

COMP 537: Cryptography

Bulletin Description

Introduces both the applied and theoretical sides of cryptography. Main focus will be on the inner workings of cryptographic primitives and how to use them correctly. Begins with standard cryptographic tools such as symmetric and public-key encryption, message authentication, key exchange, and digital signatures before moving on to more advanced topics. Potential advanced topics include elliptic curves, post-quantum cryptography, and zero-knowledge proofs. Honors version available.

General Course Info

Term: Fall 2024
Department: COMP
Course Number: 537
Section Number: 001

Time: TTh, 3:30pm – 4:45pm
Location: SN0014
Website: https://crypto.unc.edu/crypto_class/

Instructor Info

Name: Saba Eskandarian
Office: Brooks 346
Email: saba@cs.unc.edu
Web: <https://crypto.unc.edu/>
Office Hours: See course website

Textbooks and Resources

We will primarily use Canvas for course announcements and sharing lecture notes. Assignments will be available on the course website linked above. If you have any questions, comments, or suggestions regarding the course organization and policies, please feel free to reach out via email. An anonymous feedback form is linked on the course website if you would like to give feedback anonymously. Assignment submission and grading will be handled via Gradescope through the Canvas integration.

Optional textbooks: There is no required textbook. *A Graduate Course in Applied Cryptography* by Dan Boneh and Victor Shoup ([free](#) online) and *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell are good resources for students looking to go deeper into the material covered in class.

Course Description

Cryptography is an indispensable tool for protecting information in computer systems. Our web browsers use it almost every time we connect to a website; it protects our private messages from prying eyes; it enables the modern world of online commerce; and it guards the freedoms of journalists, dissidents, and oppressed groups throughout the world.

At the same time, cryptography has deep connections to the theory of computation, number theory, algebra, and computational complexity theory. Major open questions in cryptography have immediate ramifications for whether $P=NP$, and cryptography research has given rise to several of the most beautiful ideas in computer science. These ideas (which we will cover) have been recognized by several Turing awards.

This course will introduce you to both sides of cryptography. Our main focus will be on the inner workings of cryptographic primitives and how to use them correctly. We will begin with standard cryptographic tools such as encryption, message authentication, key exchange, and digital signatures before moving on to more advanced topics like elliptic curves, post-quantum cryptography, and zero knowledge. See the course schedule page for a more detailed list of topics. Throughout the course we will also explore the techniques used in modern cryptography to reason about the security of cryptographic schemes.

Target Audience

This course is intended for anyone who wishes to understand and use the fundamental techniques of modern cryptography. There will be both programming assignments and problem sets that involve writing proofs, so a solid foundation in basic computer science topics will be expected.

Prerequisites

Prerequisites for this course are COMP 283, COMP 210, COMP 211, and COMP 301 (or their equivalents).

Goals and Key Learning Objectives

By the end of this course, students should:

- Understand how crypto primitives used in practice work
- Know how to use cryptography to meet various security goals
- Be able to reason about the security of cryptographic schemes

Course Requirements

Classes will primarily be lectures, although a few group problem solving sessions or discussions may be included as well. In addition to attending lectures, students will solve problem sets that exercise various topics covered in class and complete programming assignments to develop practical experience using cryptography.

Key Dates

See course website for a listing of assignment deadlines and exam dates.

Grading Criteria

- Problem set average: 45%
- Programming assignment average: 30%
- Midterm exam: 20%
- Final exam: 5%

Course Policies

You must use LaTeX to write up your problem sets using the provided template. All assignments are due at 11:59pm on the listed day and must be submitted via Gradescope.

You get five “late days” in total during the semester. You may use a late day to submit a problem set after the deadline via Gradescope. You may only use late days in one-day increments (no partial late days), and **you may use at most two late days on a single assignment**. If you submit an assignment late after running out of late days, you will receive no credit for the submission. Please submit your assignments on time and save your late days for extraordinary situations. Please contact me in advance if there are extenuating circumstances that may warrant an exception to this policy.

Honor Code

You may (and are strongly encouraged to) discuss the problem sets with other students, and you may work together to come up with solutions to the problems. If you do so, you must list the names of your collaborators on the first page of your submission.

Each student must write up their problem set solutions independently, even if they collaborated with others in solving the problems. Programming assignments can be completed independently or in pairs. Please submit one assignment (including both names) for the pair on Gradescope in this case.

Sharing code or helping other groups debug their code in programming assignments is not allowed. You can come to office hours for help with this.

You may use the Boneh-Shoup textbook, or any other textbook of your choosing, as a reference. If you use a result from a textbook in the course of solving a problem, please cite the textbook in your write-up. Please do not search the Internet or use online tools for answers or help on assignments.

I expect all students to follow the guidelines of the UNC honor code. In particular, students are expected to refrain from “lying, cheating, or stealing” in the academic context. You can read more about the honor code at honor.unc.edu. Please see me if you are unsure about what may or may not violate the honor code in this class.

Course Schedule

See course website for schedule of topics

Attendance and Participation

Class meetings will be held in person, and attendance is strongly encouraged. That said, students who are not feeling well should not come to class. You will not be penalized for missing class. If you do miss class, be sure to ask a friend in class for any notes or announcements you may have missed.

Please let me know in advance if you will miss an exam date, so you can be scheduled to take the exam at an alternative time.

Acknowledgments

The structure of this course is inspired by Stanford's [CS255](#) and [CS355](#) courses.

Grade Appeal Process

If you feel you have been awarded an incorrect grade, please discuss with me. If we cannot resolve the issue, you may talk to our departmental director of undergraduate studies or appeal the grade through a formal university process based on arithmetic/clerical error, arbitrariness, discrimination, harassment, or personal malice. To learn more, go to the [Academic Advising Program](#) website.

Accessibility Resources and Services

The University of North Carolina at Chapel Hill facilitates the implementation of reasonable accommodations, including resources and services, for students with disabilities, chronic medical conditions, a temporary disability or pregnancy complications resulting in barriers to fully accessing University courses, programs and activities.

Accommodations are determined through the Office of Accessibility Resources and Service (ARS) for individuals with documented qualifying disabilities in accordance with applicable state and federal laws. See the ARS Website for contact information: <https://ars.unc.edu> or email ars@unc.edu.

Counseling and Psychological Services

CAPS is strongly committed to addressing the mental health needs of a diverse student body through timely access to consultation and connection to clinically appropriate services, whether for short or long-term needs. Go to their website: <https://caps.unc.edu/> or visit their facilities on the third floor of the Campus Health Services building for a walk-in evaluation to learn more.

Title IX Resources

Any student who is impacted by discrimination, harassment, interpersonal (relationship) violence, sexual violence, sexual exploitation, or stalking is encouraged to seek resources on campus or in the community. Reports can be made online to the EOC at <https://eoc.unc.edu/report-an-incident/>. Please contact the University's Title IX Coordinator (titleixcoordinator@unc.edu), Report and Response Coordinators in the Equal Opportunity and Compliance Office (reportandresponse@unc.edu), Counseling and Psychological Services (confidential), or the Gender Violence Services Coordinators (gvsc@unc.edu; confidential) to discuss your specific needs. Additional resources are available at safe.unc.edu.

Policy on Non-Discrimination

The University is committed to providing an inclusive and welcoming environment for all members of our community and to ensuring that educational and employment decisions are based on individuals' abilities and qualifications. Consistent with this principle and applicable laws, the University's [Policy Statement on Non-Discrimination](#) offers access to its educational programs and activities as well as employment terms and conditions without respect to race, color, gender, national origin, age, religion, creed, genetic information, disability, veteran's status, sexual orientation, gender identity or gender expression. Such a policy ensures that

only relevant factors are considered and that equitable and consistent standards of conduct and performance are applied.

If you are experiencing harassment or discrimination, you can seek assistance and file a report through the Report and Response Coordinators (see contact info at safe.unc.edu) or the [Equal Opportunity and Compliance Office](https://eoc.unc.edu/report-an-incident/), or online to the EOC at <https://eoc.unc.edu/report-an-incident/>.

Diversity Statement

I value the perspectives of individuals from all backgrounds reflecting the diversity of our students. I strive to make this classroom an inclusive space for all students. Please let me know if there is anything I can do to improve. I appreciate suggestions.

Syllabus Changes

I reserve the right to make changes to the syllabus, including assignment due dates and test dates. These changes will be announced as early as possible.