Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 3
February 23, 2015
Due: March 9, 2015

Problem Set 2

This problem set is due on *Monday, March 9* at **11:59 PM**. Please note our late submission penalty policy in the course information handout. Please submit your problem set, in PDF format, **on Stellar**. *Each problem should be in a separate PDF.* Have **one and only one group member** submit the finished problem writeups. Please title each PDF with the Kerberos of your group members as well as the problem set number and problem number (i.e. *kerberos1_kerberos2_kerberos3_pset1_problem1.pdf*).

You are to work on this problem set with your assigned group of three or four people. Please see the course website for a listing of groups for this problem set. If you have not been assigned a group, please email `6.857-tas@mit.edu`. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration.

Homework must be submitted electronically! Each problem answer must appear on a separate page. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for LaTeX and Microsoft Word on the course website (see the *Resources* page).

Grading: All problems are worth 10 points.

With the authors' permission, we may distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this in your profile on your homework submission.

Our department is collecting statistics on how much time students are spending on psets, etc. For each problem, please give your estimate of the number of person-hours your team spent on that problem.

Problem 2-1. Secret Sharing

The Shamir secret-sharing scheme shows how to share a secret among n people, so that any t people are able to reconstruct the secret from their shares, but a combination of any fewer than t shares is insufficient to reconstruct the secret. (Here t and n are integer parameters, with $1 \leq t \leq n$.)

In this problem, you will show how to implement more complicated reconstruction requirements.

(a) (Easy.) Using the Shamir secret sharing scheme, show how to require that A AND B must both cooperate to reconstruct the secret. Here A and B are two parties receiving shares of the secret.

(b) Show that you can create a secret sharing scheme that shares a secret with a reconstruction requirement defined by a given monotone circuit (a boolean circuit with n inputs x_1, x_2, …, x_n whose input x_i is **1** if and only if party i is collaborating in the secret reconstruction), and whose gates are restricted to AND, OR, and t'-out-of-n' gates. Argue that a combination of parties satisfying the reconstruction requirement will be able to reconstruct the secret, while a combination of parties not satisfying the reconstruction requirement will be unable to reconstruct the secret.

(c) Describe a scheme that shares a secret according to the following reconstruction requirement:

(Professor Rivest) OR ((2 out of 3 TA's) AND (10 out of 20 students))

Problem 2-2. Hash functions

Assume that $h : \{0,1\}^n \rightarrow \{0,1\}^d$ is a hash-function. For each of the following questions provide an answer and a proof.

(a) In ROM, we need to hash about $2^{d/2}$ x-values and search for repeated outputs in order to find even one collision. How many collisions do we expect to find if we hash $c \cdot 2^{d/2}$ x-values for $1 \leq c \leq 2^{d/2}$?

(b) We define $h' : (\{0,1\}^n)^2 \to \{0,1\}^d$ by $h'(x,y) = h(x \oplus y)$. If h is a one-way function, is h' one-way as well?

If $h'' : (\{0,1\}^n)^2 \to \{0,1\}^d$ is defined as $h''(x,y) = h(x \wedge y)$, explain why the situation regarding the one-wayness of h'' is not the same as for the one-wayness of h'. (You do not need to provide a proof of whether h'' is one-way or not.)

(c) We define $h' : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^d$ by $h'(x,y) = h(x) \oplus y$. If h is collision resistant, is h' collision resistant as well?

(d) We define $h' : (\{0,1\}^n)^2 \to \{0,1\}^d$ by $h'(x,y) = h(x) \oplus h(y)$. If h is weak-collision resistant, is h' weak-collision resistant as well?

Problem 2-3. Cryptocurrency

Your task is to build a 6.857Coin miner using the blockchain API described here:

`http://6857coin.csail.mit.edu/`

You do not need to turn in any code for the following problems.

(a) Add a block containing your group number as block number 2 in a length-2 chain containing your new block and the genesis block. What is your block's hash?

(b) Ensure there is a block containing your group number in the longest block chain (as measured on the problem set due date on March 9 at 11:59 PM). What is your block's hash? Describe your approach. How many "confirmations" did you wait for in order to feel confident that your block would appear in the longest chain?

(c) Estimate the cost (in dollars) of reversing a Bitcoin transaction with 6 confirmations. Consider that the chain is always growing. State your assumptions regarding the current hash rate and difficulty and the cost of mining.

(d) **Optional:** What did you do with your $100 worth of Bitcoin?

(e) **Extra credit:** Mine as many blocks as you can! The groups with the most mined blocks will receive extra credit:

- 1st place: 6 points extra credit
- 2nd place: 4 points extra credit
- 3rd place: 3 points extra credit
- 4th place: 2 points extra credit

Only blocks in the longest chain (as measured on March 9 at 11:59 PM) will be considered. Late submissions are not eligible for extra credit. You may use any strategy, as long as you follow the rules described on the 6.857Coin webpage. You may form mining pools as described on the webpage, but the rewards will be split among the groups in the pool. For example, if your pool consists of 3 groups and mines the most blocks, then each group in the pool will receive 2 points of extra credit.