

Course Information

Instructors	Henry Corrigan-Gibbs	32-G970	henrycg@mit.edu
	Yael Tauman Kalai	32-G682	tauman@mit.edu
	Nikolai Zeldovich	32-G994	nickolai@mit.edu

Teaching Assistants	Ben Kettle	BK	bkettle@mit.edu
----------------------------	------------	----	-----------------

Questions?	61600-staff@csail.mit.edu
-------------------	---------------------------

Websites

Stellar	Announcements, calendar, grades, and PDF course content. https://61600.csail.mit.edu
Piazza	All discussion related to course material. https://piazza.com/mit/fall2022/61600
Gradescope	L ^A T _E X problem set submissions and regrades. Entry Code: 577GE7 https://www.gradescope.com/courses/415361/

Content

6.1600 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. 6.1600 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—6.5610 [6.857], 6.5660 [6.858], and 6.5620 [6.875], which focus on applied cryptography, systems security, and theoretical cryptography, respectively.

Prerequisites

6.1200 [6.042]	Basic knowledge of discrete mathematics: set theory, relations and logic, combinatorics, proofs, recursion, number theory, graph theory, and probability.
6.1210 [6.006]	Basic algorithms experience and programming in Python 3.
6.1800 [6.033]	Basic knowledge of computer systems.

We caution against taking 6.1600 before having fulfilled the listed prerequisites. You will be able to evaluate your entering understanding of the prerequisite material via lab 0 and problem set 0. **Note that all students must submit Lab 0 as it counts towards your overall grade.**

Lectures

All times listed for lectures 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 90-minute slot).

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 assignments (each comprising a lab portion and a problem set portion), a midterm exam, and a final exam.

	Weight
Midterm	20%
Final Exam	40%
Assignments	40% (Assignment 0: 5%, assignments 1-5: 7% each)

MIT provides definitions¹ 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

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.

Assignments

There are two types of assignments in 6.1600: labs and problem sets.

Each problem set must be submitted into Gradescope; you will upload a PDF file compiled from a provided L^AT_EX template.

Each lab assignment will be provided on Github, and you will submit your code to Gradescope (a different assignment from the problem set). 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 assignments 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 L^AT_EX submission.

¹<http://catalog.mit.edu/mit/procedures/academic-performance-grades/#gradestex>

- 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.