Joanna Klukowska
joannakl@cs.nyu.edu

Homework 2

Due date: Feb. 11, 11:55PM EST. Scored: 0-3

You may discuss any of the assignments with your classmates and instructional staff (or anyone else) but **all work for all assignments must be entirely your own**. Any sharing or copying of assignments will be considered cheating.

The purpose of this assignment is to give you more practice on writing C programs.

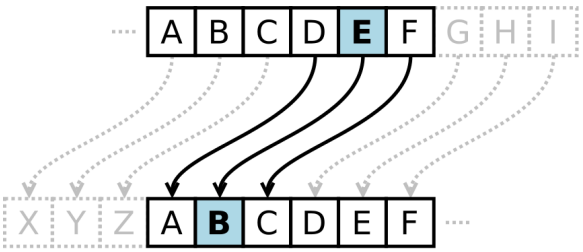
You should be working within the virtual machine that you downloaded for the course, so that you get used to that environment.

Program Description:

You are going to write a simple encryption/decryption program. The algorithm used is very easy to break, so do not start using your program to "securely store your bank account!

Encryption is a process of encoding a message or information in such a way that only authorized parties can read it. (At least this is the idea until somebody discovers how to break an encryption pattern.)

Caesar cipher is one of the simplest encryption techniques. It was used by Julius Caesar to encrypt his private correspondence. It is sometimes called shift cipher because each letter in the unencrypted message is replaced by a different letter which is a fixed number of places down the alphabet (hence shifting).



"Caesar cipher left shift of three" by Matt_Crypto - http://en.wikipedia.org/wiki/File:Caesar3.png. Licensed under Public Domain via Wikimedia Commons. Accessed June 2015.

The figure above illustrates a left shift of three, so that each occurrence of E in the plaintext becomes B in the ciphertext.

When encrypting a message, a person needs to lookup each plain letter, find its corresponding cipher letter and perform a substitution. The following example uses a right shift of three:

```
Plain:  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
Cipher: 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
```

The message "Hello class" is encrypted by replacing each character with a character three spaces to the right in the alphabet resulting in "Khoor fodvv". The message "Ohz Brun" is decrypted by replacing each character with a character three spaces to the left in the alphabet resulting in "New York". It is easy to perform both tasks once we know the shift value and the alphabet.

Your Assignment

Write a program that performs encryption/decryption based on the Caesar cipher. Here is a detailed outline of the program:

- Display the application banner:

```
======================
 Encrypt/Decrypt Tool
======================
```

- Ask the user if they want to perform encryption or decryption.

```
What would you like to do? (E)ncrypt or (D)ecrypt?
```

Joanna Klukowska
joannakl@cs.nyu.edu

The program should accept both upper and lower case letters. If the user enters a different letter, the program should display an error message `ERROR: invalid choice.` and terminate immediately.

- Ask the user for the key value. The key value is the shift amount. It can be any integer that is representable by `int` type. A shift of zero indicates that no encryption is performed since each letter in the plaintext is replaced with itself in the ciphertext. A positive number means shift right during encryption and left during decryption. A negative number means shift left during encryption and right during decryption.
  For example, a shift of 1 converts `a` to `b` and `A` to `B` during the encryption process.
  The alphabetic characters must always remain alphabetic, i.e., when the shift is 27, `A` should become `B`, not `[` (even though `[` is 27 positions away from `A`. You will need to use the modulus `%` operator to achieve this. Note that a shift of 1, 27 and 53 are all equivalent.
- Ask the user for the message. You may assume that the message is contained in one line of text (ends with a new line), but may contain spaces and punctuation characters.
- Compute the encrypted/decrypted message and print it to the screen. All alphabetic characters should be replaced by their encrypted/decrypted equivalents. Any other characters (including digits) should be left unmodified. Your program should preserve case of the letters: encrypting 'a' using the above cipher should result in 'd' and encrypting 'W' should result in 'Z'.

Your program should use functions: you should have an `encrypt` function and a `decrypt` function. Both functions should take the string to be encrypted/decrypted as a parameter along with an integer variable that holds the key value. Both functions should modify the string that is passed to them.

Tools to research and use

You can use the manual pages on Linux to find out about some useful functions that may help with this program. To lookup the definition of a C function `isalpha` use the following:

```
man 3 isalpha
```

(the C functions are in section 3 of the manual, hence the 3 in the above command). The manual page tells you which header file has to be included in your code in order to use this function, provides the description of the function and lists parameters and return values.

The homework directory contains two files: `inputlib.c` and `inputlib.h`. They contain functions that will help you read input from the user. Read through the source code of these files to make sure that you can use them (rather than implement your own versions of them). Reading through these files and understanding what the functions do is also a great practice of your newly acquired capabilities that may come in handy on the midterm exam.

Accessing and submitting this homework

You will be given access to a private repository called `YOUR_GITHUB_USERNAME_homework02` on GitHub and, of course, `YOUR_GITHUB_USERNAME` should be replaced by yout GitHub username). It contains an empty file `caesar.c`. You need to implement your code in that file. It also contains the above mentioned `inputlib.c` and `inputlib.h` files. Finally, it contains a file called `Makefile` - do not edit this file for now (we will learn more about makefiles later on in the course). It is used to compile and build your code. After you make changes to the source code, simply run

```
make caesar
```

This will either produce errors resulting from compilation errors (preprocessing, compilation or linking), or produce an executable file called `caesar`. In the first case, you need to fix the bugs and rerun `make`. In the second case, you can run your program as usual, i.e.,

```
./caesar
```

Running

```
make clean
```

removes all the temporary files, object files and the `caesar` executable from your directory.

To submit the homework, **push** the final version to that repository. You should push intermediate versions as well - this is a way to make sure that you have a backup of the files. We will collect your files from your repository at the due date. (You may make further changes to the code, but they will not be graded.)

Questions

Post any questions you have regarding this assignment to Piazza under the "homeworks" topic.

Joanna Klukowska
joannakl@cs.nyu.edu

Sample Runs of the Program:

Assume user selects encryption, shift of 5 and the message "This is a nice day!"

```
======================
 Encrypt/Decrypt Tool
======================

What would you like to do? (E)ncrypt or (D)ecrypt?  e

Enter your encryption key: 5

Enter your message: This is a nice day!

Your encrypted message is: Ymnx nx f snhj ifd!
```

Assume user selects decryption, shift of 5 and the message "Ymnx nx f snhj ifd!"

```
====================
Encrypt/Decrypt Tool
====================

What would you like to do? (E)ncrypt or (D)ecrypt?: D

Enter your encryption key:  5

Enter your message: Ymnx nx f snhj ifd!

Your decrypted message is: This is a nice day!
```

Assume user selects decryption, shift of 7 and the message "Ymnx nx f snhj ifd!" (Note that this is not the same decryption key that was used for encruption, so the message is displayed, but does not match the original.)

```
====================
Encrypt/Decrypt Tool
====================

What would you like to do? (E)ncrypt or (D)ecrypt?: d

Enter your encryption key:  7

Enter your message: Ymnx nx f snhj ifd!

Your decrypted message is: Rfgq gq y lgac byw!
```

Assume user selects decryption, shift of 2 and the message "Orug ri wkh Ulqjv"

```
======================
 Encrypt/Decrypt Tool
======================

What would you like to do? (E)ncrypt or (D)ecrypt?  D

Enter your encryption key: 3

Enter your message: Orug ri wkh Ulqjv

Your decrypted message is: Lord of the Rings
```

Joanna Klukowska
joannakl@cs.nyu.edu

Assume user selects encryption, shift of -10 and the message ”Lord of the Rings”

```
======================
 Encrypt/Decrypt Tool
======================

What would you like to do? (E)ncrypt or (D)ecrypt?  E

Enter your encryption key: -10

Enter your message: Lord of the Rings

Your encrypted message is: Vybn yp dro Bsxqc
```

Assume user enters invalid choice

```
======================
 Encrypt/Decrypt Tool
======================

What would you like to do? (E)ncrypt or (D)ecrypt?  A

ERROR: invalid choice.
```