Instructor: Anna Lysyanskaya  
Email: anna@cs.brown.edu  
Office: CIT 501  
Phone: 37605  
Office hours: TBA

Grad TA: Megumi Ando (mando@cs.brown.edu)  
Hours: Tuesday 12-3PM in CIT 421  
Grad TA: Liz Crites (ecrites@cs.brown.edu)  
Hours: Tuesday 12-3PM in CIT 421  
HTA: Laura Shea (lmshea@cs.brown.edu)  
Hours: Monday and Wednesday 6-8PM in CIT 219

Course homepage: http://www.cs.brown.edu/courses/cs151/  
Course email address: cs1510tas@lists.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 definitions 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.

**Prerequisite** CS 1010 (formerly CS 51).

**Recommended background** Basic familiarity with algorithms, some number theory, discrete probability, and elementary complexity theory.

**Reading** No textbook is required for this course, but links to several suggested readings are provided on the course webpage.

**Problem sets** There will be twelve problem sets spaced evenly throughout the course. (See the online course syllabus for the schedule.) Problem sets will be due in class at the beginning of lecture *sharp*. No extensions will be given; this is a firm policy to ensure that we can post solutions and discuss them in class. To account for special cases, your lowest problem set grade will be dropped.

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. Similarly, 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.

**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. The midterm will account for 15% of your overall grade.

**Final exam** The final exam will 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.

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