Assignment 8 – The Gold-Bug Cipher

Maximum Points = 50

The purpose of this lab is to continue your introduction to solving problems using Java programming with arrays and Strings.

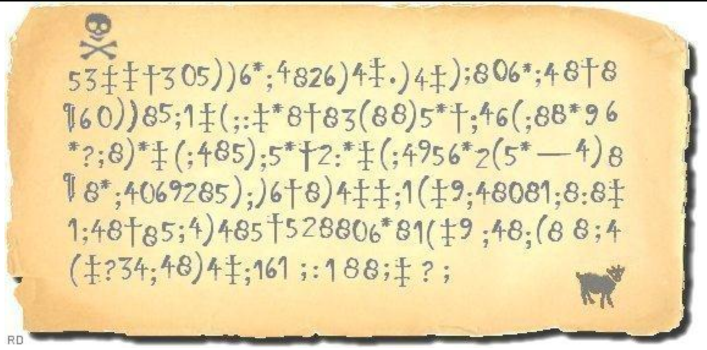
"**The Gold-Bug**" (http://www.poestories.com/text.php?file=goldbug , http://books.google.com/books?id=_B8eAAAAMAAJ) is a short story written by Edgar Allan Poe and published in 1843. The story is a mystery that includes the deciphering of a coded message.

The coded message to the right uses a substitution cipher (http://en.wikipedia.org/wiki/Substitution_cipher) where each letter of the alphabet is replaced with a different symbol. For example in this message,

5	represents	a
!	"	d
8	"	e
3	"	g
4	"	h
6	"	i
*	"	n
+	"	o
(	"	r
;	"	t

and the message translates to:

'A good glass in the bishop's hostel in the devil's --twenty-one degrees and thirteen minutes --northeast and by north --main branch seventh limb east side --shoot from the left eye of the death's-head --a bee-line from the tree through the shot fifty feet out.'"



53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;

*Image by Dirk Rijmenants - **Cipher** Machines & Cryptology*

"**Encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as ciphertext). In many contexts, the word **encryption** also implicitly refers to the reverse process, **decryption** (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted)." [http://en.wikipedia.org/wiki/Encryption] Cryptography is the practice of hiding and retrieving information by enciphering and deciphering messages by means of transformations. Cryptanalysis is the process of converting ciphertext into plaintext without knowing the key used in encryption. Cryptology is the study of cryptography and cryptanalysis.

Encryption techniques have been around for thousands of years [http://csc.ColumbusState.edu/summers/Research/cipher-machines2.ppt]. One of the oldest and simplest techniques is the Caesar Cipher where each letter of the plaintext is shifted a fixed distance from the original position in the alphabet. For example, if the plaintext is "Java Rocks" and the shift distance is 5, then the ciphertext is "Ofaf Wthpx". To decipher, you just shift by five in the other direction.

As a cryptographer, you have been asked by the *National Signal Academy (NSA)* to write a program that allows the user to create her/his own substitution. Your program will also allow the user to encrypt and decrypt messages using the given substitution.

- Your program must first read the substitution key data from a file (filename key.txt) containing pairs of symbols, e.g.

```
5a
!d
8e
3g
4h
6i
*n
+o
(r
;t
y!
:
```

where the first symbol (cipher text) will substitute for the second symbol (the plain text.)

- Your program will then ask the user
  - whether to encrypt or decrypt a message using the key,
  - for the name of the file containing the message,
  - read the message from the file,
  - perform the appropriate substitution on the message, and
  - display both the plain text and the cipher text.

You can assume that punctuation will be substituted for, capitalization will be ignored, and that spaces will be preserved. For example, the plaintext message

“Dig here!” using the key data above will generate the following output:

```
PLAIN TEXT                                   CIPHER TEXT
Dig here!                                    !63 48(8y
```

- Your program must include a class(es) that will hold the sets of text (complete with constructor(s), get and set methods for each instance variable, and a toString method that returns the contents of the instance variables).
- Allow the user to continue using the key to translate messages until she/he wants to quit.
- **Modularize your program to minimize the amount of changes you would need to make if we modify the specifications.**

You MUST work with a classmate. In the comments, indicate the primary author of each class and methods. Both names MUST appear in the documentation for each class and both students must submit the assignment.

You must also keep track of the hours you spent on this project and include it with both assignments:

Student name	Requirements Analysis	Design	Implementation (coding)	Testing

EXTRA CHALLENGES:

i) allow for additional types of encryption, e.g. Caesar Cipher.
ii) Use a GUI to handle the I/O.
iii) Store the “translated” messages for later retrieval

Make sure that your program uses proper indentation and complete documentation. See http://csc.columbusstate.edu/summers/NOTES/1301/style.htm for guidelines.

The program heading should occur at the top of the program and should include:

```
/**
 * PROGRAM SPECIFICATIONS
 * NARRATIVE DESCRIPTION:
 *
 * @author (your name)
 * @version (date)
 */
```

(Due before 8 a.m. on Monday, November 26, 2012) Submit a .doc file containing the UML class diagrams (including the “main” class) all the classes used in your program and your timesheet documenting your time so far to the dropbox in WebCT. [10 pts]

(Due before 8 a.m. on Monday, December 3, 2012) Submit your .java files containing your program and your timesheet documenting your time to the dropbox in WebCT.

Grades are determined using the following scale:

□ Header..…………………..:___/2	• Runs correctly..…………………:___/10
□ Data members…….……..:___/4	• Correct output……..……………:___/10
□ Methods..………………..:___/4	• Design of output..………………:___/8
	• Design of logic…………………:___/10
	• Standards………………………:___/7
	• Documentation..………………..:___/5

Grading Rubric (Word document)