UNIVERSITY AT ALBANY
State University of New York

DEPARTMENT OF COMPUTER SCIENCE

ICSI-526/426 Cryptography – Spring 2016

Assignment 4

Give out date: April 8, 2016,
Due date: April 30, 2016, 11:59 p.m. **Total marks: 10**

Late submissions would have penalty 10% every day up to five days.

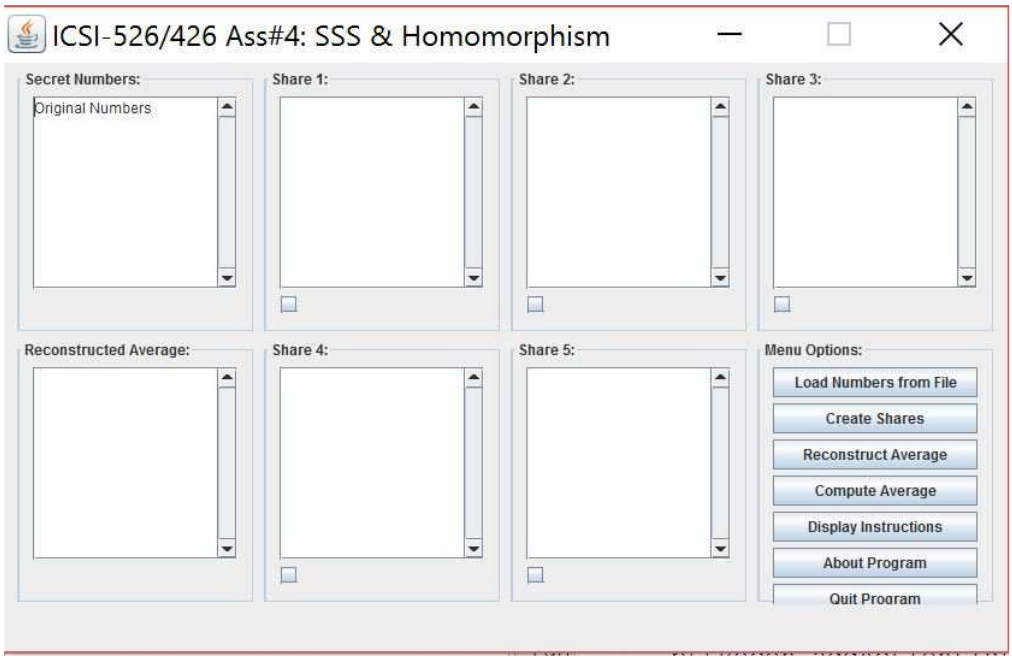
Objective

The purpose of this assignment is to solidify the concepts of **Secret Sharing** and **Homomorphism** that were discussed in class.

Problem

Implement Shamir's (k, n) Secret Sharing (SSS) scheme, with $k = 3$, $n = 5$, to
(a) Find shares of a given set of numbers.
(b) Compute average from shares
(c) Choose any three averages from the five shares and reconstruct the average of original set of numbers

You may choose to develop an interface as shown below.



The code for this interface is provided here: http://www.cs.albany.edu/~patrey/ICSI526-426/assignments/ass4/ShareHomo.java. However, you are free to write your own code for the interface.

In the above interface, function of each component is as follows:

- "Load Numbers from File" button: allows loading numbers from a file. Alternatively you may directly enter the numbers in "Secret Numbers" area.
- "Secret Numbers" area: displays the loaded or entered numbers.
- "Create Shares" button: creates five shares of the loaded or entered numbers and displays them in the respective "Share 1" to "Share 5"components.
- "Share 1" to "Share 5" areas: display the shares.
- "Compute Average" button: calculates the average within each share and displays it in the share area.
- "Reconstruct Average" button: allows reconstructing the average of original set of numbers from the averages in the encrypted domain (i.e. averages within the shares) and displays it in the "Reconstructed Average" area.
- "Display Instructions" button: displays the instructions to use the interface.
- "About Program" button: displays the information about the program.
- "Quit Program" button: closes the program.
- Checkboxes: To select the shares for secret reconstruction.

You are required to do the following:

Write code to create the shares, compute averages in the shares and reconstruct the average of secret numbers (using SSS and Homomorphism taught in the class), and add it to the provided GUI code (or to the GUI code that you write yourself). Recall, in SSS, we use only the first polynomial coefficient as secret.

Also analyze whether you can get some knowledge about the secret numbers from the shares. Specifically, does it withstand the frequency analysis attack? If no, how; if yes, suggest the changes you would do in the methodology to make it secure against this attack?

Extra work (2 bonus marks)

For bonus marks, you will use Ramp Secret Sharing (RSS) i.e. more than one polynomial coefficient (say *two* coefficients) as secret. Is it possible to perform the above homomorphic operations using RSS? If yes, redo the above analysis. If not, explain why.

Submission

You must submit the following via UAlbany Blackboard:

1) Source code along with the instructions to run it.
2) A pdf file containing your answers as mentioned above.
3) A video (of max 5 min) that shows the working of your program.