Course Information

Instructors

Henry Corrigan-Gibbs	32-G970	henrycg@mit.edu
Srini Devadas	32-G844	devadas@mit.edu
Yael Tauman Kalai	32-G682	tauman@mit.edu
Nickolai Zeldovich	32-G994	nickolai@mit.edu

Teaching Assistants

Jules Drean	JD	drean@mit.edu
Derek Leung	DL	dtl@mit.edu

Questions? 6.s060-questions@mit.edu

Websites

Stellar	Announcements, calendar, grades, and PDF course content. http://6S060.csail.mit.edu
Piazza	All discussion related to course material. http://piazza.com/mit/fall2021/6S060
Gradescope	LaTeX problem set submissions and regrades. Entry Code: KYRBPK https://www.gradescope.com/courses/281655/

Content

6.s060 is a class broadly focused on computer security that covers the foundations of secure systems and cryptography. It focuses on basic principles of designing secure systems with critical cryptographic components and the integration of these components into said systems. 6.s060 will allow undergraduates to enter the important field of computer security earlier in their undergraduate program and also serve as an entry point for the graduate offerings, 6.857, 6.858, and 6.875, which focus on applied cryptography, systems security, and theoretical cryptography, respectively.

Prerequisites

6.006	Basic algorithms experience and programming in Python 3.
6.042	Basic knowledge of discrete mathematics: set theory, relations and logic, combinatorics, proofs, recursion, number theory, graph theory, and probability.
6.033	Basic knowledge of computer systems.

We caution against taking 6.s060 before having fulfilled the listed prerequisites. You will be able to evaluate your entering understanding of the prerequisite material via a Lab 0 assignment (Released W 9/08 and Due on F 9/17). **Note that all students must submit Lab 0 as it counts towards your overall grade.**

Lectures

All times listed for lectures, recitations and office hours are Eastern Time.

80-minute lectures will occur **LIVE in the classroom** Mondays and Wednesdays (11a-12.30p, with the usual MIT five-minutes after and before the hour start and end times but with staff availability for the whole hour).

Recitations

50-minute **Recitations** will be held weekly on Fridays at two different times (11a and 3p). The same material will be covered in each recitation.

Recitations will preview the laboratory released on the day of the recitation so students understand what is expected of them, and/or review the laboratory that was due the previous week and present the staff solutions, so students can receive additional feedback on their solutions. We note that we will not release code solutions to the coding assignments; solutions to the theory questions will be released.

Students are responsible for material presented during both lecture and recitation.

Office Hours

The TAs will hold office hours each week, both in-person and on Zoom. We will announce the time and location of office hours on Piazza during the first week of classes. Instructors will hold individual office hours by appointment.

Grading Policy

Your grade will be based on six laboratories (that comprise a theory portion and a coding portion), a midterm exam, and a final exam.

	Weight	Date	Time
Midterm	20%	Tuesday, November 2, 2021	7:30–9:30 P.M.
Final Exam	40%	December 13-16, 2021	3 hour block
Laboratories	40%	6 Labs, Lab 0 5%, others 7%	

MIT provides definitions[1] for the letter grades A, B, C, D/NE, and F/NE. We will follow these guidelines in assigning letter grades based on your overall score computed as described above.

Exams

There will be no recitation during midterm week. A review will be given during the recitation preceding the midterm. The midterm and the final exam will be open book. Since the exam durations are relatively short, we **strongly recommend** that you treat exams as closed book exams and prepare a short set of notes that you can quickly refer to during the exam.

Attendance at the midterm and the final exam is mandatory and may not be excused. A midterm may be rescheduled at the emailed request of an Institute Dean. Course-wide makeup midterms will be given within a day of the scheduled date. Conflict Final Exams will be scheduled by the registrar.

Laboratories

Labs and problem sets are the same thing in 6.s060. Each laboratory has a theory part and a coding part.

Lab	Release	Due	Topic
0	W 9/08	F 9/16	Basic Probability and Coding
1	F 9/17	F 9/30	Hashing and Client-Server Synchronization
2	F 10/1	F 10/14	Web of Trust
3	F 10/15	F 10/28	Confidentiality
4	F 11/05	F 11/18	Access Control
5	F 11/19	F 12/2	Capstone

[1] `http://catalog.mit.edu/mit/procedures/academic-performance-grades/#gradestex`

Each laboratory will contain a theory portion and a coding portion. Each theory portion must be entered into Gradescope; you will upload a PDF file compiled from a provided LaTeX template. Each coding portion will be provided on Github, and you will submit your code to Gradescope (a different assignment from the theory portion). Coding must be done in Python 3. Problem set submissions are **due by 10 P.M.** on the posted due date. We will do our best to return graded submissions one week after they are due.
If you feel that any assignment has been graded incorrectly, you may submit a **regrade request** to the relevant assignment on Gradescope, within a regrade window after the assignment's grade has been released (typically about a week). For any regrade request, we reserve the right to regrade the **entire assignment**, and your grade may be adjusted **up or down** as a result of the regrade.

Collaboration

The goal of the problem sets is for you to practice applying the course material. In this class, you are **encouraged** to collaborate on problem sets. Students who work together on problem sets generally do better on exams than students who work alone, but you will learn the material best if you **work on the problems FIRST on your own**. Some forms of collaboration are **not allowed**; some examples are listed below. Violating the collaboration policy to increase your score on a problem set is likely to lower your score on an exam, which carries significantly more weight. A violation may also lead to academic action and/or a significant penalty on your grade.

- Identify any **collaborators** or **outside sources** at the top of each LaTeX submission.
- Write code and theory problem solutions **by yourself** in your own words.
- Do **NOT** directly copy the work of others.
- Do **NOT** look at written solutions or code by other students before submitting your own solution. You may look at another student's code on their screen, only to help them debug, and only after you have submitted your own solution.
- Do **NOT** let other students see your written solutions.
- Do **NOT** send other students your code.
- You may ask TAs to help you debug your code during office hours or in a private Piazza post.