6.857 Course Information (Spring 2022)

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: Andres Fabrega
`andresfg@mit.edu`
Office Hours: **TBD**

Kyle Hogan
`klhogan@mit.edu`
Office Hours: **TBD**

Lucas Camelo Sá
`jlucas16@mit.edu`
Office Hours: **TBD**

or write to **6.857-tas@mit.edu** to email to all the TAs

Course Assistant: Sally Lee
32-G846, 253-6837,
`rivest-assistant@csail.mit.edu`

Staff Email: `6.857-staff@mit.edu`

1 Course Name and Units

The course name is new this year: *Applied Cryptography and Security*. It used to be called *Network and Computer Security*; the new title better captures what is covered. The course number is the same (6.857) and the syllabus is largely unchanged.

6.857 is a 12-unit (4-0-8) G-level course intended primarily for seniors and first-year graduate students. It fits within the Computer Systems Concentration (this is for the "old" checklist).

2 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 (*Introduction to Algorithms*) or 6.046J *Design and Analysis of Algorithms*) and experience with modular arithmetic.

You *must have completed* 6.042 in order to take for 6.857. 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, please see a TA or 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.

3 Spring 2022: Additional Flexibility

Given the circumstances surrounding this semester, the course staff believes that, as much as possible, instructors should be flexible with requirements imposed on students. As such, this year we are taking the following approach regarding due dates and deadlines:

1. Treat every stated deadline as normal, with no late assignments accepted.
2. However, if something comes up that impedes your ability to meet a deadline, we are offering a no questions asked policy for extensions up to 72 hours. In this case, no S3 notice is necessary, although of course you may include one if you would like. The TAs will respond promptly regarding your request, and you may treat no response as tacit acceptance in the meantime (i.e., you will at least get an extension equal to the amount of time between sending your request and receiving a response.)
3. If no request is sent, then the assignment will not be graded out of respect to the graders' schedules. For extensions longer than 72 hours, please do contact S3 and we will work with them to ensure your needs are met.
4. **Exceptions:** The deadlines that we cannot extend are:
    - The final project submission deadline on May 20 (due to MIT's grade-submission requirements).

Furthermore, please do feel free to contact the teaching staff if there might be anything else we can do to help throughout the semester. In the any case, we might be able to point you to other resources that could be useful.

Finally, regarding all your courses this semester, please see the directory of academic continuity resources:

`https://registrar.mit.edu/covid-19/academic-continuity/resources`

Section 7 gives links to additional support resources.

4 Course Materials and Resources

4.1 Notes for OpenCourseWare

This semester OCW is looking to hire onw or two students from this course to to scribe the lectures and/or recitations into high-quality, textbook-style notes in LaTeX. The position will pay $15/hour, with potential for bonuses based on the quality of the work. Last semester the students hired in various classes spent around 2 hours per lecture on creating the notes. If you're interested, please fill out this form before Wednesday (2/2) night:

`https://forms.gle/HNmnrrkNkFW5RmU57`

4.2 Lectures and Recitation

Lectures are "in-person" and are held on Mondays and Wednesdays from 11:00AM to 12:30PM in Room 6-120. There is **no** option to view the lectures via Zoom in real time. However, recordings of the lectures will be made available in the "Top Secret" student-only section of the 6.857 website shortly after they are given (see Piazza for the password).

There will be a recitation section held on Fridays from 11:00AM to noon, in room 6-120.

Attendance at lectures and recitations is not required. Attendance at final project presentations (even if your team is not presenting) may be incentivized.

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 available through the class website.

4.3 Course Websites

The **main course website** is:

`http://courses.csail.mit.edu/6.857/2022/`

Handouts, assignments, and announcements will be available online only.

There may be a "course schedule" posted, although the schedule this year will be essentially the same as for last year.

The course **Piazza** site can be found at:

`https://piazza.com/mit/spring2022/6857`

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 and for non-public posts; most announcements, assignments, and all other material will be posted on the class website.

Submit your pset solutions via **Gradescope**; you will be automatically enrolled in Gradescope for this class.

Note that we do **NOT** use *Canvas* for this course, unlike many other MIT courses.

4.4 Office Hours

The TAs will be available for "office hours." See the course website and/or Piazza for timing details.

4.5 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.

4.6 Readings

The course website will list recommended readings associated with each lecture.

4.7 Previous Years

The course website includes a link to the course websites for previous years; you are encouraged to consult these pages if you'd like. The "Top Secret" section from last year contains links to video recordings of last year's lectures; you may also wish to consult these (the password for last year's "Top Secret" site will be posted on Piazza).

5 Expected Work and Grading

5.1 Grading

The work we expect from you for this course includes: problem sets, a quiz, and the final project.

Grades are weighted as follows:

40% for three contributing problem sets.
20% for the quiz.
40% for the final project.

We will have four problem sets. For additional flexibility, we will weight each problem set depending on your relative performance on it, using the following scheme: your highest pset grade is re-weighted to have 16 as a max score, the second-highest pset grade is re-weighted to have 12 as a max score, the third-highest pset grade is re-weighted to have 8 as a max score, and your lowest pset grade is re-weighted to have 4 as a max score. So, the total scores add up to 40, but they are weighted in a 4-3-2-1 proportion.

5.2 Groups

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

For the first three homeworks, the 6.857 staff will assign you to a group of two, three, or four 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 last homework, and for the final project, you may work in groups of your own choosing.

When you choose your homework groups, 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.

5.3 Homework

We will distribute four problem sets on approximately a biweekly basis, and they will be due about two weeks later.

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. Please start each problem (and sub-problems where relevant) on a new page. Gradescope will let you assign markers to the pages of your submission; please do so to facilitate the grading process. Once graded, marked homeworks will be returned and example solutions will be posted on the course website.

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 without prior permission. 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.

Important (planned) dates for each problem set (may change slightly):

- **Problem set 1:** released on Monday, February 7 and due on Tuesday, February 22..

- **Problem set 2:** released on Tuesday, February 22 and due on Monday, March 7.
- **Problem set 3:** released on Monday, March 7 and due on Monday, March 28.
- **Problem set 4:** released on Monday, March 28 and due on Monday, April 11.

5.4 Quiz and (no) Final Exam

We will have one in-class quiz on **Monday, April 4th, 2022**. The quiz will test your knowledge of material from lectures, problem sets, and readings.

There is *no* final exam.

5.5 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 potential topics, sample proposals, and additional project-related resources. Be sure to check out the corresponding project pages on previous years' course websites, too (the final project reports are posted)! 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 and deadlines for the project (subject to change):

- **February 28–March 04** Students should meet with a instructor or TA to discuss potential project ideas. This may be done individually or in groups. This meeting is intended to help you brainstorm topics for your project. No written submission is required, just be prepared with ideas for your project.
- **Monday, March 07:** 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.
- **Friday, March 11:** Turn in team membership. Feel free to choose your teammates as you wish. We expect groups to be three or four people.
- **Friday, March 18:** Each team must submit a multi-page project proposal and bibliography. 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 18–22:** During this period, each project group will meet with a member of the teaching staff to review their progress. You may send a draft for written feedback or provide a list of main questions in advance, but are not required to do so.
- **May 2, 4, 6*, 9:** Groups will give short presentations on their projects in class.
  (*: Recitation on May 6 may or may not be used for presentation depending on time.)
- **May 10:** Written projects are due. (Last day of classes for MIT spring semester 2022.)

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.)

6 Collaboration, Plagiarism, and Ethics

6.1 Collaboration and Plagiarism

No collaboration is permitted on the in-class quiz. This quiz is 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.)

6.2 Ethics

This is a course on Applied Cryptography and Security. Although the course is primarily concerned with cryptographic 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 generally will require that you obtain permission from the vendor/supplier (depending on the nature of your proposed evaluation). The TAs can supply a "template" letter for asking for such permission from a vendor.

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.

7 MIT Support Resources

Because the pandemic or other events may affect your life and ability to study adversely, please get in touch with the course staff if you wish to discuss your situation and make alternative arrangements for any assignments.

Also, we have set up an anonymous feedback form where you can send us comments at any point during the semester, and help improve the class. Given the atypical nature of this semester, continuous feedback is very important. So, please don't hesitate to let us know as soon as you feel like there is something we should improve! Of course, you may send the staff questions/requests/comments directly to the staff if you prefer.

`https://mit.co1.qualtrics.com/jfe/form/SV_6EiHyMlgqF1JQ10`

In addition, you may wish to consult with the excellent MIT support services:

- Student Mental Health and Counseling Services: Working with students remotely to identify, understand, and solve problems, and to help transform that understanding into positive action.

  `https://medical.mit.edu/services/mental-health-counseling`

- Student Support Services: An easily accessible hub of online support for undergraduates.

  `http://studentlife.mit.edu/s3`

- GradSupport and the Graduate Assistance Information Network: These offer a wide variety of resources to help grad students and families deal with the unexpected.

  `https://oge.mit.edu/development/gradsupport/`
  `http://www.mitgain.com/`

- MIT Office of Religious, Spiritual, and Ethical Life: Chaplains are available by phone, email, or videoconference to offer support and counsel to anyone in the MIT community.

  `http://studentlife.mit.edu/orsel/who-we-are`

- Dean on Call: Students living on campus can dial 100 from campus phones or 617-253-1212 to reach MIT Police, then ask to speak to the Dean on Call. The Dean on Call is available Monday through Friday, 5 pm – 9 am, and on Saturdays, Sundays, and MIT-observed holidays.

  `http://studentlife.mit.edu/dean-call-system`

- ask.mit.edu, where students can submit questions on personal topics from relationships to COVID to academics, and get a prompt reply from a Student Support and Wellbeing team member.

  `https://ask.mit.edu/`

- MIT's WorkLife Center, including MyLife Services for faculty and staff.

  `https://hr.mit.edu/worklife/center`
  `https://hr.mit.edu/worklife/mylifeservices`