

**Name:** Deep Pawar(A20545137)  
**Professor:** Yousef M Elmehdwi  
**Institute:** Illinois Institute of Technology

# CS 458: Introduction to Information Security

Spring 2024 - Coding Assignment I

---

**OBJECTIVE:** The objective of this assignment is to implement a simple encryption and decryption program in any programming language.

## PROGRAM FEATURES:

### (1) Encryption:

- Prompt the user to enter plaintext and a key.
- Use the entered key to perform encryption (e.g., Shift cipher).
- Display the resulting ciphertext.

### (2) Decryption:

- Prompt the user to enter ciphertext and the corresponding key used for encryption.
- Use the entered key to perform decryption and retrieve the original plaintext.
- Display the decrypted plaintext.

### (3) Brute Force Attack:

- Prompt the user to enter only the ciphertext (without the key).
- Implement a brute force attack to try all possible keys (shift values) for a Caesar cipher.
- Display all the possible plaintext results.

**USER INTERACTION:** The program should display a menu with options for encryption, decryption, and brute force attacks. The user can choose the desired operation by entering the corresponding option number.

## EXAMPLE INTERACTION:

Choose an option:

1. Encryption
2. Decryption
3. Brute Force Attack

Enter your choice (1/2/3): 1

Enter plaintext: Hello World

Enter key: 3

Ciphertext: Koor Zruog

## REQUIREMENTS:

- The code should be well-documented, including comments explaining the logic of encryption, decryption, and the brute force attack.
- Ensure error handling for invalid inputs (e.g., non-numeric key, empty plaintext/ciphertext).

**SUBMISSION:** Students are required to submit the source code via Blackboard.

- **Encryption:**

Encryption is the method of transforming plaintext data into ciphertext or a coded form, which is known as encryption. Sensitive data should be protected, and encryption should ensure that only people with permission can view or decipher the original information.

Numerous applications, such as safeguarding stored data, and guaranteeing the privacy of sensitive information, heavily rely on encryption.

- **Decryption:**

The process of translating encrypted data called ciphertext back into its original, readable form called plaintext is known as decryption. It is encryption working in reverse. A particular key or procedure that can undo the transformation used during encryption is needed for decryption.

For secure communication and data security, decryption is essential. Accessing and decoding the original data should only be limited to those with the appropriate decryption key.

- **Shift cipher:**

A shift cipher, sometimes referred to as a Caesar cipher, is a straightforward and traditional encryption method in which the plaintext's letters are rearranged either up or down the alphabet by a predetermined amount for each letter. The amount of shifts each letter undergoes in a shift cipher is its key. The letters are shifted using the designated key during the encryption and decryption processes. If the end of the alphabet is reached, the shift can be circular, looping back to the start.

While the shift cipher is easy to implement, it is not considered secure for significant cryptographic applications due to its vulnerability to brute force attacks. Because there are only 26 possible keys for the English alphabet, exhaustive search techniques can be used to try every key until the right one is located.

- **Brute Force Attack:**

A brute force attack seeks to gain unauthorized entry to a system, encrypted data, or protected information by continuously trying every possible combination of keys or passwords until the proper one is identified. A brute force assault on a shift cipher entails attempting every key until the right one is discovered and the ciphertext can be successfully decoded. whether the shift cipher key, for instance, can have values between 1 and 25, attempting each of these keys would be the first step in a brute force attack to determine whether any of them produces a useful result. A brute force attack's effectiveness is dependent upon various elements, including the

A brute force attack's effectiveness is dependent upon various elements, including the encryption algorithm's strength, the key's length and complexity, and the attacker's processing capacity. Brute force attacks are less effective against well-built encryption systems since they require a lot more time and resources to succeed when using strong encryption algorithms with lengthy, complicated keys. To prevent brute force attacks and improve the general security of systems and data, security measures like applying long and difficult keys are frequently used.

## • OUTPUT:

### ➤ Encryption and Decryption using Shift Cipher:

```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 1
Enter the Plain text : I am Deep Pawar
Enter the key : 5
Cipher text : N fr Ijju Ufbfw
>>>

= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 2
Enter the Cipher text : N fr Ijju Ufbfw
Enter the key : 5
Decrypted Text : I am Deep Pawar
>>>
Ln: 23 Col: 0

```

### ➤ Brute Force Attack:

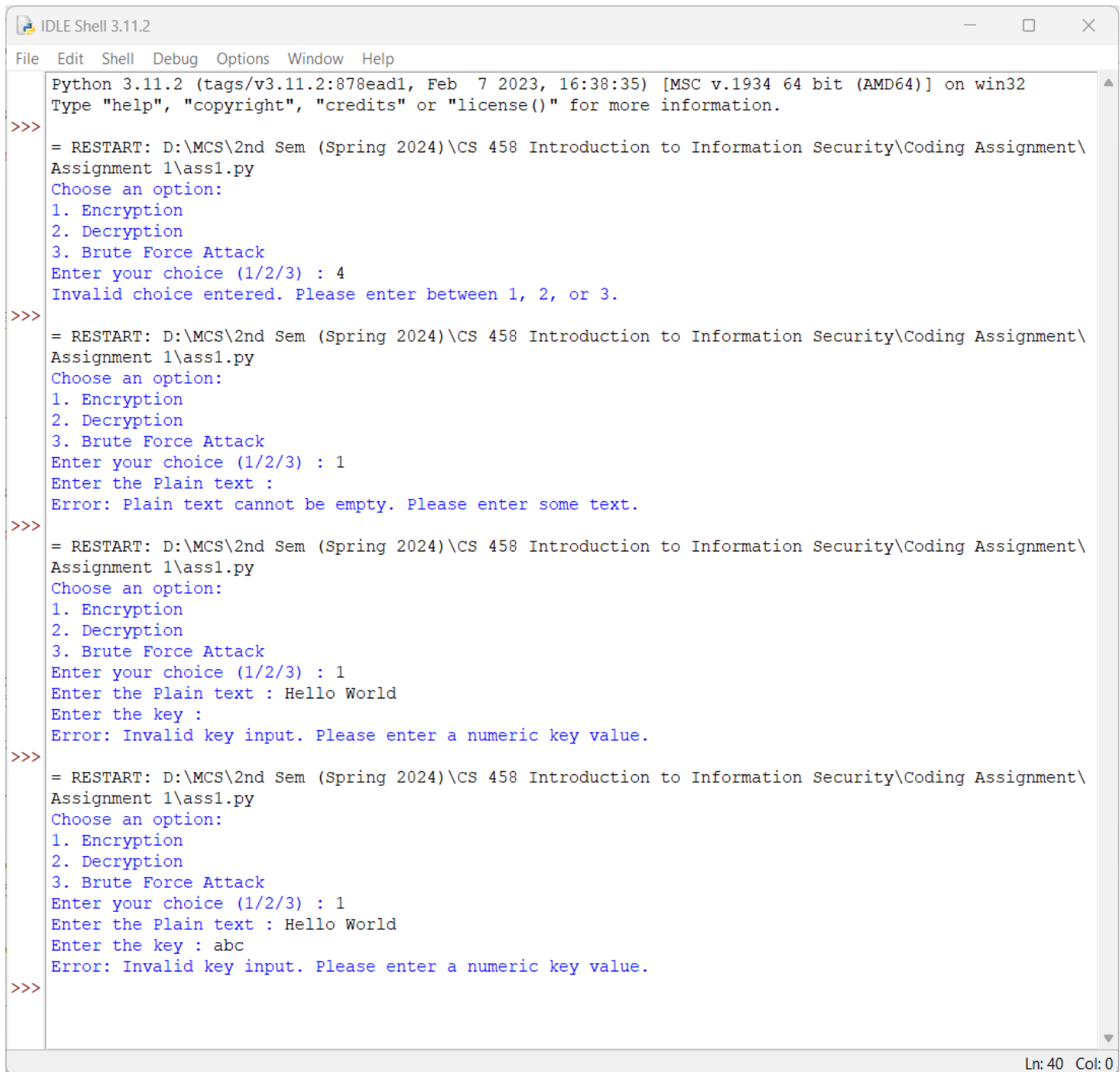
```

= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 3
Enter the Cipher text : N fr Ijju Ufbfw
Possible Decryption texts :
For Key 1 : Decrypted Text is M eq Hiit Teaev
For Key 2 : Decrypted Text is L dp Ghhs Sdzdu
For Key 3 : Decrypted Text is K co Fggr Rcyct
For Key 4 : Decrypted Text is J bn Effq Qbxbs
For Key 5 : Decrypted Text is I am Deep Pawar
For Key 6 : Decrypted Text is H zl Cddo Ozvzq
For Key 7 : Decrypted Text is G yk Bccn Nyuyp
For Key 8 : Decrypted Text is F xj Abbm Mtxo
For Key 9 : Decrypted Text is E wi Zaal Lwswm
For Key 10 : Decrypted Text is D vh Yzzk Kvrvm
For Key 11 : Decrypted Text is C ug Xyyj Juqul
For Key 12 : Decrypted Text is B tf Wxxi Itptk
For Key 13 : Decrypted Text is A se Vwwh Hsosz
For Key 14 : Decrypted Text is Z rd Uvvg Grnri
For Key 15 : Decrypted Text is Y qc Tuuf Fgmqh
For Key 16 : Decrypted Text is X pb Stte Eplpg
For Key 17 : Decrypted Text is W oa Rssd Dokof
For Key 18 : Decrypted Text is V nz Qrrc Cnjne
For Key 19 : Decrypted Text is U my Pqqb Bmimd
For Key 20 : Decrypted Text is T lx Oppa Alhlc
For Key 21 : Decrypted Text is S kw Nooz Zkgkb
For Key 22 : Decrypted Text is R jv Mnny Yjfja
For Key 23 : Decrypted Text is Q iu Lmmx Xieiz
For Key 24 : Decrypted Text is P ht Kllw Whdhy
For Key 25 : Decrypted Text is O gs Jkkv Vgcgx
>>>
Ln: 57 Col: 0

```

➤ **Error Handling:**

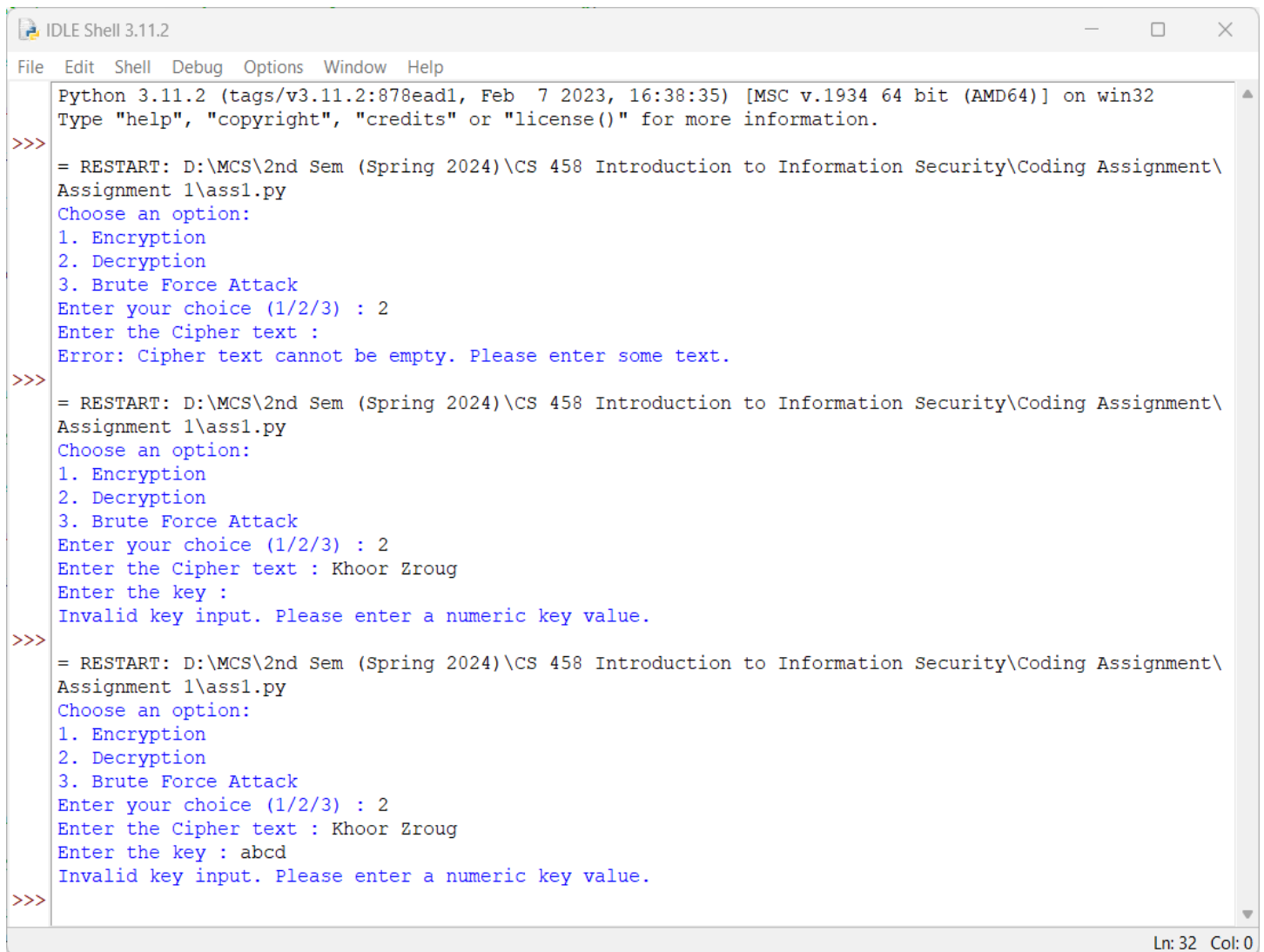
• **Error handling for invalid inputs while performing Encryption:**



```
IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 4
Invalid choice entered. Please enter between 1, 2, or 3.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 1
Enter the Plain text :
Error: Plain text cannot be empty. Please enter some text.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 1
Enter the Plain text : Hello World
Enter the key :
Error: Invalid key input. Please enter a numeric key value.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 1
Enter the Plain text : Hello World
Enter the key : abc
Error: Invalid key input. Please enter a numeric key value.
>>>
```

Ln: 40 Col: 0

- **Error handling for invalid inputs while performing Decryption:**

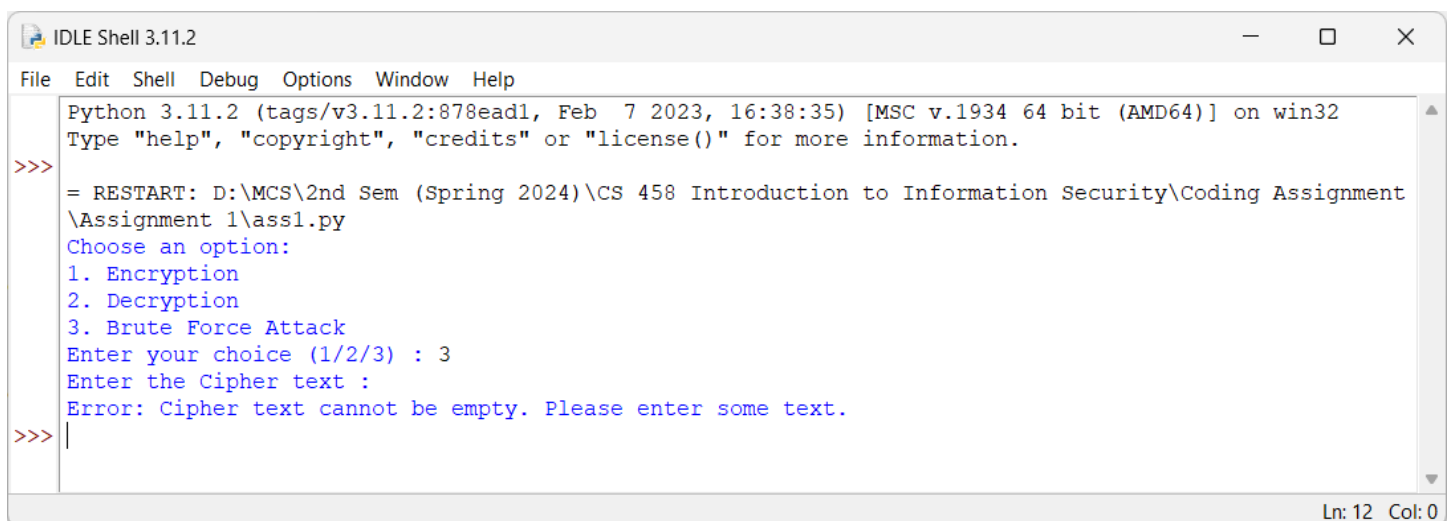


```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 2
Enter the Cipher text :
Error: Cipher text cannot be empty. Please enter some text.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 2
Enter the Cipher text : Khoor Zroug
Enter the key :
Invalid key input. Please enter a numeric key value.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 2
Enter the Cipher text : Khoor Zroug
Enter the key : abcd
Invalid key input. Please enter a numeric key value.
>>>
Ln: 32 Col: 0

```

- **Error handling for invalid inputs while performing Brute Force Attack:**



```

IDLE Shell 3.11.2
File Edit Shell Debug Options Window Help
Python 3.11.2 (tags/v3.11.2:878ead1, Feb 7 2023, 16:38:35) [MSC v.1934 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:\MCS\2nd Sem (Spring 2024)\CS 458 Introduction to Information Security\Coding Assignment\
Assignment 1\ass1.py
Choose an option:
1. Encryption
2. Decryption
3. Brute Force Attack
Enter your choice (1/2/3) : 3
Enter the Cipher text :
Error: Cipher text cannot be empty. Please enter some text.
>>> |
Ln: 12 Col: 0

```