COS 433: Cryptography

Fall 2007

Instructor: Boaz Barak (`boaz@cs.princeton.edu`). Office hours: Thursday after class (3pm) or make an appointment by email.

Course times: Tuesday and Thursday, 1:30pm - 2:50pm.

AI: Rajsekar Manokaran (`rajsekar@cs.princeton.edu`)

Before Thursday:

1. Join the course's mailing list.
2. Think how would you make a *precise definition* of a secure (private key) encryption scheme.
3. After thinking about this, read the excerpt from the Katz-Lindell book on the principles of modern cryptography.

1 Course Description

Cryptography or "secret writing" has been around for about 4000 years, but was revolutionized in the last few decades. The first aspect of this revolution involved placing cryptography on more solid mathematical grounds, thus transforming it from an art to a science and showing a way to break out of the *"invent-break-tweak"* cycle that characterized crypto throughout history. The second aspect was extending cryptography to applications far beyond simple codes, including some paradoxical impossible-looking creatures such as *public key cryptography*, *zero knowledge proofs*, and *playing poker over the phone*.

This course will be an introduction to modern "post-revolutionary" cryptography with an emphasis on the fundamental ideas (as opposed to an emphasis on practical implementations). Among the topics covered will be *private key* and *public key* encryption schemes, *digital signatures*, *one-way functions*, *pseudo-random generators*, *zero-knowledge proofs*, and security against active attacks (e.g., *chosen ciphertext security* (CCA)). As time permits, we may also cover more advanced topics such as the *Secure Socket Layer (SSL/TLS) protocol* and the attacks on it (Goldberg and Wagner, Bleichenbacher), *secret sharing*, *two-party and multi-party secure computation*, and *quantum cryptography*.

There are no formal prerequisites for the course, but I will assume that students are able to read and write mathematical proofs. In addition, familiarity with algorithms and basic probability theory will be helpful.

Note about schedule: There may be a lecture or two canceled during the term, in which case there will be make-up lectures during the reading period.

2 Course Requirements and Grading.

Homework There will be weekly homework assignments, handed each Thursday and due at the beginning of class the next Tuesday. You can submit the homework to Rajsekar by e-mail (`rajsekar@cs`), in his mailbox, or by hand in the beginning of the lecture. (The preferred method is electronic submission of LaTeX-typeset homework.) The homework will count for 50% of the course grade (see below).

Flexibility in homework: (1) The total points on many assignments will be more than 100. This means that if you obtained say 120 points on the first assignment, and 80 points on the second assignment you can still get a perfect score on the homework. Sometimes these "bonus" questions (which may be harder or take more time to do) will be explicitly identified and sometimes not. **(2)** You have a total of 4 late days to submit your homework throughout the term. Note that part of a day counts as a full day. Beyond that there will be no credit (even not partial) on the homework except in extraordinary circumstances.

Important note: There will be no flexibility on the quality of answers. I expect accurate and well written answers (although not Pulitzer-winning essays...).

Final: There will be one take home final in the course, counting for 50% of the grade.

Collaboration policy: Collaboration with other *students* on homework exercises is encouraged. However, each student should write on his/her own the solutions, and should not look at other student's written solutions. Also, if an idea for a solution came from a different student or another source, you should give proper credit to the student/source. Using preexisting solutions from previous years of this course or similar courses of other institutions is *strictly prohibited*.

Course grade: The course grade will be 50% based on the homework grades and 50% on the final grade.