COMP 307
Principles of Web Development

Mini Assignment 2
Due: September 26, 2016

In Lecture #4 you were introduced to Asymmetric ciphers. This Mini assignment asks you to write a simple C program using GCC that performs an asymmetric cipher. In class we saw two ways to do the cipher: an easy cyclic modulo version, and a more proper public/private key version (however simplified by multiplication).

This question asks you to use the simplified public/private key version of the asymmetric cipher. Your C program will be a command-line driven application with the following command-line signature:

```
a.out -CHECK   PUBLIC_KEY   PRIVATE_KEY   MODULO
a.out -CIPHER   filename    KEY
```

The option -CHECK tests to see if PUBLIC_KEY, PRIVATE_KEY and MODULO are valid keys that can be used to form an asymmetric cipher. It deduces this based on the slides from class. It prints out: VALID KEYS or INVALID KEYS.

The option -CIPHER opens the text filename (optionally with a path) provided and ciphers the message using the KEY. The ciphered information is saved in a new file using the provided filename but with the extension .CIPHER. This option should be able to cipher and return the message back to its original form. You wold run it once to convert the original message (eg. Message.txt) to the ciphered data (eg. Message.txt.cipher), and then you would decrypt it using the same -CIPHER option (eg. Message.txt.cipher.cipher).

WHAT TO HAND IN

Submit the C file and the a.out file to myCourses Mini Assignment #2 electronic drop box.
This mini assignment has two late days with -5% penalty per late day.
Make sure that it runs on the Trottier computers.