CSE 4702/5852: Modern Cryptography: Foundations

Spring 2023

January 16, 2023

1 Administrative

Description Covers the foundations of modern cryptography introducing basic topics such as one-way functions, pseudorandom generators, and computational hardness assumptions based on number theory. The course will cover fundamental cryptographic constructions such as hard-core predicates, secure symmetric encryption and message-authentication codes, and public-key cryptography.

We'll learn the process of understanding a real-life security goal, formalizing it, using mathematics to help solve the problem, and prove that our solution meets our security goals. We'll focus on problems of importance to everyday citizens and be rigorous in our claims.

Course Objectives Successful students will be able to mathematically formalize security goals from informal discussions. They will also be able to write formal proofs by reduction. Students will be able to identify and reproduce common cryptographic definitions and constructions. When given a set of definitions, assumptions, and constructions, students will be able to assess whether or not the stated definitions are met by the constructions and assumptions.

Contact Benjamin Fuller, benjamin.fuller@uconn.edu, 6-2122, ITE (Information Technologies Engineering) room 243.

Office hours (changes will be posted on HuskyCT): Monday 2-3pm, Thursday 1-2pm. I encourage attending office hours. If you cannot make office hours, please ask technical questions on HuskyCT and email me. I'm in the office 9-4 each day but not always available. If there is a recurring conflict we can find another time.

Course Content We will be covering the following topics in roughly the following order:

- Overview of Cryptography
- Probability Theory Review
- One Time Pad, Information Theoretic Security, and Perfect Secrecy
- Definitions for Computational Security

- Modern Cryptographic Assumptions
- Hash Functions
- Pseudorandom Number Generators, Functions and Permutations
- Message Authentication Codes
- Number Theory Review for Asymmetric Cryptography
- Public Key Cryptography
- Cryptographic Signatures
- Overview of Transport Layer Security
- The last three meetings of the semester are reserved for student presentations on oral final exams on topics of interest.

Meeting and Notes Class meetings are in McHugh 307 on Tuesday and Thursday from 11-12:15pm.

Our class meetings will be a mix of lecture, discussion and critical thinking. Attendance is highly encouraged but not required. The course will be interactive and discussions may not be completely captured in class notes. We will not follow any text, class is the best resource to learn the material. Each student will be required to write class notes for at least one session. These notes may depend on the preceding and following classes, thus, attendance is required for those three classes.

Textbook We will generate class notes during the semester that will contain the major ideas and concepts. As supplementary reading, I recommend Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell. This book is not required but I encourage students to jointly purchase a few copies to share. The book web site is here: `http://www.cs.umd.edu/~jkatz/imc.html`.

For those interested in pursuing theoretical cryptography, I recommend Foundations of Cryptography by Oded Goldreich. This text is dense and serves better as a reference. It is incredibly detailed and discusses important technical details that often omitted in other texts. Please don't try and read it as a text!

Several books consider more practical aspects of implementing cryptography. These include:

- Handbook of Applied Cryptography by Alfred Menezes, Paul van Oorschot and Scott Vanstone
- Applied Cryptography by Bruce Schneier

In this class we will cover modern (reduction-based) cryptography that was developed starting in the mid 20th century. However, cryptography is thousands of years old and I encourage students to explore the history of cryptography as well. One example is Cryptography: The Science of Secret Writing by Laurence Smith.

Communication The class notes, problem sets, and solutions will be posted on the course web site at `http://benjamin-fuller.uconn.edu/teaching/modern-cryptography-foundations/`. Right now that webpage has notes from a 2016 offering. These will be updated through the semester.

Announcements, discussion, and homework submission will be done on HuskyCT. Please ensure you receive emails from HuskyCT so you get announcements. In addition, I encourage students to post and answer questions about class material and problem sets. I will also answer questions but I encourage students to try and jointly answer questions. **Do not directly ask or answer homework problems.**

Personal questions should be directly to my email or handled in person during office hours. I will not answer emails from Friday 6pm to Sunday 6pm.

Grading, assignments and exams There will be problem sets throughout the semester, expect ten assignments. These assignments are due via HuskyCT and should be submitted in LaTeX. For those that haven't used LaTeX before I recommend installing LaTeX now and getting familiar (perhaps by volunteering to do lecture notes for an early lecture).

All students have five late days to be used however they wish throughout the semester. Each assignment should be marked with the number of late days used. Students who exceed this number of late days will receive 20% off the assignment for each additional day the assignment is late. Assignments will be graded no more than one week after they are due.

Time to complete will be heavily influenced on students' mathematical maturity, a lower estimate is 4 hours and an upper end should be 10 hours. If you are spending more time than this please come talk to me!

Each student is expected to create notes for at least one class meeting. These notes should be cohesive with the surrounding classes and will require some communication with me and the students doing the surrounding notes. I'll start you from notes from a prior offering but these are just a starting point. The signup is here and the previous offerings notes are here.

The class will be graded as follows:

- 70% homework assignments.
- 20% final exam or final project.
- 10% lecture notes.

Important caveat: The final exam is the main individual evaluation. In order to pass the class you must score about 50% on the final exam.

With that in mind grades will be assigned according to the scale in Table 1.

Final examination/project Students will take a final exam to assess their overall knowledge of course material. Students enrolled in 4702 will be able to pick between an oral exam and a written exam. Students enrolled in 5852 are expected to do **both an oral exam and a written exam**. In order to pass the class, students must receive at least a 50% on the final exam. In the oral exam, students can do one of two options:

1. Present a 15 minute presentation to the class on a topic not covered in the class (the last 3 classes will be saved for these presentations). Or,
2. Do a 1-1 exam with the instructor where the student is asked to solve one or more problems using a white board. Students should be able to express their thought processes while doing so.

Number Grade	Assigned Grade	Grade Points
90+	A	4.0
86-89	A-	3.7
82-85	B+	3.3
79-81	B	3.0
76-78	B-	2.7
73-75	C+	2.3
69-72	C	2.0
66-68	C-	1.7
65-67	D+	1.3
62-64	D	1.0
59-61	D-	.7
0-58 (Or at most 50 on final exam)	F	0

Table 1: Grading Scale

Both options will be interactive where the instructor (and other students for option 1) will ask questions and ask for explanations while the student is presenting.

The written exam will be five questions of which four must be answered. This is a timed, individual test. Students will be given questions and asked to provide answers with supporting work. There will be a final exam to be scheduled by the registrar. There will be no midterm.

The last day to drop a class without a 'W' is January 30. Last day to convert to pass/fail/withdraw is April 10. Since there will not be an exam before that date, please come talk to me before that date if you have concerns about your performance.

Collaboration Thoughtful discussion will help you answer the problem sets. At the same time, we need to measure individual performance and contribution. In an effort to balance these two needs, abide by the following conditions:

- You may collaborate with up to three other students. Each student you collaborate with should be named on the homework assignment.
- You must first consider each problem on your own and generate ideas on how to solve the problem.
- You may discuss problems and solution ideas jointly. The goal of collaboration is to understand the high level ideas of how to solve the problem. Do not go further than this.
- You must write solutions completely on your own. If an issue arises during writing the solutions you may speak to your collaborators. Do not bring your write-up; you need to be able to describe the problem without referring to the solutions.
- The final exam will be an individual effort. As noted above, students cannot pass the class without scoring at least 50% on the final exam.

- Do not use other resources (outside of your textbooks and collaborators) to attempt to find the problem or the solution. This includes using the internet to search for parts of the problem.

2 Course contents

This course will focus on modern, reduction-based cryptography. We will focus on rigorous definitions and relations between cryptographic objects. Concrete mathematical examples of cryptography concepts will be presented but will not be the focus of the class. The class will cover information-theoretic security, one-way functions/permutations, pseudorandom generators, pseudorandom functions, symmetric encryption, public-key encryption and signature schemes, block ciphers and message authentication codes, and other topics of interest.

Special care will be taken to understand security goals and constructing formal definitions to codify this intuition. We will show constructions from other cryptographic objects and directly from mathematical objects. We will generate formal mathematical proofs that an object satisfies our definition.

We will be writing proofs (in LaTeX) throughout this course. A background in proofs and mathematics is necessary to understand and contribute to the class. If you have not written mathematical proofs, this class will be very difficult (if not impossible).

We will briefly discuss concerns that arise when implementing and using cryptography. I emphasize that cryptography is not a solution to computer security, it is a tool to be applied in system design. Done poorly, cryptography can decrease system security.

3 Policies

Academic Honesty This course expects all students to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. If you have questions about academic integrity or intellectual property, you should consult with your instructor. Additionally, consult UConn's guidelines for academic integrity.

The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, talk to me!

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include: not reporting collaborators, jointly writing solutions, copying or plagiarizing solutions from other sources, and cheating on the exam.

Student Conduct Code Students are expected to conduct themselves in accordance with UConn's Student Conduct Code.

Copyright My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expression.

Students may take notes. In addition, we will ask you to release your created notes. In addition, students will be consulted before using their solutions either with or without their name.

Students with Disabilities The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. Students who require accommodations should contact the Center for Students with Disabilities, Wilbur Cross Building Room 204, (860) 486-2020, or http://csd.uconn.edu/.

Final Exam Policy In accordance with UConn policy, students are required to be available for their final exam and/or complete any assessment during the time stated. If you have a conflict with this time you must obtain official permission to schedule a make-up exam with the Office of Student Support and Advocacy (OSSA). If permission is granted, OSSA will notify the instructor. Please note that vacations, previously purchased tickets or reservations, graduations, social events, misreading the assessment schedule, and oversleeping are not viable reasons for rescheduling a final.