CS 5158/6058 Data Security and Privacy, Spring 2018
Homework 5

Instructor: Dr. Boyang Wang

Due Date: 04/19/2018 (Thursday), 11:59pm.
Format: Please **type** your solutions and submit a pdf of your solutions in Blackboard.
Total Points: 6 points

Problem 1 (3 points). Assume the current blockchain in the Bitcoin network has $1,234$ blocks, the next block will be added to the blockchain should be No. 1235. In addition, assume the hashing power of the entire Bitcoin network is $1,000,000$ hashes per second. If Alice would like to mine bitcoins with her laptop, and she can compute $5,000$ hashes per second with this laptop

1. What is the probability that **both** block No. 1235 and block No. 1236 in the blockchain will be added by Alice?
2. If Alice increases her hashing power to $10,000$ hashes per second and the hashing power of the entire Bitcoin network increases to $2,000,000$ hashes per second, will Alice have a higher probability to add the next block into the blockchain?

Problem 2 (3 points). Assume you have a secret message $m = 34$ you would like to share with 3 users, Alice, Bob and Charlie using Shamir Secret Sharing. Assume there is an attacker who can compromise at most 2 users. Assume you choose a 2-degree polynomial

$$y = ax^2 + bx + c = 12x^2 + 21x + 34$$

where $a = 12$, $b = 21$ and $c = m = 34$. And you will give (x_1, y_1) to Alice, (x_2, y_2) to Bob, and (x_3, y_3) to Charlie. If you choose $x_1 = 1$, $x_2 = 2$, and $x_3 = 3$,

1. Compute y_1, y_2 and y_3
2. If you choose $x_1 = 0$, compute y_1 based on the above polynomial, and give point (x_1, y_1) to Alice, what is the potential privacy leakage?
3. If you can share your secret message with 20 users with Shamir Secret Sharing, and an attacker could compromise at most 18 users. In order to recover your secret message, you need to contact at least 19 users, then what is the degree of the polynomial you should use in Shamir Secret Sharing?