CS195-7: Introduction to Cryptography September 3, 2002

Handout 1: Course Information

Instructor: Anna Lysyanskaya

Instructor.

Anna Lysyanskaya

E-mail:	anna@cs.brown.edu
Office:	CIT 501
Phone:	37605
Office Hours:	Monday 10 a.m. – noon

Course homepage. http://www.cs.brown.edu/courses/cs195-7/

Course material. Cryptography is about communication and computation in the presence if an adversary. In this course, we will address questions such as:

- Can a secret message be sent over an insecure channel? How can Alice send a message to Bob such that Bob will understand it but no eavesdropper will? Can we guarantee authenticity of data?
- How can Bob be sure that the message he received is indeed from Alice? How can he convince someone else of this fact?
- Can we guarantee that it is impossible to cheat in an on-line game? Can Alice and Bob play cards over the Internet?

To answer these questions, we will first decide what security property are desirable for the situation at hand. We will then formally define the objects that we wish to derive: encryption schemes, signature schemes, secure protocols. Finally, we will give suitable constructions and prove that they satisfy the definition we have given.

The topics include: provable security, secure encryption and authentication mechanisms in both the private- and the public-key settings, pseudorandomness, complexity-theoretic assumptions in cryptography, secret sharing, zero-knowledge proofs.

This course is theoretical. If you are interested in computer security at large, keep in mind that cryptography is only a part of it. Secure systems require appropriate architecture, operating system, secure hardware – all these things are beyond the scope of this course and we will take them largely for granted.

Prerequisites. One of 155, 157, 159, or permission of the instructor. This is a *theory* course, with emphasis on formal mathematical definitions and proofs. Recommended background: basic familiarity with algorithms, some number theory, discrete probability, and elementary complexity theory.

Reading. No textbook is required. Several copies of O. Goldreich, "Foundations of Cryptography" will be placed on reserve in the Science Library. S. Goldwasser and M. Bellare, "Lecture Notes on Cryptography" is available free on the web at `http://www-cse.ucsd.edu/~mihir/papers/gb.html`. Relevant papers will be handed out from time to time.

Lectures. Since we will not follow any textbook, your main source of information will be the lectures. The more your participate in class, the more you will learn! After each lecture, I will post the notes I made while preparing the lecture.

Weekly problem sets. Roughly every Tuesday you will have a problem set due. Problem sets will be due at 1 p.m. *sharp.* No extensions will be given; this is a firm policy that makes sure that we can discuss solutions in class once you hand in the problem sets. To account for special cases, your two lowest problem set grades will be dropped. (Of course, in case something terrible happens, you will also be excused from turning in the relevant homework assignments.)

You may collaborate on solving the problems, but the write-up of your solutions should be your own. You must list your collaborators. The problem sets will account for 60% of your grade.

You should make an effort to typeset your homeworks. LaTeX is especially recommended for it. LaTeX templates for doing the homeworks will be regularly posted.

Take-home midterm exam. The midterm exam will be of the same difficulty as the weekly problem sets. The main difference will be that you will not be allowed to collaborate on the midterm exam. It will account for 15% of your grade.

Final projects for 200-level credit. In order to obtain 200-level credit, you will have to carry out an individual research project.

In mid-October, you will choose a cryptography-related problem of interest to you. It does not have to be an open problem, but it can be an open problem if you prefer. You will also need to come up with a list of papers and/or books that you think are relevant and that you plan to read in order to familiarize yourself with the problem at hand. I will help you with this.

By the middle of November, you will have to become an expert on the problem you chose. You will meet with me and tell me what you have discovered about your problem as a result of reading up on it and thinking about it. Following our meeting, I will prepare a list of questions about the state-of-the-art on your problem. I will not ask you to solve any open problems. Rather, my questions will be about your reading, such as "How does such-and-such construction work?" or "Is it known whether..." I will ask you to write up the answers and hand them in to me by the end of the semester.

The project will account for 25% of your grade. If you choose to do the final project, you will not need to take the final exam, and you will receive 200-level credit for this course.

Take-home final exam for 100-level credit. The final exam will cover all the material we have gone through during the semester. It will account for 25% of your grade. If you choose to take the final exam, you will not need to do the final project, and you will receive 100-level credit for this course.

Grading. The final grade will be computed as follows:

For 100-level credit	**For 200-level credit**
Weekly problem sets: 60%	Weekly problem sets: 60%
Take-home midterm: 15%	Take-home midterm: 15%
Take-home final exam: 25%	Project: 25%

Tentative plan. Below is a tentative plan for the semester. It indicates when your homework assignments will be due, so as to help you plan your semester. Note that since I want to keep this class interactive, I will adjust both the pace and the material to your requests. As a result, I only list the topics for the first few weeks of the course. You will receive regular updates of this plan.

September

- 9/3, Lecture 1: Introduction, perfect security and its limitation, history of public-key crypto. *Please remember to give me your e-mail address so that I can put you on the mailing list for the course.*
- 9/5, Lecture 2: Common cryptographic assumptions and applications.
- 9/10, Lecture 3: Relevant number-theoretic facts and applications. *Problem set 1 due.*
- 9/12, Lecture 4: Relevant number-theoretic facts and applications, continued.
- 9/17, Lecture 5: Indistinguishability and applications to security. Security for one encrypted bit. *Problem set 2 due.*
- 9/19, Lecture 6: The Goldwasser-Micali cryptosystem.
- 9/24, Lecture 7. Guest lecture. *Problem set 3 due.*
- 9/26, Lecture 8. Guest lecture.

October

- Problem set 4 will be due Tuesday, October 1.
- The take-home midterm exam will begin on Thursday, October 3, and will be due on Thursday, October 10.
- If you are taking the class for 200-level credit, schedule a meeting with me for the week of October 15—19 to prepare a proposal for your final project.
- Problem set 5 will be due on Tuesday, October 22.
- Problem set 6 will be due on Tuesday, October 29.

November

- Problem set 7 will be due on Tuesday, November 5.
- Problem set 8 will be due on Tuesday, November 12.
- If you are taking the class for 200-level credit, schedule a meeting with me for the week of November 11–15, to bring me up to date with what you have done on your final project.
- Problem set 9 will be due on Thursday, November 21.

December

- Problem set 10 will be due on Tuesday, December 3.
- (*Tentative*) The final exams and final projects will be due at the end of the final examination period. The final exam will be posted on the course website on December 12.