Cyber Security Fundamentals

Assignment 1

Python script used in VS Code to encrypt and decrypt using the Caesar cipher with the specified shift:

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

def caesar_decrypt(text, shift):
    return caesar_encrypt(text, -shift)

def main():
    shift = 4

    # Prompt user for message to encrypt
    message = input("Enter message to encrypt: ")
    encrypted = caesar_encrypt(message, shift)
    print("Encrypted message:", encrypted)

    # Prompt user for message to decrypt
    ciphertext = input("Enter message to decrypt: ")
    decrypted = caesar_decrypt(ciphertext, shift)
    print("Decrypted message:", decrypted)

if __name__ == "__main__":
    main()
```

1. Define the Encryption Function

The **caesar_encrypt** function shifts each alphabetic character in the input text forward by the specified shift.

- It loops through each character.
- Checks if the character is a letter (ignores punctuation and spaces).
- Preserves case (uppercase/lowercase) using ASCII values.
- Converts characters with wrapping around Z to A.
- Non-alpha characters are added unchanged.

Example: 'A' shifted by 4 becomes 'E'.

2. Define the Decryption Function

The **caesar_decrypt** function simply calls **caesar_encrypt** with the negative of the shift:

- To decrypt, we move letters backward by the same shift.
- This reuse of the encrypt function keeps the code concise and clear.

3. Main Program Logic

The **main()** function runs when you execute the script.

- Sets the shift to 4.
- Prompts the user to enter a message to encrypt.
- Prints the encrypted message.
- Prompts the user to enter a ciphertext to decrypt.
- Prints the decrypted message.

This interaction happens in the terminal with simple input/output.

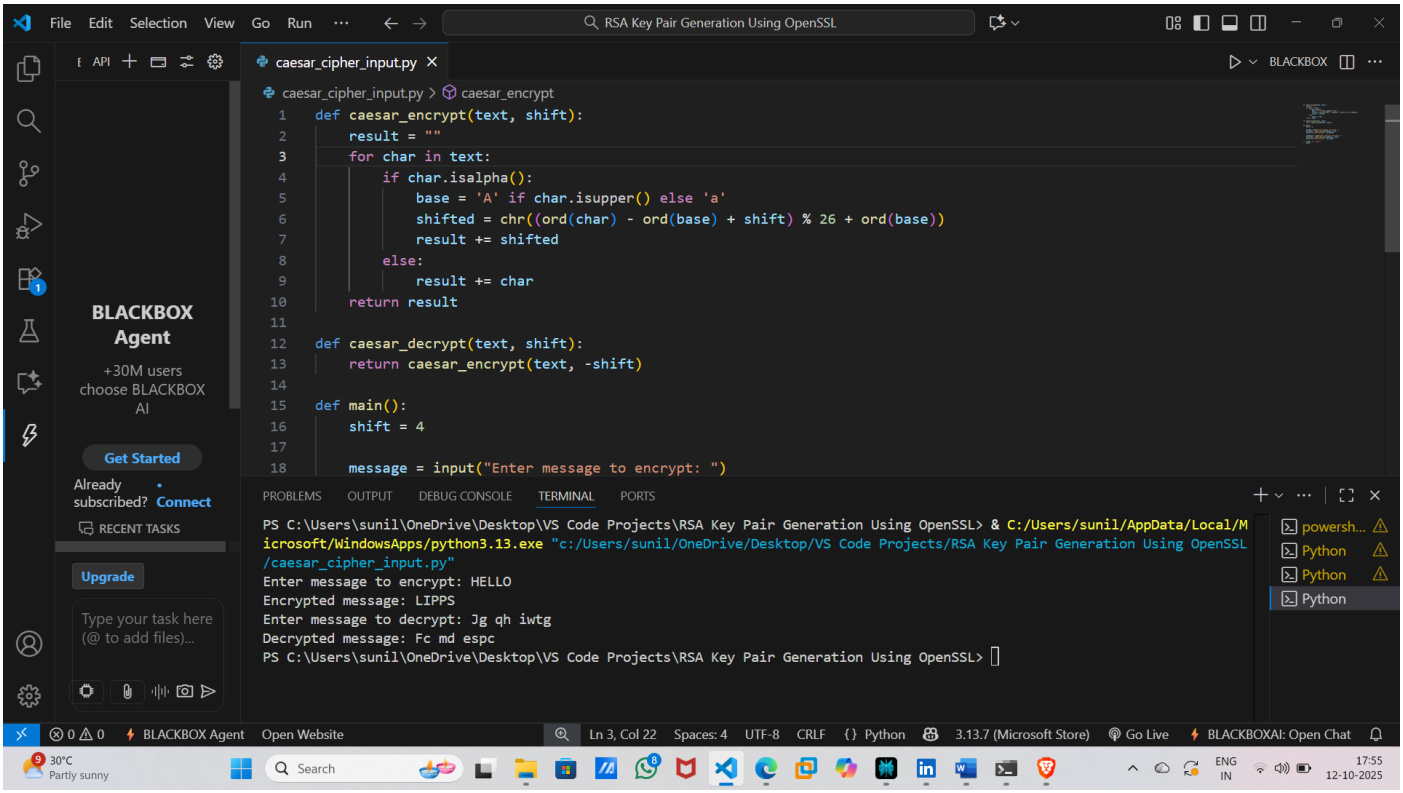
4. Running the Script

- Open VS Code terminal.
- Execute with python **caesar_cipher_input.py**.
- Follow prompts to enter your messages.

This makes the program easy to test with different inputs without changing the code.

Key Takeaways

- The Caesar cipher shifts letters with wrapping.
- Case and non-letter characters are handled gracefully.
- The script is interactive, user-friendly.
- Code reuse by calling encryption with negative shift for decryption.


File Edit Selection View Go Run
RSA Key Pair Generation Using OpenSSL
caesar_cipher_input.py
BLACKBOX
caesar_cipher_input.py > caesar_encrypt
def caesar_encrypt(text, shift):
result = ""
for char in text:
if char.isalpha():
base = 'A' if char.isupper() else 'a'
shifted = chr((ord(char) - ord(base) + shift) % 26 + ord(base))
result += shifted
else:
result += char
return result
def caesar_decrypt(text, shift):
return caesar_encrypt(text, -shift)
def main():
shift = 4
message = input("Enter message to encrypt: ")
BLACKBOX Agent
+30M users choose BLACKBOX AI
Get Started
Already subscribed? Connect
RECENT TASKS
Upgrade
Type your task here (@ to add files)...
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\sunil\OneDrive\Desktop\VS Code Projects\RSA Key Pair Generation Using OpenSSL> & C:/Users/sunil/AppData/Local/Microsoft/WindowsApps/python3.13.exe "c:/Users/sunil/OneDrive/Desktop/VS Code Projects/RSA Key Pair Generation Using OpenSSL/caesar_cipher_input.py"
Enter message to encrypt: HELLO
Encrypted message: LIPPS
Enter message to decrypt: Jg qh iwtg
Decrypted message: Fc md espc
PS C:\Users\sunil\OneDrive\Desktop\VS Code Projects\RSA Key Pair Generation Using OpenSSL>
powersh...
Python
Python
Python
BLACKBOX Agent
Open Website
Ln 3, Col 22
Spaces: 4
UTF-8
CRLF
Python
3.13.7 (Microsoft Store)
Go Live
BLACKBOXAI: Open Chat
30°C
Partly sunny
Search
ENG
IN
17:55
12-10-2025