# Course Information

| | |
|---|---|
| Lecturers: | Professor Ronald L. Rivest |
| | 32-G692, 253–5880, `rivest@mit.edu` |
| | Office Hours by appointment |
| Teaching Assistant(s): | Jayant Krishnamurthy |
| | `jayant@mit.edu` |
| | Office Hours: TBA |
| Secretary: | Be Blackburn |
| | 32-G675A, 253–6098 |
| | `be@csail.mit.edu` |
| Staff Email: | `6857-staff@mit.edu` |
| TA Email: | `6857-tas@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 6.006 or 6.046J (*Introduction to Algorithms*) and experience with modular arithmetic. You may take the course without having the pre-requisites, *if* you can convince the TAs that you have equivalent background.

## 2  Units

This is a 12-unit (3-0-9) H-level course intended primarily for seniors and first-year graduate students. It fits within the Computer Systems and Architecture Engineering Concentration. Graduate students will receive H-credit for this class.

## 3  Lectures

Lectures will be held in Room 2-105 on Mondays and Wednesday from 11:00AM to 12:30PM. A schedule of topics will be posted on the class web site; you can also get a sense of the topics to be covered by looking at the web sites from previous years. We will not provide lecture notes with the exception of a few lectures covering bleeding-edge material. Notes from previous years are on the class web site.

## 4  The class online

The course web site is online at:

   `http://courses.csail.mit.edu/6.857/`

Handouts, assignments, and announcements will be available online only (except for this first handout, which is also available in dead-tree format).

The web site includes an online registration form (click: *Course Registration*). You **must** register for the course by completing this form no later than Friday, February 6th. Once you have registered, you will be automatically subscribed to the course mailing list:

```
6857-students [at] mit.edu
```

We will use this list to make important class announcements. Notify the TAs if you wish to be removed from this list.

# 5   Textbook

There is no required textbook for this course. A list of recommended books will be made available. See the *References* page on the course web site for the relevant bibliographic information.

# 6   Groups

6.857 is a group-oriented course. Students will work in groups on both homeworks and the final project.

For the first three homeworks, you must work in groups of three or four per group as assigned by the 6.857 staff. For the later homeworks, and for the final project, you may work in groups of your own choosing. You may re-organize your groups at any time, with permission of the TA(s). It is not expected that your project group will be the same as your homework group(s), although that is perfectly OK.

The final project team should be determined by the date given below. Students who need help finding a project group or group for the later homeworks should contact the staff. To keep groups running smoothly, students should ensure that their fellow members are actively participating and should communicate regularly. Students who cannot resolve group problems should contact the TA(s). If necessary, groups can be dissolved and reformed, with permission of the TA(s).

# 7   Homework

We will distribute approximately five problem sets on approximately a biweekly basis. They will generally be handed out on Monday and be due two weeks later.

Homework submissions are to be sent to the TAs at `6857-hw@mit.edu` in either PostScript, PDF, or MS Word format. Homework templates will be available on the course web site. For homework involving non-trivial mathematics, students are strongly encouraged to use LaTeX to typeset their answers. Homework that is difficult for the graders to read will lose points.

Late homework will **not** be accepted. If in doubt, turn your problem set in early. Solutions will be distributed with corrected homework—hopefully within a week of being collected.

Generally, homework must be done in groups. You are to work on group problem sets and final projects in groups of three or four (preferably three). 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. As noted above, the initial organization into groups for the first three problem sets will be established by the staff, but you may organize your own groups for the later homeworks and for the final project.

We may occasionally assign homework that you must answer individually; see Section 11 for the policy governing these assignments.

# 8   Tests

We will have one in-class quiz on Monday, April 6, 2009. There is *no* final exam. The quiz will test your knowledge of material from lectures, problem sets, and readings.

# 9 Final project

Students will be responsible for a final project. You must work in a 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. See the *Term Projects* page on the course web site for a list of topics from previous years, sample proposals, and additional project-related resources. We will generally approve interesting topics about network and/or computer security.

It is advisable to get started early; we will gladly accept proposals before the deadline. Early submission gives us a chance to review and approve your project proposal, and to suggest references that you may have overlooked.

Important dates for the project:

- By Monday, February 23 - Students individually submit one-page project ideas via e-mail. These ideas will be posted on the course web site. After reviewing their classmates' project ideas, students will form three or four person teams. These teams need not be the same as homework groups.

- By Wednesday, April 1 - Turn in team composition and a multi-page project draft and bibliography.

- April 13-17 - During this week, each project group will meet with a TA to review their progress.

- May 6, 11, and 13 - Groups will present short talks on their projects in class.

- Wednesday, May 13 (last class)- Written projects are due.

# 10 Grading

Grades are:

45% for the problem sets
20% for quiz
35% for the final project

# 11 Collaboration and plagiarism

No collaboration is permitted on the in-class quiz. All tests are open book and open notes. We encourage you, however, to prepare for the quiz 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 material from previous years. However, 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. (When we have found instances of plagiarism and/or unauthorized collaboration in the past, we have given reduced or failing grades for the class (not just for the particular assignment), reported the incident to the Dean for Student Affairs, and/or filed a complaint with the Committee on Discipline.

## 12   Ethics

This is a course on Network and Computer Security. Although the course is primarily concerned with techniques that are designed to increase the security of networks and computer systems, a proper understanding of those systems requires that you be versed in their vulnerabilities and failings as well.

*Nevertheless, unless you have explicit written authorization from the owner and operators of a computer network or system, you should never attempt to penetrate that system or adversely affect that system's operation. Such actions are a violation of MIT policy and, in some cases, violations of State and Federal law. Likewise, you should refrain from writing computer viruses, worms, self-reproducing code, or other kinds of potentially damaging software for this course unless you have explicit, written approval for the specific type of software that you wish to create. These kinds of programs are notoriously difficult to control and their release (intentional or otherwise) can result in substantial civil and criminal penalties.*

We strongly recommend that you consult the *Athena Rules of Use* at `http://web.mit.edu/olh/Rules/`, and Section 13.2 of the MIT Policies and Procedures "Policy on the Use of Information Technology" at `http://web.mit.edu/policies/13.2.html`.

Finally, we recommend that you read and review the *ACM Code of Ethics and Professional Conduct* which can be found online at `http://www.acm.org/constitution/code.html`. (Or Google for "acm ethics".)

We expect all students in this class to follow the guidelines presented in this document, and in the documents just cited. If you are in doubt about the legality or ethics of any activity related to this course, please consult the staff before undertaking any such activity.