Homework 6 - Encryption/Decryption

Jee Whan Choi & Chris Misa

May 21, 2019

DUE DATE: 11:59 PM 5/25/2019

The objective of this assignment is to use inheritance to implement two different types of encryption schemes.

- Provide implementation for decrypting a text, given an implementation for encrypting it.
- Provide implementation for encrypting a text using Caesar cipher.
- Provide implementation for decrypting a text encrypted using Caesar cipher
- Provide implementation for other supporting functions (see `Fill in code here`)

We have implemented a simple encryption algorithm. The encryption algorithms converts an input text (stored in a file, e.g., input.txt in the provide tarball), by using a cipher text (also stored in a file, e.g., cipher.txt in the provided tarball).

The algorithm works as follows. The cipher text is 27 characters long, so that it can convert the 26 characters in the alphabet plus the space. For a given input text that you want to encrypt, it takes each character in the input and converts it to an integer ranging from 0-26, where 0 corresponds to 'a', 25 corresponds to 'z', and 26 corresponds to ' '. Then, it uses this integer to access the corresponding character in the cipher text and replaces the input character with whatever it finds in the cipher text. For upper case letter, it first converts it to lower, find the corresponding character in the cipher text, and then converts it back to an upper case letter.

Figure 1 shows an example.

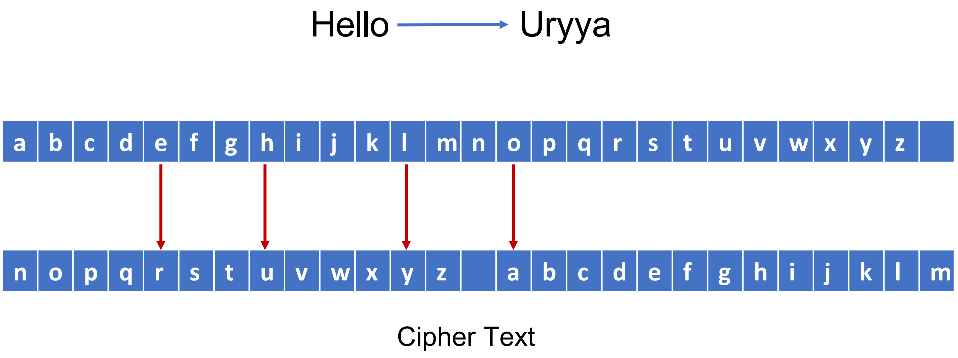
Hello
Uryya
a b c d e f g h i j k l m n o p q r s t u v w x y z
n o p q r s t u v w x y z a b c d e f g h i j k l m
Cipher Text

Figure 1: Encryption

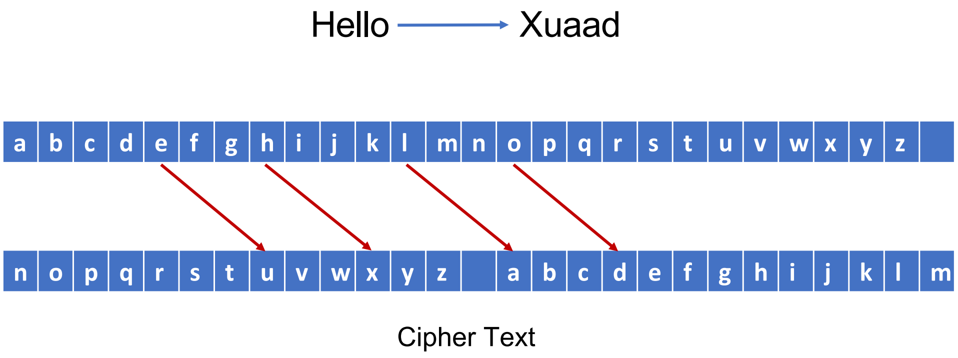
Hello
Xuaad
a b c d e f g h i j k l m n o p q r s t u v w x y z
n o p q r s t u v w x y z a b c d e f g h i j k l m
Cipher Text

Figure 2: Caesar encryption

Here, given the cipher text on the bottom, the input string “Hello” was converted to “Uryya” by calling the encrypt function. Now, if you call the decrypt function with “Uryya” and the same cipher text, the output should be “Hello”.

Caesar cipher is a vartion to this scheme. Instead of simply using the cipher text character in the corresponding position, the cipher text is shifted by a certain offset. Figure 2 shows an example of Caesar encryption with an offset by +3 for the string “Hello”, the result of which is “Xuaad”.

Simarly, decrypting this text (i.e., “Xuaad”) with the same Caesar cipher text and offset should return the original input string, “Hello”.

When you have completed your assignment, verify it on ix-dev. For this project, do not change the file names - just keep them as they are and implement the functions. Also, do not change the provided code.

Grading:

- Working decryption: 4
- Working Caesar encryption: 3
- Working Caesar decryption: 3
- Extra credit: Overload the '++' and '- -' operators for the CaesarCipher class so that they increment/decrement the offset: 5 (for this you can add to, but not delete, from the CaesarCipher class header).

Have fun with your assignment and don't hesitate to post questions on Piazza if something is ambiguous. For this assignment, I expect you to be able to read someone else's (C++) code and figure out what is going on.