

CSE 5852: Modern Cryptography: Foundations

Fall 2016

August 31, 2016

1 Administrative

Description This course covers the foundations of modern cryptography introducing topics such as one-way functions, pseudorandom generators, and computational hardness assumptions based on number theory. The course will cover cryptographic constructions such as hard-core predicates, symmetric encryption, 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.

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

Office hours (changes will be posted on HuskyCT): Monday 3-4, Thursday 1-2. I encourage attending office hours. If you cannot make office hours, please ask technical questions on HuskyCT and email me for personal questions.

Meeting and Notes Class meetings are in MONT (Monteith building) room 420 on Mondays and Wednesdays from 1:25-2:40.

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/>. 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 L^AT_EX. For those that haven't used L^AT_EX before I recommend installing L^AT_EX now and getting familiar (perhaps by volunteering to do lecture notes for an early lecture). Late assignments will not be accepted after the fact, contact me before the due date if you will not be able to complete an assignment on time. Assignments will be graded no more than one week after they are due. Solutions will be based on student responses and will include the student's name if they desire. 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!

There will be a final exam to be scheduled by the registrar. There will be no midterm.

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.

The class will be graded as follows:

- 70% homework assignments.
- 20% final exam.
- 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.

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

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

The last day to drop a class without a 'W' is Monday, Sept. 12. The last day to drop a class with a 'W' or convert to pass/fail is October 31. 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 Research is a collaborative effort. 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. A more holistic view of computer security can be found in CSE 4707.

Course Objectives By the end of this course, you will be able to:

- Have an informal discussion of a security goal and formalize it mathematically.
- Write reduction based proofs of security.
- Understand important cryptographic concepts and common building blocks.
- Read academic papers in cryptography (given enough time).

Tentative Class Schedule Table 2 contains a tentative plan for the topics week by week. We'll adjust the schedule as needed. The emphasis will be on gaining the skills to read and understand cryptography, we will remove topics as necessary. Currently, weeks 13-14 are scheduled for advanced topics to be decided by the class.

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!

Week	Topics
1	Defining security of communication, goals. Probability theory.
2-3 (three classes)	Information-theoretic security, One-time pad, message-authentication codes, Shannon's bound, overcoming bounds
4	Finite field mathematics
5	Adding integrity protections, pairwise independent hash, overcoming bounds
6	Computational security: semantic security and CPA
7	One-way functions/permutations, hardcode predicates, pseudorandom generators
8	Constructing pseudorandom generators, pseudorandom functions/permutations
9	Constructing a secure channel
10	Finite field mathematics, public-key encryption: intuition, definitions, possible constructions
11	Signatures
12	What happens when you visit a website? Cryptography in practice
13-14	Student's choice. Possible topics: zero-knowledge proof systems, secret-sharing, introduction to multi-party computation

Table 2: Tentative class schedule. Topics in weeks 13-14 to be adjusted based on student feedback.

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.