Task 01

Implement Caesar Cipher

Create a Python program that can encrypt and decrypt text using the Caesar Cipher algorithm. Allow users to input a message and a shift value to perform encryption and decryption.

**Introduction: -**

**Encryption and Decryption are fundamental processes in cryptography used to secure information and protect it from unauthorized access.**

* **Encryption** is the process of converting readable data (plaintext) into an unreadable format (ciphertext) using a mathematical algorithm and a key. This transformation ensures that only authorized individuals with the correct key can access the original data.
  + **Purpose**: To ensure the confidentiality of information.
* **Decryption** is the reverse process, where the ciphertext is transformed back into its original readable form (plaintext) using the appropriate key.
  + **Purpose**: To allow authorized users to retrieve and understand the original information.

One of the simplest and earliest methods of encryption is the **Caesar Cipher**, which demonstrates the basic principles of cryptography: **substitution** and **key-based transformation**.

### ****Working of the Caesar Cipher:****

Each letter in the plaintext is shifted by a fixed number of positions in the alphabet, determined by a numerical key. If the shift moves past the end of the alphabet, it wraps around to the beginning.

#### ****Example – Caesar Cipher (Encryption/Decryption):****

Type 'e' to encrypt or 'd' to decrypt: d

Enter your message: hello chai

Enter the shift value (integer): 123

Decrypted Message: olssv johp

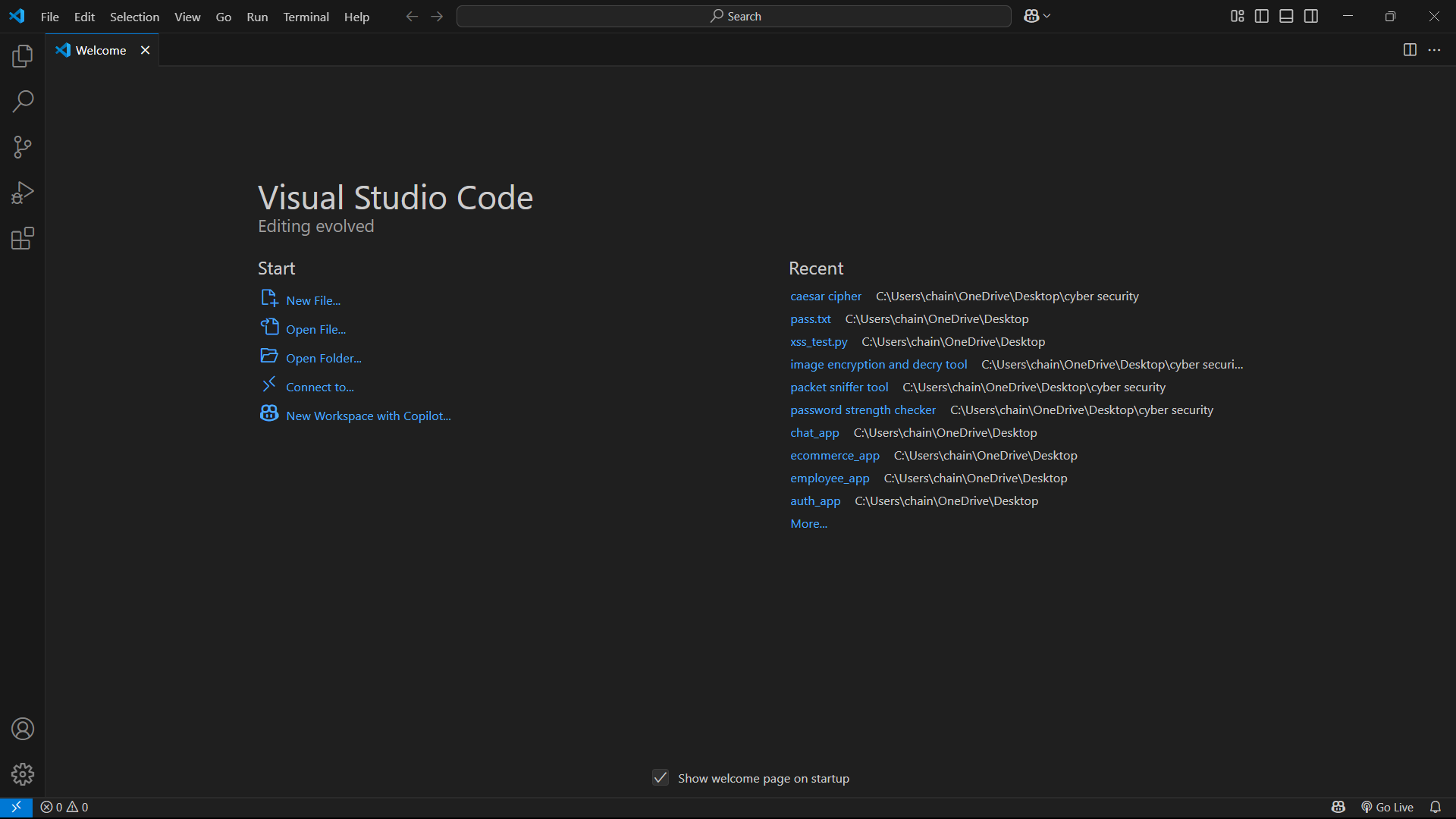
In this example, each character is shifted based on the given key (123). The Caesar Cipher illustrates how even simple techniques can secure data through transformation, making it unreadable without the correct key.

**Implementation of Caesar Cipher code in Python**

**Steps: -**

1. Choose a code editor or IDE as per your choice.
2. Install and set up **VS code.**

Download: Visit <https://code.visualstudio.com/> and install VS Code.



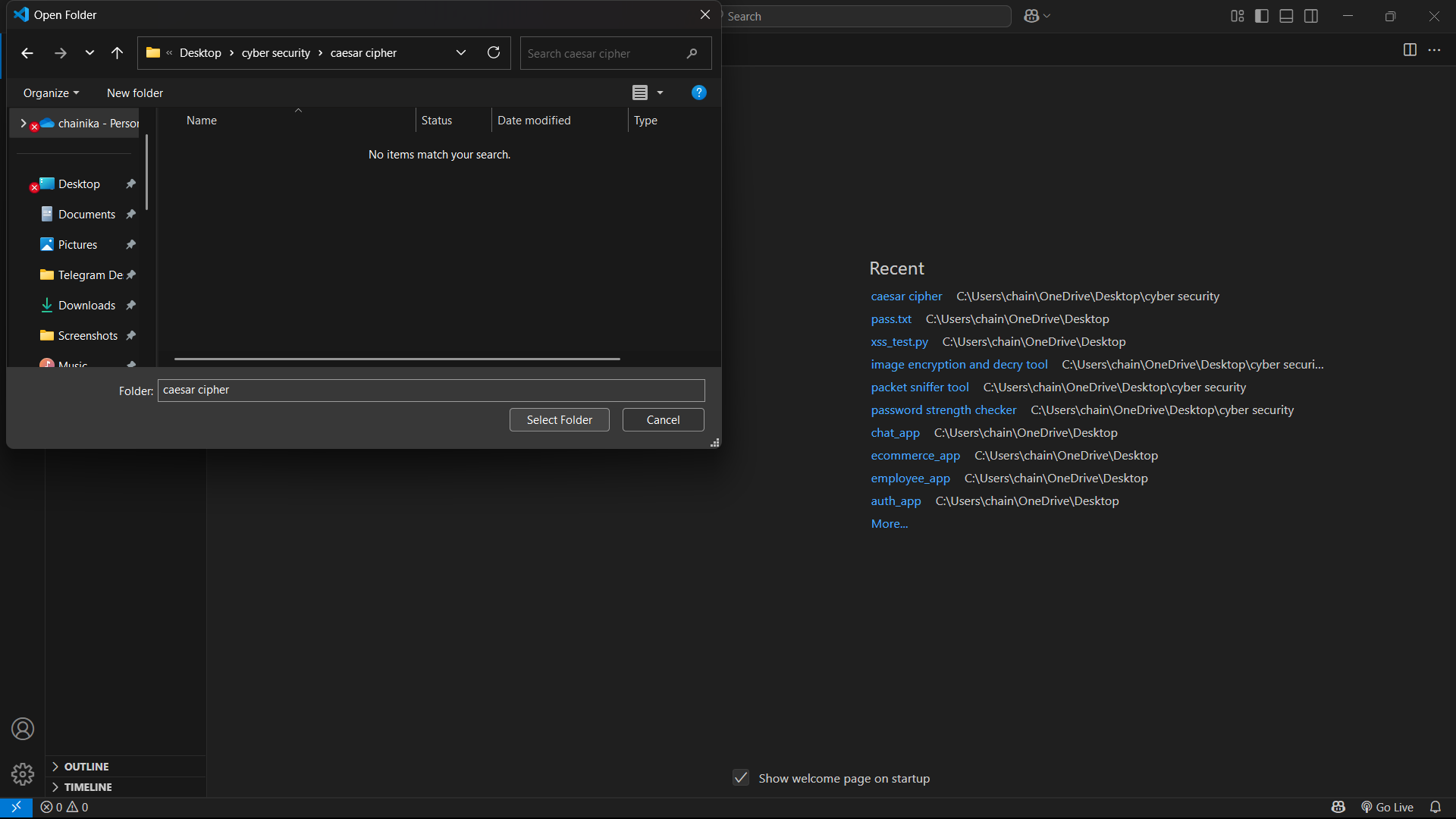
Go to extension tab (ctrl+ shift+ x) and search for Python. Click install on the official Microsoft Python extension.

Choose python interpreter (I have selected Python 3.12.7)

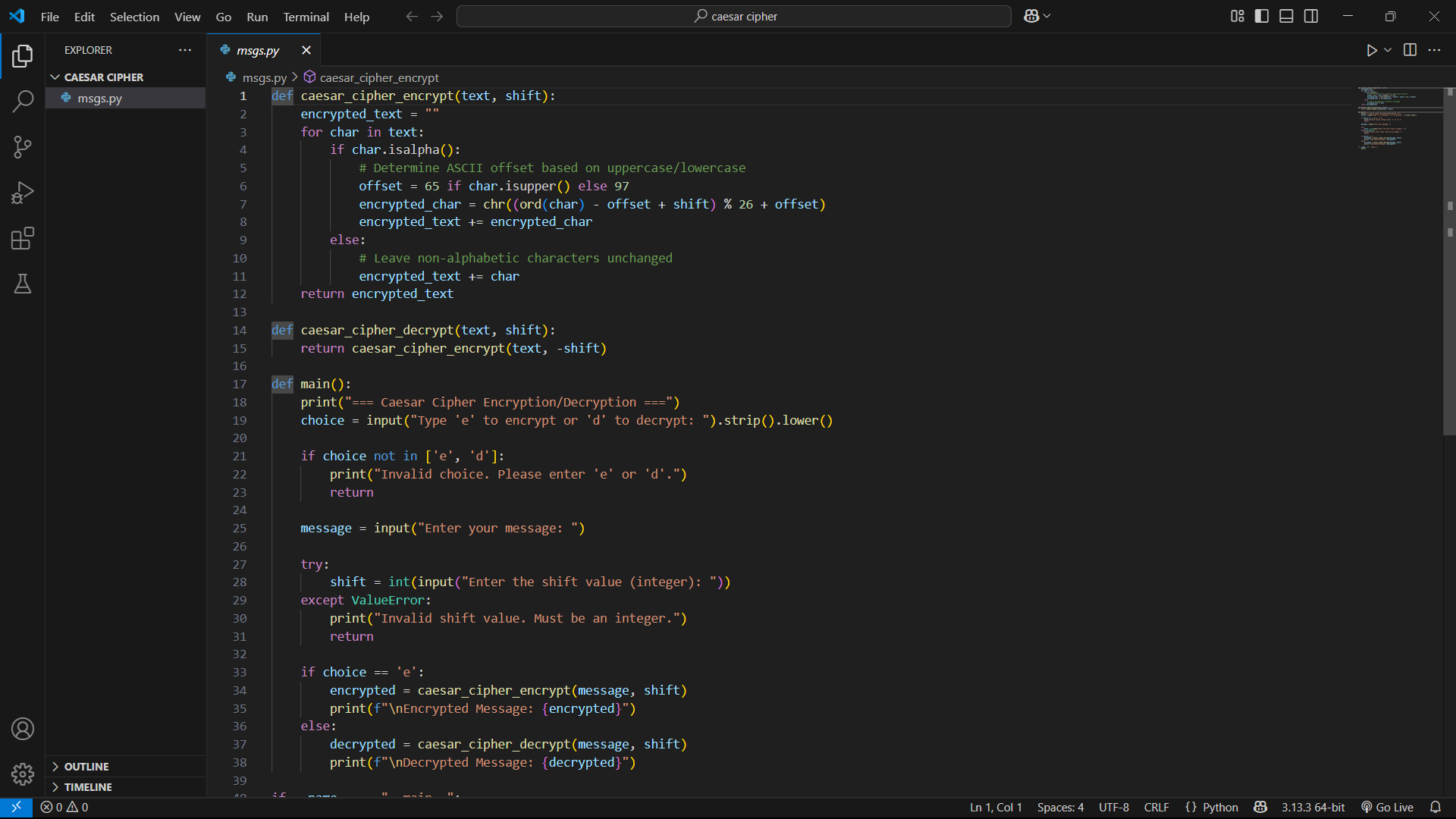
1. Create and save a python file (file having extension .py)

In VS Code: File : New File.

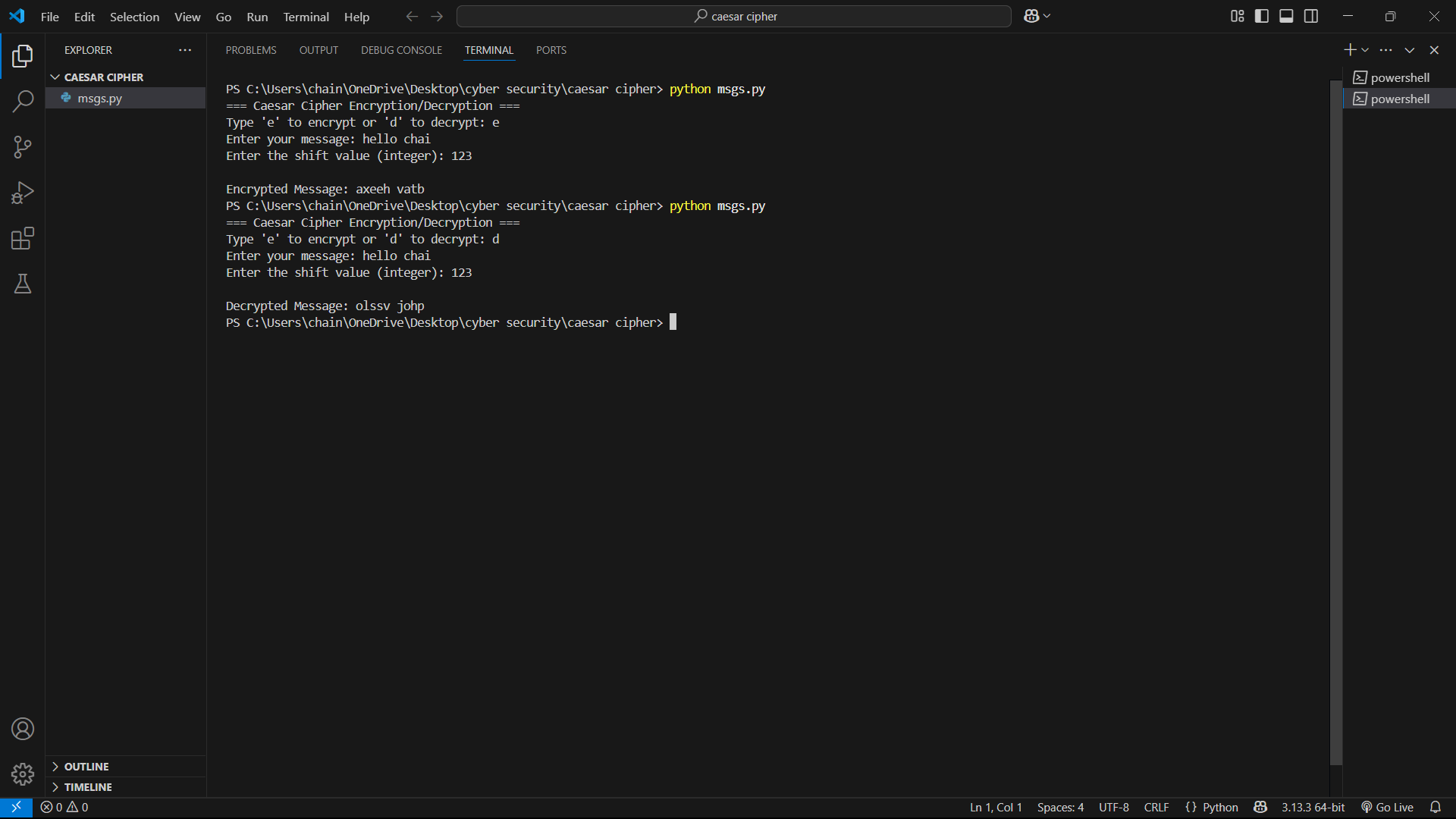
And, Save the file extension .py



1. Initiate with writing your program:



1. Then Run the program in the terminal:



Successful running of program with the result shows the correct program.

**Significance of Caesar cipher technique on encryption decryption of text: -**

The Caesar Cipher is one of the earliest known and simplest techniques in the field of cryptography. It operates by shifting each letter in a text by a fixed number of positions in the alphabet. This basic substitution method introduces the fundamental concept of encryption—transforming readable text (plaintext) into an unreadable format (ciphertext) to protect information from unauthorized access.

**Simplicity and Vulnerabilities**  
One of the key characteristics of the Caesar Cipher is its simplicity. This makes it an excellent teaching tool for those new to cryptography, as it illustrates the basic principles of encoding and decoding messages. However, this simplicity is also its greatest weakness. The Caesar Cipher is highly vulnerable to brute force and frequency analysis attacks, as there are only 25 possible key shifts in the English alphabet. As a result, it provides minimal security in any practical or modern application.

**Historical Significance**  
Despite its vulnerabilities, the Caesar Cipher holds considerable historical importance. Named after Julius Caesar, who reportedly used it to protect military messages, this cipher represents one of the earliest attempts to ensure confidentiality in communication. It laid the groundwork for more sophisticated cryptographic systems that evolved over centuries.

**Educational and Conceptual Value**  
The Caesar Cipher remains relevant in the study of cryptography due to its educational value. By exploring how this cipher works, learners can better understand the concepts of encryption, decryption, and key management. It also helps illustrate the need for stronger cryptographic algorithms in today’s digital landscape.

**Conclusion**  
In conclusion, while the Caesar Cipher is no longer used for secure communication, it plays a critical role in the history and development of cryptographic techniques. Studying it allows us to appreciate the progress made in securing information and highlights the continuous need to innovate in the face of evolving security threats.

**Presented by: - Chainika Dongre Date: - 17 May 2025**