Course Information

Lecturer:	Professor Ronald L. Rivest NE43-324, 3–5880, `rivest@mit.edu` Office Hours by appointment
Teaching Assistants:	Kevin Fu NE43-520, `fubob@mit.edu` Office Hours: Monday, Wednesday 4-5pm or by appointment
	abhi shelat NE43-313, `abhi@mit.edu` Office Hours: Tuesday, 4-6pm
Secretary:	Be Hubbard NE43-322, 3–6098 `be@theory.lcs.mit.edu`
Staff Email	`6.857-staff@mit.edu`

1 Prerequisites

The prerequisites for the course are 6.033 (*Computer System Engineering*) and 6.042J (*Mathematics for Computer Science*). It is recommended that students have had 6.046J and experience with modular arithmetic.

2 Units

This is a 12-unit (3-0-9) U-level course intended primarily for seniors and first-year graduate students. (Graduate students will *not* receive H–credit for this class.)

3 Lectures

Lectures will be held in Room 6-120 on Tuesdays and Thursdays from 2:30 to 4:00 P.M. A schedule of topics will be posted on the Web page.

4 Handouts and course notebook

Handouts will be available at the beginning of lecture or from the class file cabinet outside room NE43-311. If you take the last copy of a handout, please inform the course secretary so that more copies can be made. Handouts will be made available online (if possible) through the Web page.

5 The class on line

We have a Web page at

`http://web.mit.edu/6.857/www/`

We also have a course locker on Athena. In order to access the locker type `attach 6.857` at your Athena prompt and then `cd /mit/6.857`.

There is also a mailing list `6.857-students@mit.edu` which will be used to send out last-minute announcements. Please check your e-mail regularly if possible.

We will use the Web page and the Athena course locker to make handouts and lecture notes available on line.

6 Textbook

There is no required textbook for this course, as the material covered is broad and usually very new. There will, however, be reading handouts. Also, a list of recommended books is posted online.

7 Groups and Collaboration

You are to work on the homework problems, the scribe notes, and the final projects in groups of three or four (not one, two, five). Get your group organized as soon as you can, and let the staff know the composition of your group. If you have trouble getting a group organized, contact the staff.

No collaboration is permitted on the take–home midterm quiz.

8 Homework

Problem sets will be assigned on approximately a weekly basis. They will be handed out on Thursday and be due on the following Thursday. Late homework will **not** be accepted. If in doubt, turn your problem set in early at the course secretary's office.

You are to work on problem sets by group – one problem set will be turned in by each group, and one grade will be given for each problem set. You *must* work in groups; homeworks turned in by individuals, pairs, pentuples, etc. will not be accepted. Be sure that *you* understand and approve the solutions turned in to *each* problem.

You may collaborate with individuals from other groups, but your solutions must be written up only by individuals from your group. If you do collaborate, acknowledge your collaborators in the write-up for each problem. If you obtain a solution with help (e.g., through library work), acknowledge your source, and write up the solutions on your own. Plagiarism and other anti-intellectual behavior will be dealt with severely.

9 Lecture Notes

Each group will have to scribe one lecture of the course. Scribe notes are due one week from the date of the lecture being scribed. These scribe notes will be graded on the initial version submitted, and we expect them to be of the highest quality.

The TAs will edit/revise the notes and post them on the Web. The grade will depend in part on how much effort is required by the TAs to edit and revise the submitted notes.

Once you have formed your homework group, you can sign up for a lecture date either in class or via email to `6.857-staff@mit.edu`.

We would like the notes to be written in LaTeX. See the TAs or the Web site for assistance with LaTeX if necessary. (However, figures can be prepared separately...)

If you are scribing, see the lecturer after class to resolve any questions you may have had about the lecture, and to get any useful material he may have to share with you while preparing the notes. It is OK to use notes from previous years as a starting point, as long as credit is given.

10 Term project

Students will be responsible for a term project. You must work on the term project in your group of three or four people.

The nature and the topic of the project is your choice, although it needs the teaching staff approval. We will maintain a Web page of potential project topics and provide sample proposals later in the year. Basically, as long as it is about network and/or computer security and is sufficiently interesting, it is OK.

A one or two-page written proposal for the project (with initial bibliography) is due no later than in class on November 8th. It is advisable to get going early; we will gladly accept proposals before then. This proposal is not graded, but gives us a chance to review and approve your project proposal, and to suggest references that you may have overlooked.

The final written term project is due in the last class December 11th.

The last three classes (December 4th, 6th, and 11th) will be devoted to short presentations of each term project. Prior to presenting your work in class, you will be asked to give a practice presentation to the course staff.

11 Grading

The class will have weekly problem sets, a take–home midterm exam, lecture note scribing, and a final project. Grading will be as follows: 40% for the problem sets, 25% for the midterm, 5% for scribing, and 30% for the final project. There is *no* final exam.