Name : Ritesh Pawar
PRN : 2020BTECS00068

Assignment No 1

Cryptography and Network Security Lab (5CS453)

Name : Ritesh Pawar

PRN:2020BTECS00072

Title:

Encryption and Decryption using Ceaser Cipher.

Aim:

To Study and Implement Encryption and Decryption using Ceaser Cipher

Theory:

- Caesar Cipher, also known as the Shift Cipher, is one of the simplest and oldest encryption techniques used to secure information.
- It's a type of substitution cipher where each letter in the plain text is shifted a certain number of places down or up the alphabet.
- The number of positions a letter is shifted is determined by a key.

Encryption:

In Encryption, input is a Plain text and output is a Cipher text.

Step 1: Choose a secret key (a positive integer).
Step 2: Take the plaintext message you want to encrypt.
Step 3: Shift each letter in the message forward in the alphabet by the key positions.
Step 4: Non-alphabetical characters remain unchanged.
Step 5: The result is the ciphertext, the encrypted message.

Decryption:

In Decryption, input is a Cipher text and output is a Plain text.

Step 1: Have the same key used for encryption.
Step 2: Take the ciphertext (the encrypted message).
Step 3: Shift each letter in the ciphertext backward in the alphabet by the key positions.
Step 4: Non-alphabetical characters remain unchanged.
Step 5: The result is the plaintext, the original message.

Code:

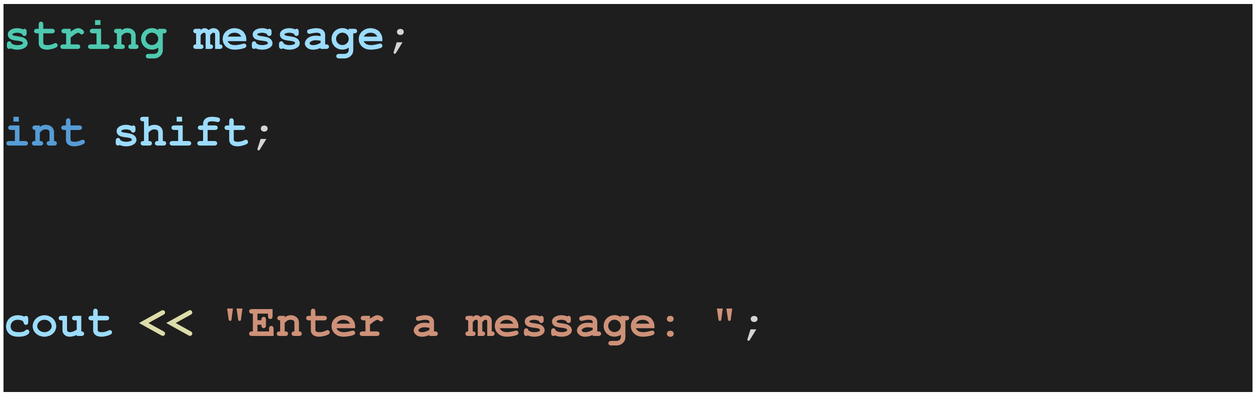
Name : Ritesh Pawar
PRN : 2020BTECS00068

```cpp
#include <iostream>
#include <string>

using namespace std;

// Function to encrypt a message using the Caesar cipher
string encryptCaesarCipher(const string& message, int shift) {
string encryptedMessage = "";

for (char c : message) {
if (isalpha(c)) {
char base = islower(c) ? 'a' : 'A';
encryptedMessage += static_cast<char>((c - base + shift) % 26 + base);
} else {
// Preserve non-alphabetical characters
```

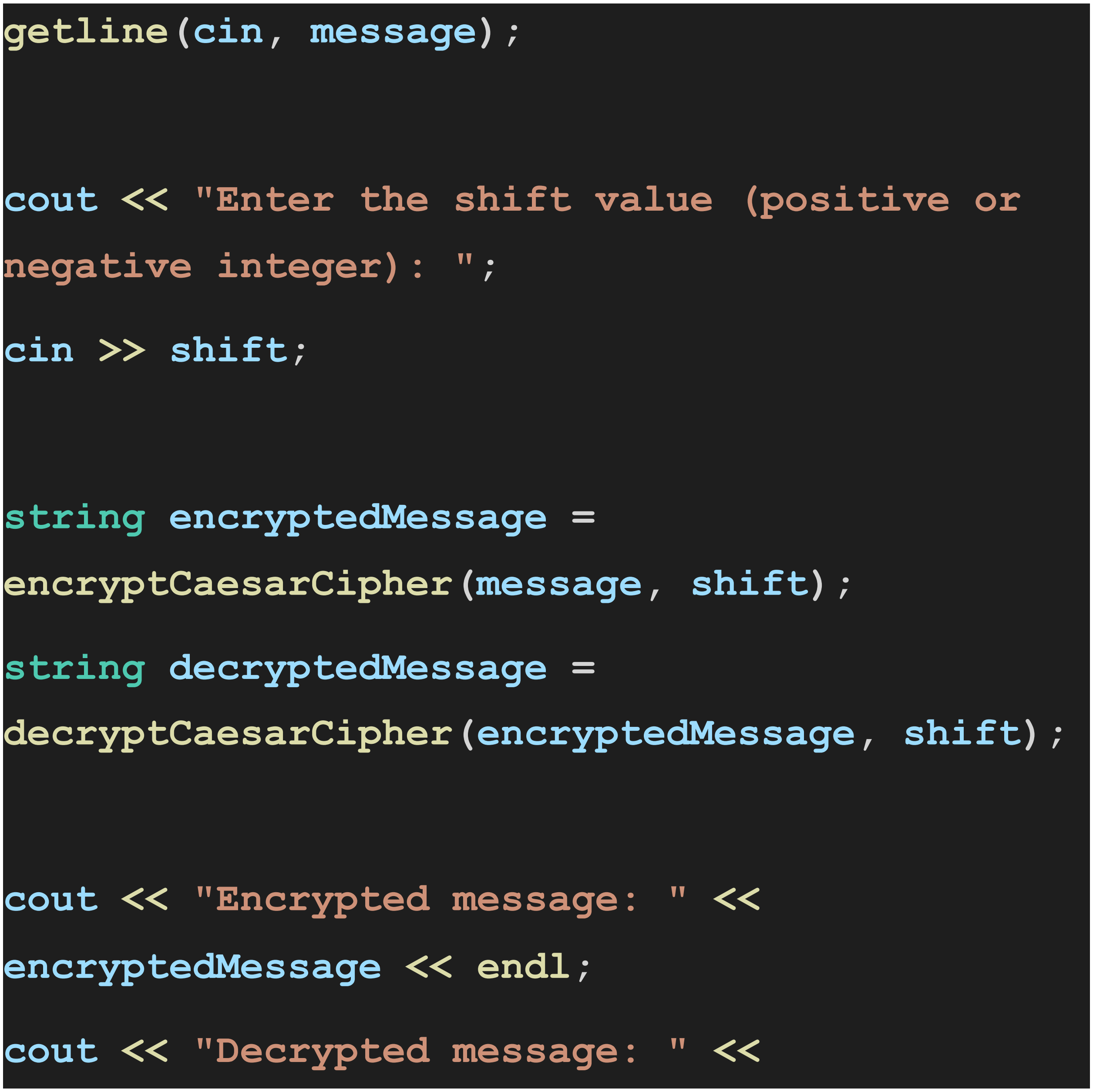
```
encryptedMessage += c;
```

```
}

}


return encryptedMessage;

}


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

string decryptCaesarCipher(const string&
message, int shift) {

// To decrypt, use the negative of the shift
value

return encryptCaesarCipher(message, -shift);

}


int main() {
```

Name : Ritesh Pawar
PRN : 2020BTECS00068



```
string message;
int shift;

cout << "Enter a message: ";
```

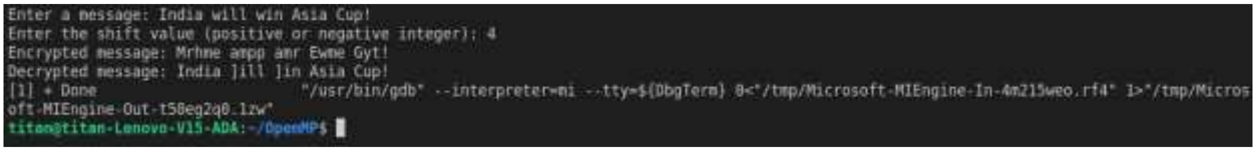


```
getline(cin, message);

cout << "Enter the shift value (positive or
negative integer): ";
cin >> shift;

string encryptedMessage =
encryptCaesarCipher(message, shift);
string decryptedMessage =
decryptCaesarCipher(encryptedMessage, shift);

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

Name : Ritesh Pawar
PRN : 2020BTECS00068

```
decryptedMessage << endl;


return 0;

}
```

Output:



```
Enter a message: India will win Asia Cup!
Enter the shift value (positive or negative integer): 4
Encrypted message: Mrhme ampp amr Ewme Gyt!
Decrypted message: India ]ill ]in Asia Cup!
[1] + Done                       "/usr/bin/gdb" --interpreter=mi --tty=${DbgTerm} 0<"/tmp/Microsoft-MIEngine-In-4m215weo.rf4" 1>"/tmp/Micros
oft-MIEngine-Out-t50eg2q0.1zw"
titan@titan-Lenovo-V15-ADA:~/OpenMP$ 
```

Limitations of the Caesar Cipher:

Weak Security: Caesar cipher is highly vulnerable to brute-force attacks. Since there are only 25 possible shift values (excluding the no-shift case), an attacker can easily try all possibilities to decrypt the message.

Lack of Key Management: In real-world cryptography, secure key management is crucial. In the Caesar cipher, the key is simply an integer representing the shift value. If an attacker discovers the key, they can decrypt all messages encrypted with that key.

Limited Alphabet: The Caesar cipher only works with alphabetic characters. It doesn't handle numbers, punctuation, or any other symbols, which limits its practicality for encoding various types of data.

Frequency Analysis: Even without knowing the key, attackers can still employ frequency analysis. In many languages, certain letters occur more frequently than others (e.g., 'E' is the most common letter in English). An attacker can analyze the frequency of letters in the ciphertext and make educated guesses about the key.

Name : Ritesh Pawar
PRN : 2020BTECS00068

Fixed Shift Value: The Caesar cipher relies on a fixed shift value. This makes it predictable and insecure. More advanced ciphers use variable keys, making them much more secure.

Not Suitable for Modern Cryptography: The Caesar cipher is a historical curiosity and not suitable for securing modern communications. It is easily breakable using modern computational power and cryptographic analysis techniques.