 128‑bit key to transform plaintext into ciphertext securely.

**One reason why AES is more secure than DES**

AES is more secure because it uses longer key lengths and more complex encryption rounds, which resist brute‑force and cryptanalytic attacks.  
In contrast, DES’s 56‑bit key can be broken quickly with modern computing power.