6.897: Selected Topics In Cryptography

Canetti and Rivest

Handout 1: General Information

5 Thursday 2004

Lectures and Office Hours

Lectures are:

- Thursdays, 11am-12:30, in 36-155, and
- Fridays, 2:30–4:00, in 36-112.

Office hours are by appointment.

Prerequisites

We assume that you have taken 6.875 Introduction to Cryptography, or have equivalent introduction to theoretical cryptography (see the instructors if you have questions about your background).

Course materials

There is no text for this course. We will make all materials for this course available on-line on our course web site:

http://theory.lcs.mit.edu/classes/6.897/spring04

Mailing lists

There are two course mailing lists. The first, 6897s04-staff@lists.csail.mit.edu, reaches only the course staff. The second, 6897s04-students@lists.csail.mit.edu, reaches all staff and students. Please feel free to contact the staff via the first list, and your fellow students via the second.

Grading Policy

There will most likely be (approximately) four homework assignments. There will be no quizzes or finals. Students will "scribe" lectures in rotation. (Scribe notes must be written up in latex, and be reasonably "polished.")

The final grade will be computed using the following weights:

• Homework: 60%

• Scribing: 30%

• Participation in class: 10%.

Homeworks

We require that all homework solutions be typed up in latex. Hand-drawn diagrams are permitted.

Collaboration Policy

We strongly encourage collaboration. We do not expect you to be able to solve every homework problem on your own. We do, however, expect you to write up your own solution to every problem even if the solution is the result of a collaborative effort. To repeat: each person must write up their solutions separately. Also, in your write-up please credit the people with whom you worked. Also, please note on your homework which sources you used for each problem.

Contact Information

- Lecturer: Ron Rivest, NE43-324, x3-5880, rivest@mit.edu
- Lecturer: Ran Canetti, NE43-324, x3-5096, canetti@theory.lcs.mit.edu
- Course Secretary: Be Blackburn, NE43-322, x3-6098, be@theory.lcs.mit.edu