Course Information

Lecturer:	Professor Ronald L. Rivest NE43-324, 253–5880, `rivest@mit.edu` Office Hours by appointment
Teaching Assistants:	Chris Peikert NE43-313, 253–7843, `cpeikert@mit.edu` Office Hours: Wednesday 3–5pm
	Simson Garfinkel NE43-536, 253–6023, `simsong@lcs.mit.edu` Office Hours: Wednesday 12:15–2pm in room 38-644
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. Notes from previous years are on the class Web page and in the Barker Engineering Library.

4 The class online

The course site page is at

`http://theory.lcs.mit.edu/classes/6.857/`

This page links to an online registration form. You ***must*** register for the course by completing this form by Friday, September 5.

There is 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 to make handouts and notes available online.

5 Handouts

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

For the first time, this course has a required textbook: "Cryptography: An Introduction," by Nigel Smart. It will be available at Quantum Books on **Monday, September 8**. Please note that the textbook is intended to be a supplement to the cryptography portion of the course; it does not offer comprehensive treatment of all the topics we will cover.

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. Solutions will be distributed with corrected homework — hopefully within a week of being collected.

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 (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. 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 him/her first. If you are unable to make a compromise or your group does fall apart, talk to the staff.

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

In lectures presenting very new material, we may ask for volunteers to scribe the lecture notes. A group which scribes a lecture will have its 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 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. We will maintain a Web page of potential project topics and provide sample proposals later in the year. We will generally approve interesting topics about network and/or computer security.

A one or two-page written proposal for the project with an initial bibliography is due no later than in class on October 23. 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 last three classes (December 2, 4, and 9) 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. Your written report is due in class on December 9.

9 Tests

We will have two in-class quizzes (October 9 and November 25) and one take-home midterm (distributed October 23, due October 30). There is *no* final exam.

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.

10 Grading

Grades are: 35% for the problem sets; 10% for quizzes; 25% for the midterm; and 30% for the final project.

11 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. 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.

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".)