Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ron Rivest

Handout 11
April 23, 2012
Due: May 4, 2012

Problem Set 5

This problem set is due as an email to the course staff, at `6.857-staff@mit.edu`, on *Friday, May 4* by **11:59 PM**. Please note that no late submissions will be accepted.

You are to work on this problem in a group of 4. (Or possibly 3– but I reserve the right to add a member to any group of 3) Please email the TAs with your group composition by 11:59 PM the day the PSet is assigned! TAs will assign remaining students to random groups the day after the PSet is assigned. 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! Submissions should be in pdf form, with the document named by each team member's last name appended. 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 will 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 the email used to turn in the submission.

Problem 5-1. Digital signatures

When you send an email, it is transmitted through many servers, each of which can potentially modify your message. Luckily we can use public key cryptography to sign our messages, and thereby allow others to verify their integrity. We can also use PKI (like OpenPGP) to safely distribute our public keys.

Figure out how to send a digitally signed message using your current mail client to your other project team members. Verify the digitally signed messages received from your project team members. If your current mail client doesn't support signatures, you can download and use Thunderbird with the Enigmail extension.

(a) Write up the steps you needed to do the above. (Include a description of your mail client, etc.) What certificates did you have to work with?

(b) Have **each member** of your team send a digitally signed message to 6857-tas. (Note: the staff needs to be able to verify your signature for you to get credit for this problem! You may need to get a certificate to them somehow. We suggest posting your certificates to a PGP keyserver such as pgp.mit.edu.)

Problem 5-2. Elliptic curves Let E be the elliptic curve defined by the equation

$$y^2 = x^3 + 1 (\text{mod } 11).$$

(a) List all of the points in the elliptic group defined by this curve (including the point at infinity). For convenience in this part and the next, you may code a point as `xy` where both x and y are either digits or X representing "ten". For example, one point on the curve is "`X0`". Use "∞" or "`0`" to represent the identity (point at infinity).

(b) Give the group operation table.

Problem 5-3. Zero-day attacks

(a) Define a "zero-day attack".

(b) You have just been hired by the Department of Internet Security (a new cabinet level department in the U.S. government) and given an annual budget of $100M to reduce the incidence and severity of zero-day attacks.

Write a proposal for how best to spend your budget. Prioritize the elements of your proposal, and don't propose spending on more than five elements. (You may wish to indicate how much funding to allocate to each element of your proposal.)

The budgeting process is very competitive. Give the best arguments you can as to why your chosen program elements should be funded.