

Last name First name	
class	CS4840
Assignment name/number	Hwk1 ver1.0 ver2.0 ver3.0
Date submitted	2014/09/19 2014/09/26
cs- login	

This is hwk of T2. Use Java. Use help2500 program style. There may be another hwk concurrently.

Design Playfair Cipher, encryption and decryption.

The project will be in default package.

So if your project is in dir playfair, there without any hierarchy will be your java files that you will sent me.

There will be tope class Playfair and Playfair.java. If you want other assist classes, you can have them, and you need to send them to me.

Also at the same top level of the project will be the data files. That is to say, the data files will have relative path only the name of the file.

In other words, when your prog is looking for data file it will be looking for msgin.txt (or for ./msgin.txt). It will NOT be looking for path1/path2/path3/msgin.txt.

Because there are lots of hidden details in this program, I am moving the due date, hopefully this will work for everyone. We will talk about it.

Some simplifications/hints:

The input files will have less than 10 lines.

In your data J becomes I. (instead dragging around I/J.)

Assume that the message will not contain any double letters within a pair (even if I will have to misspell the words in the msg), --that will simplify the program a bit.

In your program these are the required methods: encrypt(...), decrypt(...). //obvious

As I say on help2500, if you want to have additional methods, you are free to choose.

You can use List, ArrayList, etc from Java library.

Hint: The Java division and Java % operation on int violate the Division Theorem for Z. You may have to do some workarounds.

Input format.

Input files:

msgin.txt

cipin.txt

msgout.txt

cipout.txt

Each file is text file.

Each file will have on the first line the appropriate key.

For msgin it will have encryption key.

For cipin it will have decryption key.

The data will be in capital letters. It will be broken in blocks of 4 letters for readability.

The msg or ciphertext will be broken in blocks of 4 letters, with 32 letters on each line.

Example:

Your file will not have comments.

msgin.txt

ILIK EFIS HING //encrypt key

//msg

TODA YIGO TUPA NDFO UNDO UTTH ATIW ONMI

LLIO NDOL LARS ANDI WILL NOTH AVET OWOR

KANY MORE IAMG OING TOPA RIS

I will test your program by feeding it these files.

The program will compute and save the output into appropriate file, cipout.txt or msgout.txt.

In addition, it will also print to standard output the file in the same format as shown above.

So,

>java Playfair enc msgin.txt

Will result on screen in cipout.txt that looks like this:

TODA YIGO TUPA NDFO UNDO UTTH ATIW ONMI

LLIO NDOL LARS ANDI WILL NOTH AVET OWOR

KANY MORE IAMG OING TOPA RIS

The command line will look like this:

java Playfair <function> <file>

Ex:

>java Playfair enc msgin.txt

>java Playfair dec cipin.txt

Notes:

I did not ask for GUI, please do not give me gui, that is harder to test.