Course Information

| **Instructors** | Srini Devadas | 32-G844 | devadas@mit.edu |
| | Yael Kalai | 32-G682 | tauman@mit.edu |

Teaching Assistants	Katarina Cheng	TBD	katcheng@mit.edu
	Luke A Wagner	TBD	wagnerl@mit.edu
	Bill Wang	TBD	wangbill@mit.edu

Questions?   61600@mit.edu

Websites

Course site	Announcements, calendar, grades, and PDF course content.
	https://61600.csail.mit.edu
Piazza	All discussion related to course material.
	https://piazza.com/mit/fall2024/61600
Gradescope	LaTeX lab submissions and regrades.
	Entry Code: EVBV4Y
	https://www.gradescope.com/courses/844720/

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. **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 lab assignments, and two quizzes.

	Weight
Quiz 1	25%
Quiz 2	25%
Assignments	50%

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

The quizzes will be closed book. You will be allowed one double-sided cheat sheet for the first quiz, and two double-sided cheat sheets for the second quiz.

Attendance at the quizzes are mandatory and may not be excused. A quiz may be rescheduled at the emailed request of an Institute Dean.

---

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

Assignments

Each lab assignment will be provided on Github, and you will submit your code to Gradescope. 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.

Extensions. We are happy to provide 48-hour extensions for most assignments if you request them in advance. For longer extensions, we may ask you to first contact an S^3 dean, and to have the dean write us an email supporting your request. At the end of the semester, we may not be able to offer extensions if doing so would run up against the registrar's grade-submission deadline.

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 lab assignments. Students who work together on labs 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 labs is likely to lower your score on the quizzes. 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 lab solutions (code and text) **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.