CSC 150 LAB 9-1 FILE ENCRYPTION

PROF. GODFREY C̈MUGANDA
DEPARTMENT OF COMPUTER SCIENCE

Write a program that takes three command-line arguments after the name of the program:

(1) the name of an input file
(2) the name of an output file
(3) an integer

For example, the program might be invoked on the command-line like this

```
encryptprog infile.txt outfile.txt 5
```

The goal of this lab is to implement a simple encryption algorithm. Encryption is the modification of a document to make it un-intelligible to all who see the document, except those that possess the secret information required to transform the document back to its original form.

In this lab, you will open an input file and then write its encrypted form to an output file. You will use a Caesar cipher, which is an encryption method supposedly used by Julius Caesar to communicate secret information to his generals on the battle field. The Caesar cipher uses an integer as encryption key k. To encrypt a file, you replace each letter of the alphabet with the letter k steps ahead of it in the alphabet, with wrapping around to the beginning when you come to the end of the alphabet. Thus, if your encryption key is 5, then various letters are encrypted as shown below

$$a \mapsto f$$
$$b \mapsto g$$
$$c \mapsto h$$
$$\vdots \quad \vdots$$
$$u \mapsto z$$
$$v \mapsto a$$
$$w \mapsto b$$

and so on. Uppercase letters are similarly encrypted,

$$A \mapsto F$$
$$B \mapsto G$$
$$C \mapsto H$$
$$\vdots \quad \vdots$$
$$U \mapsto Z$$
$$V \mapsto A$$
$$W \mapsto B$$

All other characters are left as they were.

Your program should accept negative integers as keys. Thus a file encrypted with the key 5

```
encryptprog plain.txt cipher.txt 5
```

can be decrypted by the command

```
encryptprog cipher.txt clear.txt -5
```

and the `clear.txt` and `plain.txt` files will have identical content.

One other requirement: your program should echo to the screen whatever it writes to the output file.

This lab is due Friday of Week 9.