CS151: Intro to Cryptography and Computer Security January 28, 2016

Handout 1: Course Information

Instructor: Anna Lysyanskaya

Instructor

Anna Lysyanskaya

E-mail:	anna@cs.brown.edu
Office:	CIT 501
Phone:	37605
Office hours:	Tuesdays 3:30 - 4:30 pm

Teaching Assistants

Grad TA: Apoorvaa Deshpande (acdeshpa@cs.brown.edu)
Hours: Wednesdays, 10 am - 12 pm (CIT 421)
UTA: Nicolas Schank (nschank@cs.brown.edu)
Hours: Mondays, 7 pm - 9 pm (CIT 219)

Course homepage: http://www.cs.brown.edu/courses/cs151/
Course e-mail address: cs151tas@cs.brown.edu

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

- Can a secret message be sent over an unsecured 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 online game? Can Alice and Bob play cards over the Internet?

To answer these questions, we will first decide what security properties 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 emphasis in this course is theoretical. If you are interested in computer security at large, keep in mind that the material of this course 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. CSCI0220 and CSCI0510.
Recommended background. Basic familiarity with algorithms, some number theory, discrete probability, and elementary complexity theory.

Reading. This semester, we will be using *Introduction to Modern Cryptography: Principles and Protocols* by Katz and Lindell, which will be available at the bookstore. In addition, you can find materials from the following books available on-line:

[**GB**] Shafi Goldwasser and Mihir Bellare. *Lecture notes on cryptography.* http://www.cs.ucsd.edu/users/mihir/papers/gb.html

[**HAC**] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography.* Cambridge University Press, 1997. http://www.cacr.math.uwaterloo.ca/hac/

[**Shoup**] Victor Shoup. *A Computational Introduction to Number Theory and Algebra.* http://www.shoup.net/ntb

[**Goldreich**] Oded Goldreich. *Foundations of cryptography. Volume 1: basic tools. Volume 2: basic applications.* Cambridge University Press, 2001 (v.1), 2004 (v.2). http://www.wisdom.weizmann.ac.il/~oded/foc-book.html

Links to these documents can be found on the course webpage, along with other relevant sources.

Problem sets. There will be eleven problem sets spaced evenly throughout the course. (See the course syllabus for the schedule.) Problem sets will be due in the hand-in bin at the beginning of lecture *sharp*. No extensions will be given; this is a firm policy that makes sure that we can post solutions and discuss them in class once you hand in the problem sets. To account for special cases, your lowest problem set grade will be dropped. (Of course, in case something terrible happens, you will also be excused from turning in the relevant homework assignments.)

You are encouraged to collaborate on solving the problems, but the write-up of your solutions should be your own. You must list your collaborators.

You may use external sources, such as books, the web, etc., to help you with the problem sets. You must acknowledge all sources.

The problem sets will account for 60% of your grade.

You should try to typeset your homeworks. LaTeX is especially recommended for it. We will provide a template file for the same.

Midterm exam The midterm will be a week-long take-home exam. The exam will be of approximately 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. The midterm exam will account for 15% of your overall grade.

Final exam The final exam will also be a two-week-long take-home exam. It will cover all the material we have gone through during the semester. It will account for 25% of your grade.

Taking the course for 200-level credit. If you want to obtain 200-level credit for this course, speak to the instructor about it early in the semester.