Spring 2023 - ICSI 526
Homework 3

Written by Jacob Clouse

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

April 14, 2023

Contents

1 Question 1

1.1 Trying to find secret values

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:

$$f(37) = (a_0 + a_1 * 37) \bmod 31$$

Lets use (37,9) to try and fill in as much as we can with the formula. Lets say we have $a_0 = 3$ and $a_1 = 1$, then we have:

$$f(37) = (3 + 1 * 37) \bmod 31 \rightarrow 9$$

Or lets say we have $a_0 = 34$ and $a_1 = 1$, then we have:

$$f(37) = (34 + 1 * 37) \bmod 31 \rightarrow 9$$

Or lets say we have $a_0 = 59$ and $a_1 = 2$, then we have:

$$f(37) = (59 + 2 * 37) \bmod 31 \rightarrow 9$$

How do we know which one is correct? They all give us the same answer and each one is equally likely. This is why we can't know for sure and is why it is impossible to find the secret without having k shares.

1.2 Finding Average

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 initially thought I had to just average 9 and 18, but that will lead to a decimal. So i had to use the forumla: (9+18)*2^{-1} mod 31. Here is **my** math:

$$(9+18)*2^{-1} \bmod 31 \rightarrow (27)*16 \bmod 31 \rightarrow 432 \bmod 31 \rightarrow \mathbf{29}$$

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: (37,29) and (38,13). We plugged them into our Lagrange Formula and got the following:

$$f(x) = y_1 * \left(\tfrac{x-x_2}{x_1-x_2}\right) + y_2 * \left(\tfrac{x-x_1}{x_2-x_1}\right) \bmod 31 \rightarrow f(x) = 29 * \left(\tfrac{x-38}{37-38}\right) + 13 * \left(\tfrac{x-37}{38-37}\right) \bmod 31$$

$$f(0) = 29 * \left(\tfrac{0-38}{37-38}\right) + 13 * \left(\tfrac{0-37}{38-37}\right) \bmod 31 \rightarrow f(0) = 29 * \left(\tfrac{-38}{-1}\right) + 13 * \left(\tfrac{-37}{1}\right) \bmod 31$$

$$f(0) = 29*38 + 13*(-37) \bmod 31 \rightarrow f(0) = 1102 + (-481) \bmod 31 \rightarrow f(0) = 621 \bmod 31 \rightarrow f(0) = 1$$

f(0) = 1 for the averaged formula, we just need to work backwards and see if we can get the original values. We find secret 1 with shares (37,9) and (38,24):

$$f(x) = 9 * \left(\tfrac{x-38}{37-38}\right) + 24 * \left(\tfrac{x-37}{38-37}\right) \bmod 31$$

$$f(0) = 9 * \left(\tfrac{0-38}{37-38}\right) + 24 * \left(\tfrac{0-37}{38-37}\right) \bmod 31 \rightarrow f(0) = 9 * \left(\tfrac{-38}{-1}\right) + 24 * \left(\tfrac{-37}{1}\right) \bmod 31$$

$$f(0) = 9*38 + 24*(-37) \bmod 31 \rightarrow f(0) = 342 + (-888) \bmod 31 \rightarrow f(0) = -546 \bmod 31 \rightarrow f(0) = 12$$

f(0) for secret 1 is 12. We find secret 2 with shares (37,18) and (38,2):

$$f(x) = 18 * \left(\tfrac{x-38}{37-38}\right) + 2 * \left(\tfrac{x-37}{38-37}\right) \bmod 31$$

$$f(0) = 18 * \left(\tfrac{0-38}{37-38}\right) + 2 * \left(\tfrac{0-37}{38-37}\right) \bmod 31 \rightarrow f(0) = 18 * \left(\tfrac{-38}{-1}\right) + 2 * \left(\tfrac{-37}{1}\right) \bmod 31$$

$$f(0) = 18*38 + 2*(-37) \bmod 31 \rightarrow f(0) = 684 + (-74) \bmod 31 \rightarrow f(0) = 610 \bmod 31 \rightarrow f(0) = 21$$

f(0) for secret 2 is 21. Now we take these numbers and can feed them back into our average formula: (12+21)*2^{-1} mod 31. Here is **my** math:

$(12 + 21) * 2^{-1} \bmod 31 \rightarrow (33) * 16 \bmod 31 \rightarrow 526 \bmod 31 \rightarrow \mathbf{1}$

$1 = 1$, but why? It is because we kept proportions using scalar multiplication (the inverse modulus 2 and the normal averaging of luna's shares). This ensured that we kept everything in line and got the same average in the end.

1.3 Finding Multiplication – ASK PRADEEP – NEED HELP ON LAST PART

To calculate the multiplication value, I had to multiply my two share y values and then find mod 31 of the product. 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 multiply 9 and 18, here is **my** math:

$(9 * 18) \bmod 31 \rightarrow (162) \bmod 31 \rightarrow \mathbf{7}$

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

$(24 * 2) \bmod 31 \rightarrow (48) \bmod 31 \rightarrow \mathbf{17}$

We now had our two multiplied shares: (37,7) and (38,17). We plugged them into our Lagrange Formula and got the following:

$$f(x) = y_1 * \left(\frac{x-x_2}{x_1-x_2}\right) + y_2 * \left(\frac{x-x_1}{x_2-x_1}\right) \bmod 31 \rightarrow f(x) = 7 * \left(\frac{x-38}{37-38}\right) + 17 * \left(\frac{x-37}{38-37}\right) \bmod 31$$

Solving for f(0):

$$f(0) = 7 * \left(\frac{0-38}{37-38}\right) + 17 * \left(\frac{0-37}{38-37}\right) \bmod 31 \rightarrow f(0) = 7 * \left(\frac{-38}{-1}\right) + 17 * \left(\frac{-37}{1}\right) \bmod 31$$

$$f(0) = 7 * 38 + 17 * (-37) \bmod 31 \rightarrow f(0) = 266 + (-629) \bmod 31 \rightarrow f(0) = -363 \bmod 31 \rightarrow f(0) = 9$$

f(0) = **9** for the multiplication formula, we just need to work backwards and see if we can get the original values. We from 1.2 that secret 1 = 12 and secret 2 = 21. But we see that when we plug in these values into the original formula, we are left with a problem:

$(12 * 21) \bmod 31 \rightarrow 252 \bmod 31 \rightarrow 4$

These are not the same and this is because we didn't maintain the proportions with scalar multiplication (like we did in 1.2). This means that the aspects haven't been preserved by homomorphism.

2 Question 2

Question 2 is solved by...