UNIVERSITY AT ALBANY
State University of New York

DEPARTMENT OF COMPUTER SCIENCE

ICSI-426/526 Cryptography – Spring 2023

Homework 3

Give out date: March 22, 2023
Due date/time: April 12, 2023, 11:59 p.m. **Total marks: 14**

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

Objective

The purpose of this assignment is to solidify concepts of Shamir Secret Sharing (SSS) Scheme and Homomorphic Encryption.

For Question 1, you can use pen and paper, take a clean picture (or type) and submit it. Question 2 is a programming-based question.

Question 1 [1 + 3 + 2 = 6 points]
This question must be completed in group of two students. Using (2, ***n***) SSS scheme, shares of two secret values have been created under modulo prime number (***p*** = 31). You will receive one pair of shares, i.e., share of each of the two secret values, and the other pair of shares will be given to your partner. Information about your partner and shares will be forwarded to you via email.
You are required to do the following (show your work in detail using pen and paper):

1. Try to **find secret values**, S1 and S2. Precisely, you will be taking the following steps:
    a. You are given: $(x_1, f_{S1}(x_1))$ and $(x_1, f_{S2}(x_1))$; and your partner is given: $(x_2, f_{S1}(x_2))$ and $(x_2, f_{S2}(x_2))$, where $f_{S1}(x_1)$ and $f_{S1}(x_2)$ are the shares of secret $S1$ at x_1 and x_2, respectively, and similarly, $f_{S2}(x_1)$ and $f_{S2}(x_2)$ are the shares of secret $S2$ at x_1 and x_2, respectively.
    b. If you have turned into an adversary, and your partner doesn't provide you their shares, show the steps you will take to find the secret numbers S1 and S2? If you can't find S1 and S2, provide adequate justification.
2. **Calculate the average** of respective shares of two secret values provided to you and your partner. You are required to submit the reconstructed average value of both the shares. If it is not possible to calculate the average using given shares, provide adequate justification. Precisely, you will be taking the following steps:
    a. Same as 1(a).
    b. You will compute the average (in encrypted form) (say $f_{S'}(x_1)$) of $f_{S1}(x_1)$ and $f_{S2}(x_1)$ under mod p, and your partner will compute the average ($f_{S'}(x_2)$) of $f_{S1}(x_2)$ and $f_{S2}(x_2)$ under mod p.

c. In the next step, you and your partner will collaborate with the two averaged shares, (x_1, $f_{S'}(x_1)$) and (x_2, $f_{S'}(x_2)$), and apply Lagrange interpolation formula on the two averaged shares to reconstruct the averaged secret, S_A, of the two secret values S1 and S2.
d. To verify your answer, take the following steps:
    i. With your share, (x_1, $f_{S1}(x_1)$), and your partner's share, (x_2, $f_{S1}(x_2)$), apply Lagrange interpolation formula to reconstruct the secret value S1.
    ii. With your share, (x_1, $f_{S2}(x_1)$), and your partner's share, (x_2, $f_{Ss}(x_2)$), apply Lagrange interpolation formula to reconstruct the secret value S2.
    iii. Now, calculate the average of S1 and S2, and compare it with S_A. If they are same, your answer is correct. If not, provide adequate justification.

3. **Calculate the multiplication** of respective shares of two secret values provided to you and your partner. You are required to submit the reconstructed multiplied value of both the shares. If it is not possible to calculate the multiplication using given shares, provide adequate justification. You will be taking the following steps:
    a. Same as Que 1(a).
    b. You will compute the multiplication (in encrypted form) (say $f_{S''}(x_1)$) of $f_{S1}(x_1)$ and $f_{S2}(x_1)$ under mod p, and your partner will compute the multiplication ($f_{S''}(x_2)$) of $f_{S1}(x_2)$ and $f_{S2}(x_2)$ under mod p.
    c. In the next step, you and your partner will collaborate with your two multiplied shares, (x_1, $f_{S''}(x_1)$) and (x_2, $f_{S''}(x_2)$), and apply Lagrange interpolation formula to reconstruct the multiplication of the two secret values, S_M.
    d. To verify your answer, take the following steps:
        i. Repeat 2(d)i.
        ii. Repeat 2(d)ii.
        iii. Now, calculate the multiplication of S1 and S2, and compare it with S_M. If they are same, your answer is correct. If they are not same, provide adequate justification.

Hints: All the calculations must be under modulo prime number ($\boldsymbol{p} = 31$).

Question 2 [4 + 4 = 8 points]

1. Implement (3, 5) Shamir's Secret Sharing (SSS) scheme (both share preparation and reconstruction) for images. You need to show the working of your program by creating shares of an image and show the image shares and the reconstructed image as output. You need to operate on image data, **leaving the header intact**. You can use any BMP image of your choice. Note that the header length in BMP file format is 54 bytes.

2. Next, you are required to demonstrate the **homomorphic properties of SSS** scheme using the image downscaling operation. In a homomorphic encryption scheme, computations performed on encrypted data, when decrypted, generates the same value as when the same computations are performed on the plaintext.

   The downscaling operation takes an input image and produces an image whose width and height are less than the input image. You need to implement downscaling by a factor of 2. This means that both the width and height of your output image will be exactly half of the input image.

   You are required to do the following steps:

1) Take an input image I of certain resolution and use the downscale method on this image to obtain the downscaled image I_o. In the downscale method, each pixel of I_o is the average of four pixels of I. For example, pixel (0,0) of I_o is the average of pixels (0,0), (0,1), (1,0), (1,1) of I; pixel (1,0) of I_o is the average of (2,0), (2,1), (3,0), (3,1) of image I. As a result, the resolution of I_o will be half of I in both x and y dimensions.
2) Create 3 shares (denoted by I_1, I_2, I_3) of I using the SSS scheme.
3) Perform the downscale method on all the three shares and obtain the downscaled shares (denoted by I_{s1}, I_{s2}, I_{s3}).
4) Pick any 2 downscaled shares, i.e. from I_{s1}, I_{s2}, I_{s3}, and reconstruct the downscaled plaintext image (denoted by I_s).
5) Compute the mean average error between the two images, I_o and I_s, using the following equation:

$$\text{MAE} = \sum_{j = 1 \text{ to } w \times h} (|I_o(j) - I_s(j)|)$$

where w and h are image width and height.
6) Show the output of each step and report your observations.

Question 3 [2 Points]
This question is for those who wish to choose Option 3 for their grading. You will repeat what you did in Question 2.2, except that you **don't preserve header** information. You need to show the working of your program by creating shares of an image and show the image shares and the reconstructed image as output. You can use the same BMP image that used in Que 2.2.

Submission

You must submit the following via UAlbany Blackboard:

(a) Source code along with the instructions to run it for Question 2 (and 3, as applicable).
(b) A pdf file containing your code for Question 2.
(c) A pdf file containing answers to Questions 1 and 2 (and 3, as applicable). For Question 1, write your partner's name and share details.
(d) A video link (of max 5 minutes) that shows the working of your program.