PROJECT: **1** *(Warm-up)*
DUE DATE: **Tuesday February 3, 2015**

Description:

Cryptography is the study of codes and ciphers. It is related to several fields: information security and related issues, such as authentication and access control. It has also been used in computer and network security for things like access control and information confidentiality. The primary purpose of cryptography is hiding the meaning of messages, not usually the existence of such messages.

One of the primary applications of arrays is the representation of strings of characters. Java provides ways to create string objects from character arrays and vice versa.

- `new String(A)`: create an object of class String from a character array A
- `S.toCharArray()`: create a character array representation of string S

These important characteristics of arrays and strings are useful in cryptography. This field studies ways of performing **encryption**, which takes a message, called the **plaintext**, and converts it into a scrambled message, called the **ciphertext**. At the same time, it also studies ways of performing **decryption**, which takes a ciphertext and turns it back into its original plaintext.

The **Caesar Cipher** - simple code where every character in plaintext is shifted a constant number of positions using wrap around.

For example: assume the plaintext is "attack at dawn" and Caesar shift is 10, the generated ciphertext is "kddkmu kd nkgx".

1. Assume the text will only be lower-case letters and space. Only de/encrypt letters.
2. Provide the following class methods in the class `CaesarCipher`:
    a. `encrypt(String plaintext, int shift)`: returns the ciphertext.
    b. `decrypt(String ciphertext, int shift)` : returns the plaintext.
    c. `printLetterCounts(String text)` – prints non-zero letter counts in text using the format:
        ```
        a:3
        e:10
        p:2
        ```
3. Provide a class method `main` to verify the methods in 2.

Is Caesar Cipher a good method? Why? Why not? Explain in the report.

Project report:

- Page 1: Cover page with your name, class, project, and due date
- Page 2 to 3:
    o Section 1 (**Project specification**): Your ADT description. Description of data structures used and a description of how you implement the ADT. A Javadoc of your class.
    o Section 2 (**Testing methodology**): Description of how you test your ADT, refer to your testing output. Explain why your test cases are rigorous and complete. Demonstrate that you test each method.
    o Section 3 (**Lessons learned**): Any other information you wish to include.

Turn in:

1. Print out of project report and output

2. Print out of the source code in landscape mode using non-proportional fonts (eg. Courier).
3. Email the <u>source code</u> with the file name *flast*-**CaesarCipher.java**
    (ex. tnguyen-CaesarCipher.java) to tvnguyen7@cpp.edu with the subject: **cs240w15 p1**.
    Don't name your class *flast*-CaesarCipher. Rename the file before submitting.

Grading Guide:

- 10%: Project report and project output.
- 80%: Program correctness
- 10%: Coding – efficiency, style, comments, formats

Notes:
1. The following information is required in the beginning of every source file.

```
//
//    Name:        Last, First
//    Project:     #
//    Due:         date
//    Course:      cs-240-02-w15
//
//    Description:
//                 A brief description of the project.
//
```

2. The submission **must** be legibly printed.