# CIS7 Unit 12 Lab: Programming Cryptography in C++

In this lab activity, we will program Caesar Cipher and Linear Shift Cipher in C++. Refer to Chapter 5 content and notes for Caesar Cipher and Linear Shift Cipher details.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

Encryption of a letter by a shift n can be described mathematically as:  
(Encryption Phase with shift n)

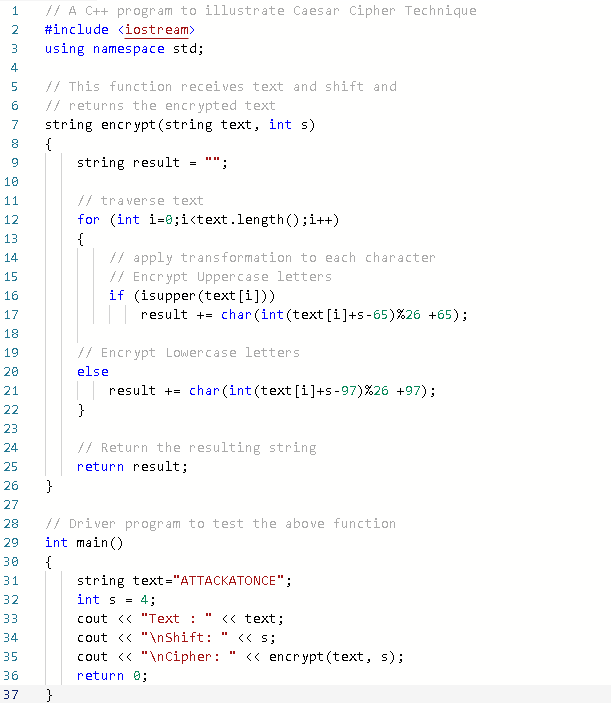
**En(x) = (x + n) mod 26**  
(Decryption Phase with shift n)

**Dn(x) = (x - n) mod 26**



Complete the following tasks and answer the questions:

### Example 2: Caesar Cipher



1. Input the Example 1 program into an IDE. Run the program and answer the following questions:

A screenshot of a computer

Description automatically generated

1. How many characters are shifted in this program to cipher the text string?

Characters are shifted right by four.

1. Use the below table, input the shifted character equivalence to verify whether the program output is accurate.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | X | A | B | C | D |

1. Edit the program to contain a **different shift-value** and **plain-text string**, then run the program. Provide screen capture containing program code and output. What is the shift-value? What is the plaintext string? What is the output?

Shift Value = 25, Plaintext String = “TESTING”

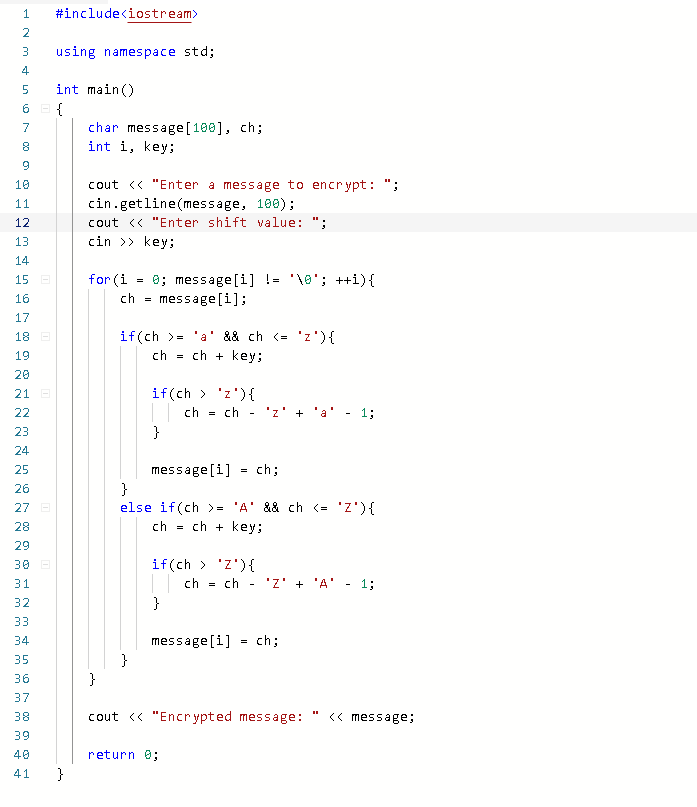
A screenshot of a computer

Description automatically generated

1. Identify the section of the code that contains the encryption mechanism in the program. Provide a brief explanation on the programming functionality of this section.

The encrypt function is responsible for encryption. It determines if the character at any given position is capitalized. If so it takes that character, adds the shift, then subtracts ‘A’ then mods that resulting number by 26 and adds ‘A’. If it isn’t capital it does almost the exact same except it subtracts ‘a’ before the mod and adds ‘a’ at the end. This new character is added onto the result string which is returned as the Cipher string.

### Example 2: Caesar Shift with User Input



1. Input the following program into an IDE, run the program and answer the following questions:
2. Given the message: ***WeareKlingons***. Use shift value of 13. Verify whether the program output is accurate through the illustration of shifting characters manually.

A screenshot of a computer

Description automatically generated

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | ?  f | ?  g | ?  h | ?  i | ?  j | ?  k | ?  l | ?  m |

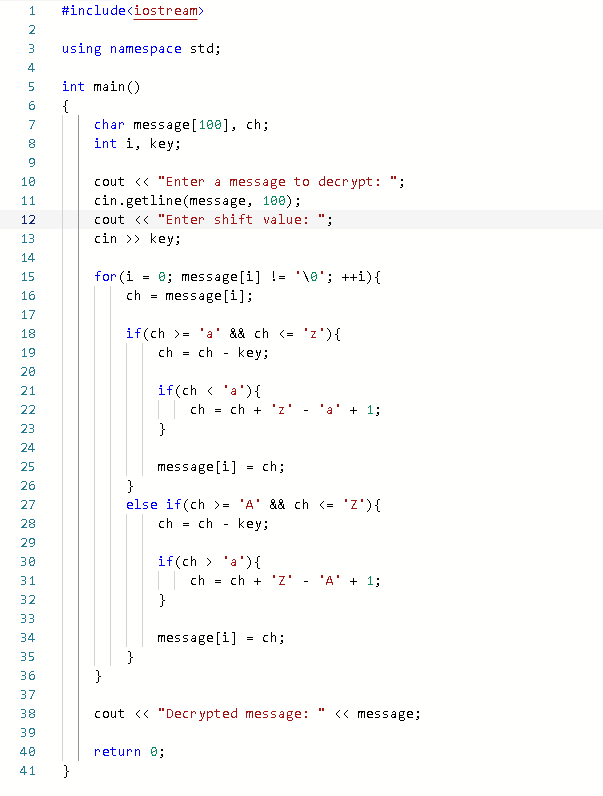
1. Review the program code and explain how Shift Cipher is integrated in the program.

Inside the for loop, we iterate through each of the characters in the message and check if it is capital or lower case and within bounds of A – Z or a – z and greater than Z or z respectively. If so the character is set to itself minus z in lower case if it is lower case or Z if it is upper case plus a if it is lower case or A if it is upper case minus 1. The characters in the message are modified in place.

1. Compare Example 2 to Example 1 program, explain the differences between the programs.

In example 1 we are taking in a string and returning a new cypher string. Furthermore, we are using the two upper functions to check for upper or lower cases and using modulus to ensure the correct character. In example 2 we modify the characters in place without the use of another function and check the case by checking if the character is within a specific range of characters.

### Example 3: Decryption Shift Cipher



1. Input the following program into IDE, run the program to test decryption and answer the following questions:
2. Determine the output using the alphabet characters substitution method when using the message **‘Crypto’** shifting 6 places.

A screenshot of a computer

Description automatically generated

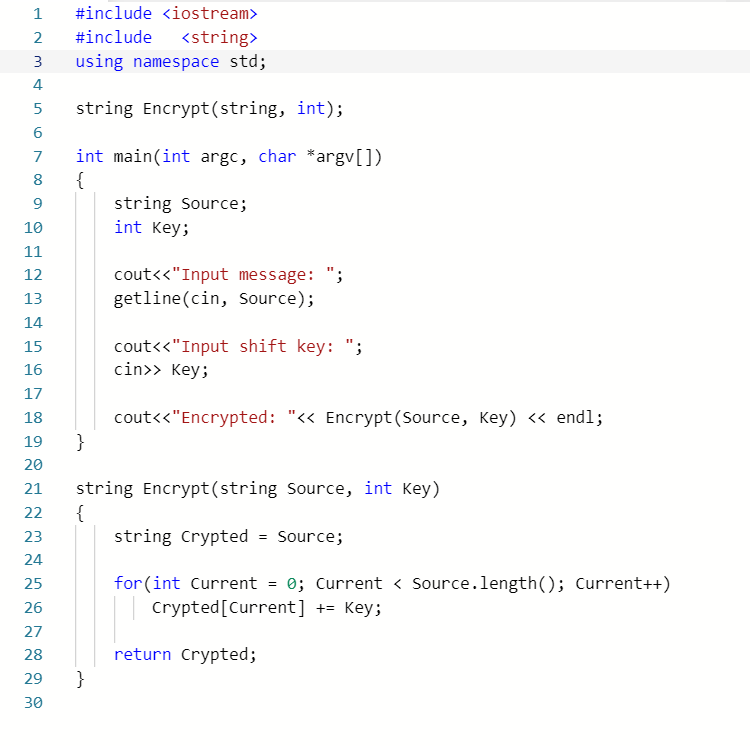
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ; | < | = | > | ? | @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [ | \ | ] | ^ | \_ | ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |

1. Explain the program decryption functionality.
2. Inside the for loop, we iterate through each of the characters in the message and check if it is capital or lower case and within bounds of A – Z or a – z and greater than ‘a’ or less than ‘a’ respectively. If the character is lower case and less than ‘a’ it is set to itself plus ‘z’ minus ‘a’ plus one. If the character is upper case and greater than ‘a’ then it is set to itself plus ‘Z’ minus ‘A’ plus 1. All characters are modified in place.
3. Compare this program to the encryption program in Exercise 2, what are the primary differences and similarities between the programs?

They are both very similar however this time the key is being subtracted from the character. We check if the character is less than ‘a’ if it is lower case and greater than a if it is upper case and we are setting it to itself plus ‘z’ minus ‘a’ plus 1 or itself plus ‘Z’ minus ‘A’ plus 1 if it is lower case or upper case respectively. Both use a for loop iterating through a C-String and range based if statements to check if a character is upper or lower case. They also both operate on the characters in place rather than returning a new array.

### Example 4: Encryption Shift String



1. Input the following program in IDE, test the program and answer the following questions:
2. Use shift cipher character substitution method to determine the output for ‘***substitution’*** when the shifting 5 places.

A screenshot of a computer

Description automatically generated

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ^ | \_ |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | { | | | } | ~ | DEL |

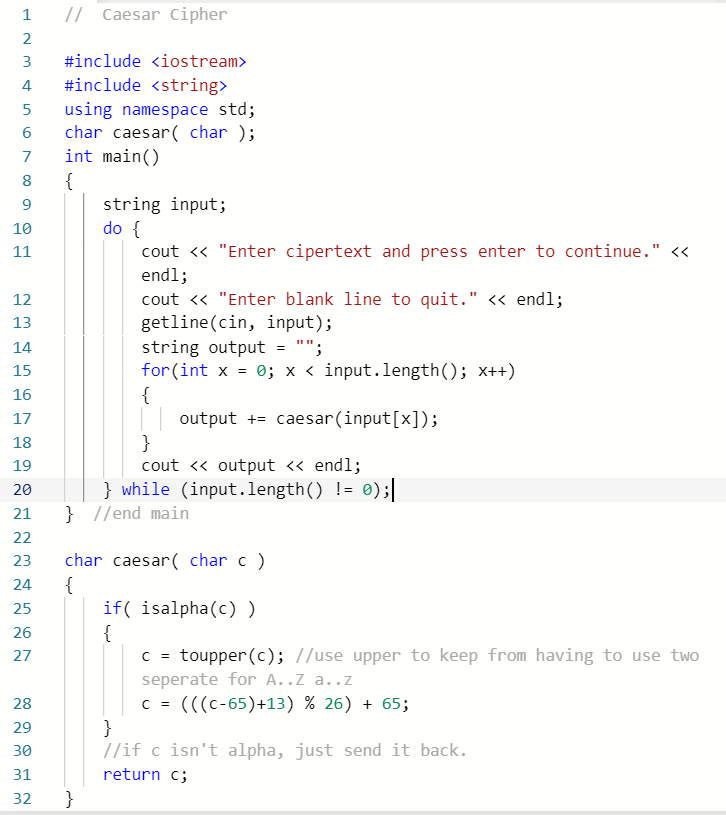
1. Review the program to identify the section that contains the primary functionality of shift cipher. Explain how the shift cipher is integrated in this program.

The encrypt function simply adds the shift cipher to a given character shifting ascii values.

1. Compare this program to the Example 1 and Example 2 programs, what are the differences and similarities in these shift cipher programs? Evaluate these programs based on complexity, efficiency, performance and accuracy.

Examples 1 and 2 only worked with letters a-z or A-Z while this program works with any ascii value. However, there is no bounds checking in this program so we can overflow the 255 ascii value limit and wrap back around. This program is the simplest of the three. As far as time complexity and efficiency all three programs are roughly the same with each of them taking N time to encrypt the string since they all use a for loop which iterates one character at a time through the string.

### Example 5:



1. Input the following program in IDE, run the program and answer the below questions:
2. What is the shift value of the program? Does the program encrypt symbols and special characters?

The shift value is 13 and it only encrypts letters and numbers (i.e. alphanumeric characters)

1. Use shift cipher character substitution method to verify whether the program output for message: ‘***characters’*** is accurate.

A screenshot of a computer

Description automatically generated

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |

1. Review the program to identify the section that contains the primary functionality of shift cipher. Explain how the shift cipher is integrated in this program.

The Caesar function first ensures that the character c passed into the function is a letter or number (alphanumeric) then converts it to upper case if it is a lower case letter. Then it sets the character to (((c-65) + 13) % 26) + 65 and returns the character.

Compare this program to Example 4 program, what are the differences and similarities in these shift cipher programs? Evaluate these programs based on complexity, efficiency, performance and accuracy.

The difference between this program and the program in example four is that this function only works with alphanumeric characters rather than just any ascii value and it has bounds checking thanks to the modulus operator. Both programs have a time complexity of N and have roughly the same efficiency.

Login Canvas and submit lab document that contains screen captures, question and answers.