King Fahd University of Petroleum and Minerals

###### Information and Computer Science Department

**ICS 102: Introduction to Computer Programming**

**Summer Semester 2018-2019 (Term 183)  
Homework #3  
[Posted: Monday July 1st 2019]  
[Due Date: Monday July 8th 2019 @ 11:59 PM (Midnight)]**

**Submission Guidelines:**

Submit a zipped file containing the following files:

* Q1.java (Java source file) containing your answer to the programming question no. 1.
* Q2.java (Java source file) containing your answer to the programming question no. 2.

PLEASE DO NOT INCLUDE .class FILES IN YOUR SUBMISSION

The zipped file should be named as follows:

**HW3\_XXXXXXXXX\_YourFamilyName.zip**

where:

XXXXXXXXX is your 9 digit KFUPM ID.

YourFamilyName is your family name

Submission should be made through your ICS 102 Blackboard course page under **Assignments** submission link.

**Important Notes:**

* **Cheating is taken seriously**. Any cheating attempt will result in an F grade in the course.
* **EACH STUDENT IS REQUIRED TO DO THE HOMEWORK ALONE**. COPYING FROM ANY SOURCE IS REGARDED AS CHEATING.
* **Submission link will be available until 9:00am for late submission without penalty.**
* **Submissions via email are not accepted and will be simply ignored**.
* Submission of the homework solution should be in a zipped filed with the format specified above. **Any different formatting/naming will result in reducing the total homework score by half!**
* **You must use proper indentation and meaningful variable names in your programs.**

This homework is related to cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge. In this question, you will develop a java program that implements a classical form of encryption. Encryption is the process of making a certain message secret. A simple encryption strategy takes each letter in the message and shifts it letters, where is an integer such that . This form of encryption is called a *shift* *cipher*. For example, assume that the message consists of the string “Hello”. Using , the encrypted message is “Wtaad”. Note that if we reach the letter “z” before the shift process ends, we start back from the letter “a”. Also, note that the encryption is case sensitive. The *shift cipher* can be easily implemented by assuming that the letters “a” and “A” have value 0, the letters “b” and “B” have value 1, …, the letters “z” and “Z” have value 25, and then applying the mapping (where “%” represent the remainder of dividing by 26) takes the letter with value and shifts it to the letter with value . The following table shows the value of each letter in the English Alphabet.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A  a | 0 | B  b | 1 | C  c | 2 | D  d | 3 | E  e | 4 | F  f | 5 | G  g | 6 | H  h | 7 | I  i | 8 | J  j | 9 |
| K  k | 10 | L  l | 11 | M  m | 12 | N  n | 13 | O  o | 14 | P  p | 15 | Q  q | 16 | R  r | 17 | S  s | 18 | T  t | 19 |
| U  u | 20 | V  v | 21 | W  w | 22 | X  x | 23 | Y  y | 24 | Z  z | 25 |  |  |  |  |  |  |  |  |

The *shift cipher* can be generalized to what is called an *affine cipher*, whereby given two integers and , each letter of value is transferred to the letter with value . Note that for *affine cipher* to work, the greatest common divisor between and 26 should be equal to 1 (i.e., should be relatively prime to 26).

**Question 1.**

Implement the *affine cipher* to encrypt a message that is stored in a text file. Your program shall prompt the user (console) to enter three inputs:

1. Filename: A string that represents the text filename containing the message to be encrypted. Note that if you enter a wrong filename, your program should display an appropriate message and seek the user’s input again for a correct filename.
2. : An integer value that is relatively prime to 26. You may assume that the user will always input an integer that is relatively prime to 26.
3. : An integer value . You may assume that the user will always enter an integer value.

The program then applies the *affine cipher* on each letter in the message and produces the corresponding encrypted message in a file that should have the extension “enc” appended to the original filename. For example, if the original filename is “message.txt”, the encrypted filename should be “message.txt.enc”.

**Note that digits, punctuation and any character other than letters in the message should be left as is.**

Upon completion of the encryption and generation of the output file, the program should display a proper message saying that the output file has been created. If, for some reason, the output file was not created, the program should display a proper message and terminate.

**Question 2.**

Implement a simple decryption Java program that takes a string that was encrypted using the shift cipher and outputs the original message. This will be achieved by repeatedly applying the shift cipher for different values of and displaying the resulting string on the screen, until the user confirms that the current string is correct. If, after “enough” trials, it was obvious that the original string cannot be retrieved, the user should prompt the program to display a message stating that “It seems that the string was not encrypted using a shift cipher”.