COS 433: Cryptography

Fall 2005

Instructor: Boaz Barak (`boaz@cs.princeton.edu`). Office hours: Thursday after class (3-4pm) or make an appointment by email.

Times and place: Tuesday and Thursday, 1:30pm - 2:50pm, room 102 in Computer Science bldg.

AI: David Xiao (`dxiao@cs.princeton.edu`)

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. I recommend that CS majors take this course after COS 226 and COS 341. If you're interested in the course but are not sure you have sufficient background, or you have any other questions about the course, please contact me at **boaz@cs.princeton.edu**.

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 Tuesday and due at the beginning of class the next Tuesday. You can submit the homework to Dave by e-mail (`dxiao@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 6 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. **(3)** In the calculation of the final grade I will discard the assignment on which you received the lowest grade.

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

Project: There will be one project in the course, with several phases which will stretch throughout the term. More details about the project and the schedule for its different phases will be provided later. You may work on it in groups of 1–3 students. The project will involve a realistic security application, preferably chosen by you (but with my guidance and advice). It is not a programming project and will likely not involve programming (although you may choose to add a programming component to it). The project counts for 25% of the course grade, but I reserve the right to raise the final course grade by any amount for truly outstanding projects.

Final: There will be one take home final in the course. You may work on it in a 24 hour period of your choice from the start of the winter recess (December 16th, 2005) to the end of the reading period (January 17th, 2006). The final counts for 25% of the course 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*.

Collaboration on the project should be only within the group. Work on the final should be done alone and as directed.

Course grade: The course grade will be based on a numeric grade X between 0 and 100 which is computed as follows: let the homework grade H be the average of your homework grade, not including the lowest-graded assignment. If $H > 100$ we let H be 100. Let P be your project grade, and F be the final grade (again if $F > 100$ we let F be 100). We compute $X = 0.5H + 0.25P + 0.25F$. I will translate X to a letter grade based on a reasonable scale to be determined later. However, as mentioned above I may raise the final letter grade for students that submitted truly outstanding projects.