14.03 Assignment Instructions

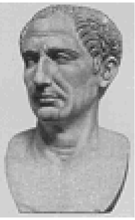
Instructions: Write a program to encode or decode a message using a Caesar Shift.

History of the Caesar Shift

Publin Domain

The first documented use of a substitution cipher in military history is attributed to Julius Caesar (around 50 BCE) during the Gaelic Wars. He sent a coded message to Cicero (who was about to surrender), by substituting Greek letters for Roman letters, and later utilized a substitution cipher that became known as the Caesar Shift. Did you own a secret decoder ring or disk as a child? If so, you have probably used the Caesar Shift. So when you write your program for this assignment, be careful to whom you send coded messages. With a few lines of Java, any Caesar Shift can be broken and your secrets revealed.

Part 1: Encryption



Public Domain

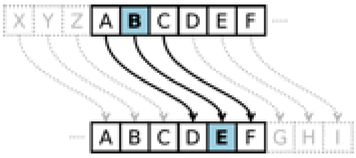
1. Read the **Background** section below to understand the Caesar Shift algorithm.
2. Create a new project called 14.03 Caesar Shift Cipher in the Mod14 Assignments folder.
3. Create two new classes called **Encryption** and **CaesarTester** in the newly-created project.
4. Read over all the specifications and create a plan before starting to write code.
5. Ask the user to input a shift key value from 0–25. Ensure the input is valid. Use the same shift key value for all instances of the **Encryption** class.
6. Declare the alphabet as a class constant.
7. Write a static method to generate the cipher alphabet based on the key.
8. Display the alphabet and cipher alphabet to the screen.
9. Provide a menu to allow the user to choose between encryption and decryption. After one message is processed, allow the user to continue entering more messages until he or she decides to quit.
10. Ask the user to input a plaintext message.
11. Display the encrypted message for the user to view.
12. Write a static method to encrypt the plaintext message and return the result.

Part 2: Decryption

1. Write a new class called **Decryption** in the current project.
2. Allow the user to input a shift key value (0–25) and a cipher text message.
3. You may reuse any previously-created methods or variables.
4. Generate the cipher alphabet based on the key and print the alphabet to the screen.
5. Write a static method to decrypt the plaintext message and print the result.
6. Display the decrypted message.

Background: The Caesar Shift

The Caesar Shift cipher is a simple encryption technique based on substitution. In this example, a shift of three was chosen as the **key**. Each letter in a plaintext message is replaced by the letter three positions further down the alphabet. For example, with a Caesar Shift of three, the letter A in the original message is substituted with the letter D in the cipher message.



Public Domain

Can you decode the message shown?

FRPSXWHU VFLHQFH URFNV

The Caesar Shift does not seem very secure, but keep in mind that most of his adversaries were illiterate. As long as the generals could decode the messages, security was maintained. However, Caesar apparently had more sophisticated encryption techniques when dealing with his political enemies.

A cipher utilizes an algorithm and a key, which specify the exact details of how to encrypt a message. The Caesar Shift algorithm designates which letter in a cipher alphabet to substitute in the plaintext alphabet. For example, if the consecutive letters of the alphabet (***x***) are represented by the integers 0–25 (e.g., a = 0, b = 1, z = 25), the encryption (E_n) or decryption (D_n) of a letter ***x*** by a shift ***n*** can be calculated as follows:

$$\begin{array}{ll} E_n(x) = (x + n) & \textit{if } 0 \leq x + n < 26 \\ E_n(x) = (x + n) - 26 & \textit{if } x + n \geq 26 \\ & \\ D_n(x) = (x - n) & \textit{if } 0 \leq x - n < 26 \\ D_n(x) = (x - n) + 26 & \textit{if } x - n < 0 \end{array}$$

Hint: The modulus operator is very helpful for keeping numbers within a range such as 0 to 25.

Writing a program to perform the Caesar Shift substitution cipher is fairly simple. Determine the identity of each consecutive letter in the plaintext message and substitute the corresponding shifted letter in the cipher alphabet. Decrypting can be done in reverse.

Computer Science Rocks

🖨 Print