6.857 Course Information (Spring 2019)

Lecturers:	Professor Ronald L. Rivest 32-G692, 253–5880, `rivest@mit.edu` Office Hours by appointment
	Professor Yael T. Kalai 32-G682, `tauman@mit.edu` Office Hours by appointment
Teaching Assistants:	Leo de Castro `ldec@mit.edu` Office Hours: Thur 4-5:30pm (Room: 24-323)
	Sean Fraser `sfraser@mit.edu` Office Hours: Wed 4-5:30pm (Room: 24-317)
	Andrew He `andrewhe@mit.edu` Office Hours: Mon 3-4:30pm (Room: 24-317)
Course Secretary:	Debbie Lehto 32-G675A, 253-6098, `rivest-assistant@csail.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 6.006 or 6.046J (*Introduction to Algorithms*) and experience with modular arithmetic.

You must have *completed* 6.042 in order to register for 6.857 this year. Taking 6.042 concurrently is not enough. If you have successfully completed 18.310, 6.045, 6.046, or 6.875, or if the department has given approval for 6.042-equivalency for some other course or program (perhaps taken elsewhere) our prerequisite requirement for taking 6.042 is satisfied.

You must have successfully completed 6.033 already, or be taking it concurrently with 6.857, or have departmental approval for some other course or program (perhaps taken elsewhere) for satisfying the 6.033 requirement.

We may (rarely) make exceptions to the above. If you wish to be considered for an exception, send an email to `6.857-staff@mit.edu` with a description of your year, your reason for requesting an exception, and what equivalent background you may have had. Describe also how 6.857 fits into your educational program and career plans.

2 Units

6.857 is a 12-unit (3-0-9) G-level course intended primarily for seniors and first-year graduate students. It fits within the Computer Systems Concentration.

3 Lectures and Recitation

Lectures will be held from 11:00AM to 12:30PM in Room 54-100 on Mondays and Wednesdays.

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 websites from previous years. Notes from previous years are on the class website.

There will be a recitation section held on Fridays from 11:00AM to noon (room 54-100).

4 The class online

The course website can be found at:

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

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

The course Piazza site can be found at:

`https://piazza.com/mit/spring2019/6857`

If you have registered for the class, you will be automatically added to Piazza. If you have not registered for the class and wish to be added, please email the staff list immediately. We will use Piazza *only* as a forum; announcements, assignments, and all other material will be posted on the class website.

5 Textbook

There is no required textbook for this course. A list of recommended books is available on the *References* page on the course website; this page also lists other references you may find useful.

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, the 6.857 staff will assign you to a group of two or three other students for each homework. Again, please notify the TAs if you haven't registered for the class, otherwise you will not be put in a group. For the later homeworks, and for the final project, you may work in groups of your own choosing.

You may choose to remain in the same group between homeworks, or select a new group between homeworks. 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) and mutual consent or sufficient reason.

7 Homework

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

Your lowest problem set grade will be dropped at the end of the semester.

Homework templates will be available on the course website. 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.

We will use Gradescope for homework submission. Homework should be submitted in PDF format. Each problem will need to submitted as a separate file to facilitate the grading process. (The submission process will be further explained in the homework handout.)

Late homework will be penalized at the rate of two points (out of ten) per problem per day of lateness. For example, if the homework is due on Monday, but you turn it in on Wednesday, then your maximum score per problem is six. (Your net score will not be allowed to go negative.) You may turn in your solutions to different problems at different times to avoid penalties for problems you have completed before the deadline. You may turn in more than one solution to a problem, but only the latest one will count, except that once the homework deadline has passed, you may not turn in a solution to a problem for which you have already turned in a solution. Because we allow late solutions, please do not talk with anyone outside of your group or the TAs until the Friday of the week in which the homework is due.

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

Generally, homework must be done in groups (although we reserve the right to require individual homework assignments). You are to work on group problem sets and final projects in groups of (preferably) 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. As noted above, the initial organization into groups for the first two 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 **Wednesday, April 17th**. The quiz will test your knowledge of material from lectures, problem sets, and readings.

There is *no* final exam.

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 website for a list of topics from previous years, sample proposals, and additional project-related resources. We will generally approve interesting topics about cryptography, network security, 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 (subject to change):

- By **Wednesday, February 27** - Every student **must** individually post one (or more) project ideas on Piazza. Each post should have a heading with the topic area. This is a way for students to learn about what other students are interested in and find teammates. If you have more than one idea or interest, feel free to post all of your ideas, but please use different posts with different headers.
- By **Friday, March 22** - Turn in team composition and a multi-page project proposal and bibliography. Feel free to choose your teammates as you wish. We expect groups to be three or four people. If doing

reverse engineering, security attack, or security analysis of an institute, app, or company, your group should have requested and received permission by this date. Please ask the class staff if you're unsure whether your group needs to request permission.

- **April 8–12** - During this week, each project group will meet with the TA to review their progress.
- **April 22–26** - During this week, each project group will again meet with the TA to review their progress.
- **May 6, 8, 10, 13, 15** (Note use of recitation time on 5/10) - Groups will present short talks on their projects in class.
- **May 15** (Last class) - Written projects are due.

Your project reports *will be posted* on the class website at the end of the term. (Exceptions may be made if vulnerabilities are disclosed in your report that are still being patched by a vendor; in that case the report will be posted at the end of the summer, or at another agreed-upon time.)

10 Grading

Grades are:

40% for the problem sets
20% for quiz
40% for the final project

We will have five problem sets. We will only use your highest four problem set grades (perhaps after some grade normalization). Thus, if you miss a pset or do poorly on one, you can make it up on the others.

11 Collaboration and plagiarism

No collaboration is permitted on the in-class quiz. All tests are open book and open notes, but closed electronic devices. 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 (if any), 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.

In particular, term projects involving an evaluation of security of existing commercial products or systems need the approval of the course staff, who may require that you obtain permission from the vendor/supplier (depending on the nature of your proposed evaluation).

We strongly recommend that you consult the *Athena Rules of Use* at

`http://ist.mit.edu/services/athena/olh/rules`

and Section 13.2 of the MIT Policies and Procedures "Policy on the Use of Information Technology" at

`https://policies.mit.edu/policies-procedures/130-information-policies/132-policy-use-information-technology-resources`.

Finally, we recommend that you read and review the *ACM Code of Ethics and Professional Conduct* which can be found online at

`https://www.acm.org/code-of-ethics`.

(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.