Topics in Applied Cryptography

Course Description

Cryptography plays a vital role in securing the systems we use everyday. This graduate level seminar course will provide an overview of cryptography and its applications. Building on the foundations in the undergraduate course, this course will aim to understand the cryptographic tools that may be used in practice to secure systems as well as their mis-use and how this can lead to attacks. Students will read, discuss, and review foundational and recent papers in this area and learn how to present conference-style talks on the papers. Students will also complete a course research project on a cryptography-related topic of their choosing.

The papers have been selected to expose students to a wide range of applied cryptography topics, including but not limited to: messaging protocols, authentication, cryptographic attacks, anonymous payments systems, voting, encrypted data computation, private information retrieval, and oblivious RAM. The precise set of topics rotates based on instructor preference, recent research developments, and current events.

General Course Information

Term:	Fall 2025
Department:	COMP
Course Number:	790
Section Number:	188
Time:	TuTh, 3:30-4:45PM
Location:	SN11
Website:	https://julialen.github.io/comp790-188/

Instructor Information

Name:	Julia Len
Office:	FB342
Email:	jlen@cs.unc.edu
Website:	https://julialen.github.io/
Office Hours:	TBD

Target Audience

This class is intended for graduate students interested in exploring various topics in applied cryptography research and how it may intersect with their own research interests.

Interested undergrads are also welcome, but should first ask the instructor for permission. A background in cryptography is not required but strongly encouraged.

Prerequisites

There are no prerequisites for this course, though it is strongly recommended for students to take COMP 537 (or equivalent).

Goals and Key Learning Objectives

By the end of this course students should:

- Be comfortable with reading cutting edge research papers in applied cryptography, and be able to analyze the papers' strengths and weaknesses.
- Be able to conduct novel research on a topic within applied cryptography.
- Be able to give a conference style presentation on their research project results.

Grading Criteria

The following plan is tentative and subject to change.

Class Participation (20%)
Students are expected to contribute to class discussions following paper presentations. Students should be able to ask insightful questions and demonstrate that they have read and understand the assigned readings.

Paper Presentations (20%)
Students will give conference style talks on assigned papers. They will prepare slides and a 15 minute presentation on the papers.

Paper Reviews (20%)
Students will submit mini-reviews on assigned papers to Canvas.

Course Project (40%)
Students will conduct original research on a topic related to applied cryptography over the course of the semester. Students will propose a project partway through the class and will submit a final report (6-12 pages) by the end of the course. Students will also give a conference style talk on their results during the final week of class. Working in groups is allowed, but a more substantial product is expected when working as a group.

Class Schedule and Important Dates

See the course website for a detailed calendar of important dates and the reading schedule.

Course Resources

There is no required textbook for the course, but there are a number of cryptography lecture notes and textbooks that students may find useful as a reference when reading assigned materials.

- A Graduate Course in Applied Cryptography, by Dan Boneh and Victor Shoup
- Lecture Notes on Cryptography, by Shafi Goldwasser and Mihir Bellare

Acknowledgments

The structure of this course is inspired by the University of Michigan's EECS 598 course.

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, 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. These changes will be announced as early as possible.