
Course Information

Course Staff	Room	Phone	Email	Office Hours
Prof. Adam Smith	IST 338K	x3-0076	asmith@cse.psu.edu	Mon. 3:00-5:15pm

Webpage: <http://www.cse.psu.edu/~asmith/courses/crypto598/F07/> Check it often.

Prerequisites: A course in discrete mathematics (CSE 260/ MATH 311), probability (STAT 418) and algorithms (CSE 465), or permission of the instructor. Courses in computability/complexity theory (CSE 368/468) or computer security would also be helpful. What you need most is “mathematical maturity” (see below).

Auditors: If you are a late-stage grad. student and would likesimply to audit the class, you are welcome. Please send me your Penn State login so I can add you to the Angel group.

Background Survey: The Angel page for this course contains a short survey on your background, goals, and knowledge. Students who complete the survey by Thursday, August 30 (or within a week of enrolling in the course, whichever is later) receive a 3% bonus to their final grade.

Lectures: T/Th 4:15-5:30pm, Room IST 333.

Canceled Lecture: I will be away on September 6. We will discuss how to reschedule the lecture in class. I would like to run late on one Tuesday night (say, September 4 or September 18) and have the replacement lecture from 5:45-7:00pm.

Textbook: Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, CRC Press, 2007. The first chapter is available online: <http://www.cs.umd.edu/~jkatz/imc.html>

Overview: The goal of the course is introduce students to the mathematical concepts underlying modern cryptography. These include, broadly:

- Complexity-theoretic foundations
- Useful number-theoretic and algebraic notions
- Rigorous definitions and proofs of security
- Reductions between cryptographic primitives

The course will expose students to these concepts by studying how they are used in secure communication, namely in protocols for encryption and authentication.

Mathematical Maturity: This is course has a significant theoretical component. You will be expected to read and write mathematical proofs. Concepts like induction, proofs by contradiction, and reductions between computational problems, should be familiar and comfortable.

Syllabus: Subject to change!

- Private-key encryption and pseudorandom number generation
 - Perfect Secrecy [KL 1,2]
 - (Tools: probability, algorithms, reductions)
 - Computational secrecy: pinning down a definition [KL 3.1,3.2]
 - Indistinguishability and pseudorandom generators [KL 3.3]
 - Private-key encryption from p.r.g.'s [KL 3.4]
 - Pseudorandom functions, permutations [KL 3.5,3.6]
 - Using p.r.p.'s for encryption
- Block Ciphers: Design and Cryptanalysis
 - Feistel networks, DES, AES [KL 5]
 - Basic cryptanalysis [KL 5.6]
- Computational Hardness
 - One-way functions [KL 6.1]
 - (Tools: modular arithmetic [KL 7.1])
 - Examples of conjectured one-way functions
 - Hard-core predicates and pseudorandom generators [KL 6.3-6.5]
- (?) Theoretical Constructions of Pseudorandom Functions and Permutations [KL 6]
 - GGM: From p.r.g.'s to p.r.f's
 - Luby-Rackoff: understanding Feistel networks
- Public-Key Encryption
 - (Tools: More number theory [KL 7])
 - Public-Key Encryption [KL 9,10]
 - Examples [KL 11]
 - (?) Factoring algorithms [KL 8]
- Authentication and Collision-Resistant Hash Functions [KL 4]
 - Message Authentication Codes
 - Examples based on block ciphers
 - Collision-Resistant Hash Functions
- Digital Signatures [KL 12]
- Protocols: Identification and Zero-Knowledge
 - Interactive proofs
 - Example: discrete logarithms
 - Commitments and 3-coloring
 - Zero-Knowledge proofs
 - (?) Fiat-Shamir signatures

Related Courses Beyond the prerequisites mentioned above, there are a number of related courses at Penn State that complement the material in this class.

- CSE: computer security (CSE 543), computability (CSE 368/468), quantum computing (CSE 598x), data privacy (CSE/STAT 598x), **theory seminar** (CSE 597x).
- Math: factoring and primality testing (Math/CSE 467), plus all the courses in number theory and abstract algebra
- EE: information theory (EE 561)

Evaluation The grade will be calculated as follows:

Homework 60%

In-class quizzes: 40%

Quizzes There will be a short, in-class quiz approximately every $2\frac{1}{2}$ weeks (5 lectures).

Homework There will be six or seven problem sets due over the course of the semester. Late homework will generally not be accepted. If there are extenuating circumstances, you should make arrangements at least 48 hours in advance with the instructor. Only serious excuses will be considered in cases where prior arrangements were not made.

You should be as clear and concise as possible in your write-up of solutions. Understandability of your answer is as desirable as correctness, because communication of technical material is an important skill. A simple, direct analysis is worth more points than a convoluted one, both because it is simpler and less prone to error and because it is easier to read and understand. Points may be subtracted for illegible handwriting and for solutions that are too long.

“I’ll take 15%” option: Partial credit is only given for answers that make significant progress towards correct solution. Understanding whether a solution is correct is an important skill. If you realize that you cannot solve a problem, you have an option of writing “I’ll take 15%” instead of your answer. In this case, you will get 15% for this problem (or part of the problem). If you do write an answer, however, that answer will be graded and your score will be 0 if your solution is completely wrong.

Randomized grading Homework assignments will each consist of several problems. I will provide solutions to *all* problems but will only grade a subset of the problems (not known to you in advance).

Collaboration and Honesty Policy Collaboration on homework problems, with the exception of programming assignments, is permitted, but not encouraged. If you choose to collaborate on some problems, you are allowed to discuss each problem with at most 3 other students currently enrolled in the class. Before working with others on a problem, you should think about it yourself for at least an hour. Finding answers to problems on the Web or from other outside sources (these include anyone not enrolled in the class) is strictly forbidden.

You must write up each problem solution by yourself without assistance, even if you collaborate with others to solve the problem. You must also identify your collaborators. If you did not work with anyone, you should write “Collaborators: none.” It is a violation of this policy to submit a problem solution that you cannot orally explain to an instructor or TA.

No collaboration whatsoever is permitted on exams or quizzes.

Violations of this policy will be dealt with according to University regulations.