Spring 2023 - ICSI 526
Homework 3

Written by Jacob Clouse

(Partner 1: Jacob Clouse
Partner 2: Luna Dagci)

April 8, 2023

Contents

1 Question 1

1.1 Trying to find secret values - ASK PRADEEP

I am Partner 1 in this instance and my shares are: (37,9) and (37,18), with our prime being 31. These are two different shares from two different equations, and we know that the original cipher is a (2, n) SSS

scheme. This means we need 2 shares (k) at least in order to retrieve it, but we have only 1 for each (k - 1). We know that from our text that we can not find the original value from this, but lets look deeper. To retrieve our original secret (a_0), we use the formula: (f(x) = (a_0 * a_1x) mod p). We would get to this formula by using the Lagrange Interpolation formula (L(x) = y_1 * (x - x_2) / (x_1 - x_2) + y_2 * (x - x_1) / (x_2 - x_1) mod q) in conjunction with our 2 shares.

Lets use (37,9) to try and fill in as much as we can with the formula:
L(x) = 9 * (x - x_2) / (37 - x_2) + y_2 * (x - 37) / (x_2 - 37) mod q
This leaves too many potential solutions that are all equally likely but lead to drastically different formulas and results.

For example, if we choose x2 = 10 and y2 = 25, we see our formula develop like this:
f(x) = 9 * (x - 10) / 27 + 25 * (x - 37) / (-27) = 25 - (x - 10) / 3 - (x - 37) or (-2x + 96) mod q

Or we can choose x2 = 20 and y2 = 15 and have our formula look like:
f(x) = 9 * (x - 20) / 17 + 15 * (x - 37) / (-17) = 15 - 3(x - 20) / 17 - 5(x - 37) / 17 or (-8x + 351) mod q

How do we know which one is correct? Each one is equally valid, and we can not know for sure, this

is why it is impossible to find the secret without having k shares. This is why Shamir's Secret Sharing is secure to use.

1.2 Finding Average – ASK PRADEEP – NEED HELP ON LAST PART

For the average, I had to take my two shares and average the y coordinates together, my partner had to do the same with their shares and then we could feed the result into the Lagrange Formula to get our f(0) value.
Again, as Partner 1, my two shares were: (37,9) and (37,18). So I had to average 9 and 18, here is **my** math:

$$\left(\tfrac{9+18}{2}\right) \bmod 31 \rightarrow \left(\tfrac{27}{2}\right) \bmod 31 \rightarrow (13.5) \bmod 31 \rightarrow \mathbf{13.5}$$

Luna was Partner 2 and her two shares were: (38,24) and (38,2). She had to average 24 and 2, here is **her** math:

$$\left(\tfrac{24+2}{2}\right) \bmod 31 \rightarrow \left(\tfrac{26}{2}\right) \bmod 31 \rightarrow (13) \bmod 31 \rightarrow \mathbf{13}$$

We now had our two averaged shares: (37,13.5) and (38,13). We plugged them into our Lagrange Formula and got the following:

$$f(x) = y_1 * \left(\tfrac{x-x_2}{x_1-x_2}\right) + y_2 * \left(\tfrac{x-x_1}{x_2-x_1}\right) \bmod 31 \rightarrow f(x) = 13.5 * \left(\tfrac{x-38}{37-38}\right) + 13 * \left(\tfrac{x-37}{38-37}\right) \bmod 31$$

Solving for f(0):

$$f(0) = 13.5 * \left(\tfrac{0-38}{37-38}\right) + 13 * \left(\tfrac{0-37}{38-37}\right) \bmod 31 \rightarrow f(0) = 13.5 * \left(\tfrac{-38}{-1}\right) + 13 * \left(\tfrac{-37}{1}\right) \bmod 31$$

$$f(0) = 13.5 * 38 + 13 * (-37) \bmod 31 \rightarrow f(0) = 513 + (-481) \bmod 31 \rightarrow f(0) = 32 \bmod 31 \rightarrow f(0) = 1$$

f(0) = **1** for the averaged formula, we just need to work backwards and see if we can get the original values. But we see that when we plug in our values into the original formula, we are left with a problem:

$$f(x) = (a_0 * a_1 x) \bmod p \rightarrow 13.5 = (1 * a_1(37)) \bmod 31$$

We need to find out what a_1 is here. If

2 Question 2

Question 2 is solved by...