Spring 2023 - ICSI 526
Homework 3

Jacob Clouse

April 6, 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(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)) 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)
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

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

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.

2 Question 2

Question 2 is solved by...