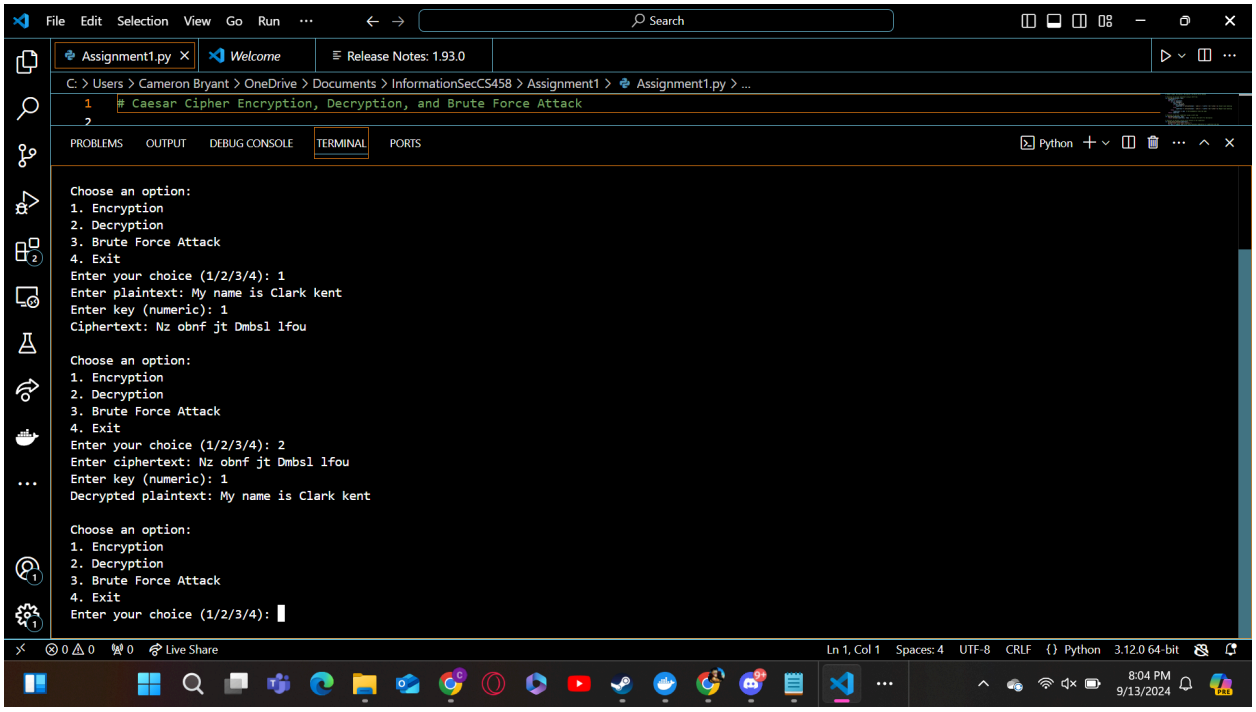
Cameron Bryant
Assignment 1
CS458

Source code:

```
# Caesar Cipher Encryption, Decryption, and Brute Force Attack

# Function to encrypt plaintext using a shift key
def encrypt(plaintext, key):
    ciphertext = ""
    for char in plaintext:
        if char.isalpha():
            shift = key % 26
            if char.islower():
                ciphertext += chr((ord(char) - ord('a') + shift) % 26 +
ord('a')) #Lower-case handling
            else:
                ciphertext += chr((ord(char) - ord('A') + shift) % 26 +
ord('A')) #Upper-case handling
        else:
            ciphertext += char  # Non-alphabetics stay the same
    return ciphertext

# Function to decrypt ciphertext using a shift key
def decrypt(ciphertext, key):
    return encrypt(ciphertext, -key)  # Reverse the shift for decryption

# Function to perform a brute force attack on the ciphertext
def brute_force_attack(ciphertext):
    print("Brute force attack results:")
    for key in range(1, 26): #Try every possible combination of ciphertext
and key
        possible_plaintext = decrypt(ciphertext, key)
        print(f"Key = {key}: {possible_plaintext}")

# Main function
def main():
    while True:
        print("\nChoose an option:")
        print("1. Encryption")
```

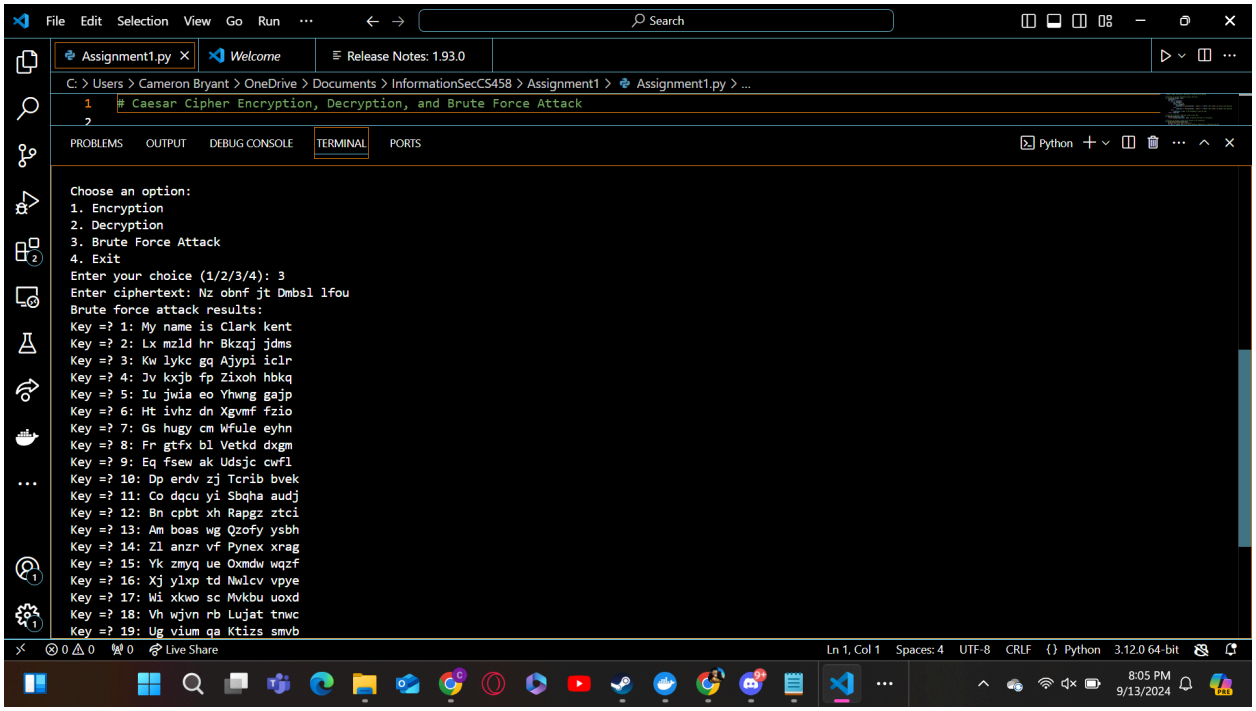
```
        print("2. Decryption")
        print("3. Brute Force Attack")
        print("4. Exit")

        choice = input("Enter your choice (1/2/3/4): ") #user inputs
number for option

        if choice == '1':
            plaintext = input("Enter plaintext: ")
            key = int(input("Enter key (numeric): "))
            ciphertext = encrypt(plaintext, key)
            print(f"Ciphertext: {ciphertext}")
        elif choice == '2':
            ciphertext = input("Enter ciphertext: ")
            key = int(input("Enter key (numeric): "))
            plaintext = decrypt(ciphertext, key)
            print(f"Decrypted plaintext: {plaintext}")
        elif choice == '3':
            ciphertext = input("Enter ciphertext: ")
            brute_force_attack(ciphertext)
        elif choice == '4':
            break
        else:
            print("Invalid choice. Please try again.")

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

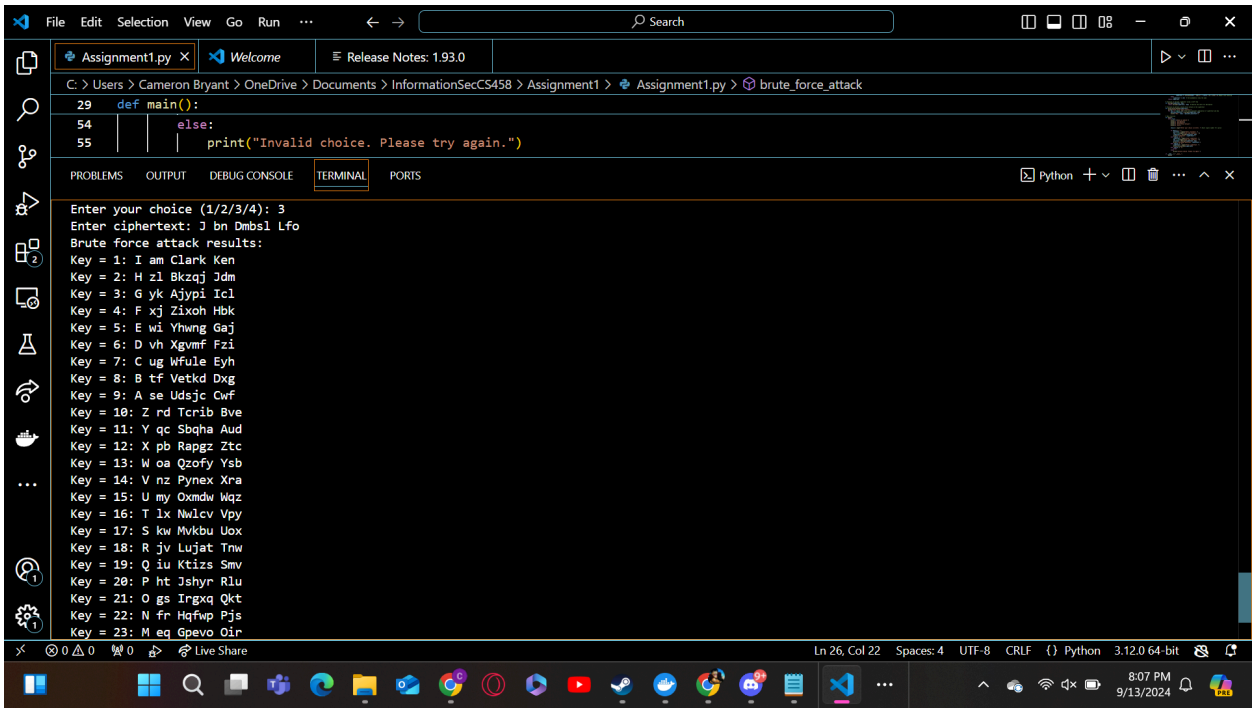
Encryption and Decryption



The encryption and decryption algorithms are very simple. When encrypting, users are expected to submit a key used for the encryption. After entering the text and key, the function encrypts by cycling the letters in each space as many times as the numeric key. This means when a user uses the letter A and encrypts using key 3, they get the letter D in return. That is because D is 3 char spaces from A in the alphabet. The encryption handles capital and lowercase letters, but not numerical values. Decryption uses the encryption function, but uses the negative of the key. This means it simply performs the shift in the opposite direction of the original encryption. Here, I encrypted and decrypted the phrase “My name is Clark Kent” with the key “1”. It had been encrypted into”” Nz obnf jt Dmbsl lfou”. This was returned into its original text using the key used to encrypt it in the first place.

Brute Force Attack





The brute force attack works by using the decrypt function but using every possible key there is. It states the used key and the output based on the submitted ciphertext. Here I encrypted the phases “My name is Clark Kent” and “I am Clark Ken”(typo). Using brute force on both, it attempts every possible key, but at key 1 it shows the correct option, which is the key used to encrypt both.