Course Information

Lecturer:	Professor Ronald L. Rivest NE43-324, 253–5880, `rivest@mit.edu` Office Hours by appointment
Teaching Assistants:	Kevin Fu NE43-520, 253–7436, `fubob@mit.edu` Office Hours: Wednesday 3-5pm
	Thien-Loc Nguyen NE43-369, 253–1499, `nguyentl@theory.lcs.mit.edu` Office Hours: Tuesday 4-6pm
Secretary:	Be Blackburn NE43-322, 253–6098 `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 (Introduction to Algorithms) 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.

Unlike previous years, we will not provide lecture notes except for a few lectures covering bleeding-edge material. You can find lecture notes from previous years on the class Web page and in the Barker Engineering Library.

4 The class online

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-public@mit.edu` which will be used to send out last-minute announcements. You are welcome to send email to this list when you find relevant material useful to the rest of the class. We will use the Web page and the Athena course locker to make handouts and lecture notes available online.

5 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, when possible, through the Web page.

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. We will maintain a list of recommended books online. In addition, we have reserved several security books and a course reader for you in the Barker Engineering Library (building 10, 5th floor).

7 Homework

We will distribute six problem sets on approximately a weekly basis. They will generally 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.

There will be both individual and group homework assignments. You are to work on group problem sets and final projects in groups of three or four. 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. Get your group organized as soon as you can, and email the composition of your group to the teaching staff.

If you have trouble finding a group, contact the staff. To prevent your group from falling apart, make sure everyone participates and that you all communicate on a regular basis. If you have a problem with a groupmate, talk to your groupmate. If you are unable to make a compromise or your group does fall apart, talk to the staff.

Occasionally we will assign individual homework problems. The policy on individual homework appears in Section 10.

In lectures presenting very new material, we may ask for volunteers to scribe the lecture notes. A group which scribes a lecture will have their lowest problem set grade replaced with the grade awarded to the scribe notes. So make sure your scribe grade is not your lowest grade....

8 Tests

We will have two in-class quizzes (October 10 and November 26) and one take-home midterm (distributed October 24, due October 31).

Quizzes will test your knowledge of material from lectures, problem sets, and readings. The midterm will contain open-ended questions to test your application of course material to solve complex problems.

There is *no* final exam.

9 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 approval of the teaching staff. We will maintain a Web page of potential project topics and provide sample proposals later in the

year. We will generally approve topics about network and/or computer security as long as it is sufficiently interesting.

A one or two-page written proposal for the project with an initial bibliography is due no later than in class on October 24th. It is advisable to get going early; we will gladly accept proposals before the deadline. This assignment 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 on December 10th.

The last three classes (December 3rd, 5th, and 10th) 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.

10 Collaboration and plagiarism

No collaboration is permitted on the take-home midterm or the in-class quizzes. All tests are open book and open notes. You may not discuss midterm material online, with your GRT, with your mother, etc. It's a completely individual assignment. We encourage you, however, to prepare for quizzes by discussing course material with your classmates.

You may collaborate with individuals from other groups in problem sets, but your solutions must be written up only by individuals from your group. For individual homework assignments, you may discuss the problem set material with others. You must, however, write up your solutions independently.

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 or a friend), acknowledge your source and write up the solutions on your own. In most of your solutions, we will expect to see citations.

You may use any reference material to complete your homework assignments, including material on the Internet and course readers from previous years. Again, we cannot emphasize enough that you must cite all your sources properly. You must remove any possibility of someone else's work from being misconstrued as yours. Plagiarism and other anti-intellectual behavior will be dealt with severely. Figure 1 illustrates our policy on collaboration and plagiarism.

Figure 1: Never misrepresent someone else's work as your own. It must be absolutely clear what material is your original work[1]. Plagiarism and other anti-intellectual behavior will be dealt with severely. Radix comic copyright Ray and Ben Lai.

[1] `http://story.news.yahoo.com/news?tmpl=story&u=/nm/20020828/wl_canada_nm/canada_arms_comicbook_col_2`

11 Grading

The class will have six problem sets, a take-home midterm, two quizzes, and a final project. Grading will be as follows: 35% for the problem sets, 10% for quizzes, 25% for the midterm, and 30% for the final project.

Figure 2: Security in NE43.