**Cryptography & Network Security Lab**

**Assignment 01**

**Caesar Cipher:**

The Caesar Cipher, also known as the Caesar Shift or Caesar's Code, is one of the simplest and oldest encryption techniques. It is named after Julius Caesar, who is reputed to have used it to protect sensitive military information. The Caesar Cipher is a type of substitution cipher, specifically a shift cipher, where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

Here's how the Caesar Cipher works:

1. Key: The key in the Caesar Cipher is an integer value, often referred to as the "shift" or "rotation" value. It specifies how many positions each letter in the plaintext should be shifted in the alphabet. For example, if the key is 3, each letter in the plaintext will be shifted three positions to the right.

2. Encryption:

- The Caesar Cipher operates on the letters of the alphabet, both uppercase and lowercase. Non-alphabetical characters (e.g., spaces, numbers, punctuation) are typically left unchanged.

- For each letter in the plaintext, apply the following steps:

- Determine whether the letter is uppercase or lowercase.

- Calculate the new position of the letter in the alphabet by shifting it according to the key.

- Wrap around the alphabet if the shift goes beyond the end (e.g., after 'Z', wrap around to 'A' for uppercase letters).

- Replace the original letter with the letter at the new position.

3. Decryption:

- Decryption is performed by applying the reverse operation of encryption.

- For each letter in the ciphertext, apply the following steps:

- Determine whether the letter is uppercase or lowercase.

- Calculate the new position of the letter by shifting it in the opposite direction of the key.

- Wrap around the alphabet if necessary.

- Replace the original letter with the letter at the new position.

Example:

Suppose we want to encrypt the word "HELLO" with a Caesar Cipher key of 3:

- H -> K

- E -> H

- L -> O

- L -> O

- O -> L

The encrypted word is "KHOOL."

Security Note:

The Caesar Cipher is highly vulnerable to brute-force attacks because there are only 25 possible keys (excluding the key of 0, which leaves the message unchanged). Modern encryption methods offer much higher security and complexity.

The Caesar Cipher is primarily used for educational purposes or as a simple puzzle.

#include <iostream>

#include <string>

using namespace std;

*// Function to encrypt a message using the Caesar cipher*

string encryptCaesarCipher(string *message*, int *key*) {

    string encryptedMessage = "";

    for (char c : *message*) {

        if (isalpha(c)) {

            char shift = isupper(c) ? 'A' : 'a';

            encryptedMessage += (char)(((c - shift + *key*) % 26) + shift);

        } else {

            encryptedMessage += c; *// Leave non-alphabetic characters unchanged*

        }

    }

    return encryptedMessage;

}

*// Function to decrypt a message encrypted with the Caesar cipher*

string decryptCaesarCipher(string *encryptedMessage*, int *key*) {

    return encryptCaesarCipher(*encryptedMessage*, 26 - *key*); *// Decrypt by shifting in the opposite direction*

}

int main() {

    string message;

    int key;

    cout << "Enter a message: ";

    getline(cin, message);

    cout << "Enter the Caesar cipher key (an integer): ";

    cin >> key;

    string encryptedMessage = encryptCaesarCipher(message, key);

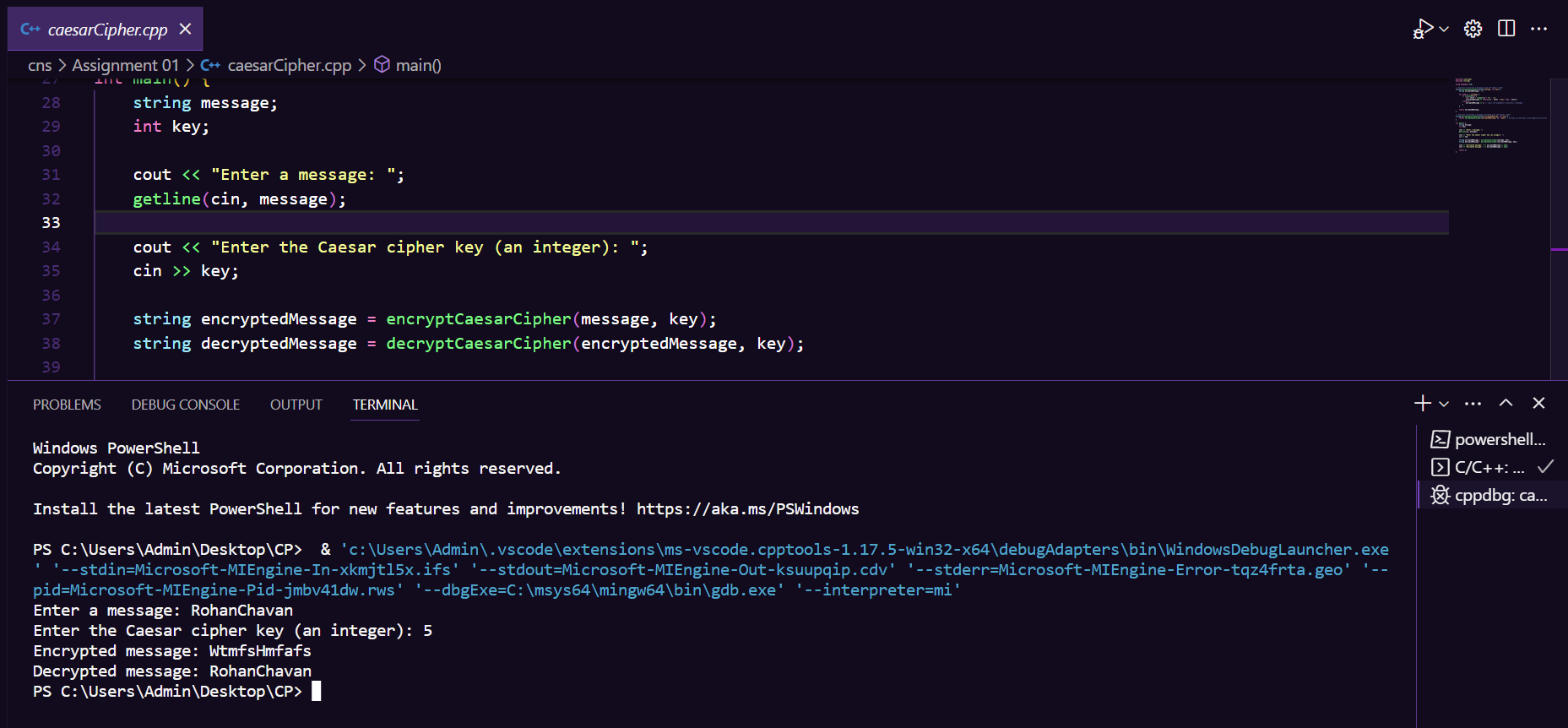
    string decryptedMessage = decryptCaesarCipher(encryptedMessage, key);

    cout << "Encrypted message: " << encryptedMessage << endl;

    cout << "Decrypted message: " << decryptedMessage << endl;

    return 0;

}

**Result:**

**Analysis:**

Drawbacks and Limitations:

1. Lack of Security: The Caesar Cipher is not secure for modern cryptographic purposes. It can be easily broken using brute-force attacks because there are only 25 possible keys (assuming a standard English alphabet) to try. An attacker can simply try all possible keys until the correct one is found.

2. Symmetric Key: The same key used for encryption is used for decryption. This means that both the sender and receiver must know and use the same key, which can be challenging to securely exchange in practice.

3. Limited Key Space: The Caesar Cipher operates on a limited key space, which makes it vulnerable to frequency analysis attacks. An attacker can analyze the frequency of letters in the ciphertext to make educated guesses about the key and plaintext.

4. Predictable Patterns: The Caesar Cipher shifts letters by a fixed amount, which means that if the same plaintext is encrypted multiple times with the same key, it will produce the same ciphertext. This predictability is a significant weakness.

5. Only Shifts Alphabetic Characters: The Caesar Cipher only encrypts alphabetic characters and leaves non-alphabetic characters (such as spaces and punctuation) unchanged. This can make patterns in the original message recognizable in the ciphertext.

6. No Authentication: The Caesar Cipher provides encryption but does not include any form of message authentication. This means that an attacker can modify the ciphertext without detection.

7. Limited Applicability: The Caesar Cipher is primarily used for educational purposes or as a simple historical example. It is not suitable for securing sensitive or valuable information.

Historical Significance:

While the Caesar Cipher has numerous limitations, it holds historical significance as one of the earliest known encryption techniques. It laid the foundation for the study of cryptography and the development of more complex and secure encryption methods.

Modern Usage:

In modern cryptography, the Caesar Cipher is rarely used for practical security. Instead, it serves as a simple example to teach the basic principles of encryption and decryption. More robust encryption algorithms, such as the Advanced Encryption Standard (AES) and public-key cryptography, are employed to secure sensitive data and communications in today's digital world.