General Information

Lectures: Wednesday 5-7pm, WWH (Courant) 312. Instructor: Prof. Yevgeniy Dodis
Email: dodis@cs.nyu.edu; Phone: 212-998-3084; Office: WWH (Courant) 413
Office hours: Wednesday 7-8pm and by appointment.

Course Web Page: All course materials, handouts, homework and announcements will be available here. You should plan on visiting this page regularly and often!

Mailing list: http://www.cs.nyu.edu/mailman/listinfo/g22.3220-001_fa09
To post a message to all the list members, send email to g22.3220-001.fa09@cs.nyu.edu.
Please, post only messages interesting to everybody taking the class. Specific class-related questions and most of your other correspondence should be directed to the instructor.

Signup Sheet (.ps,.pdf): Please fill it and return to me within the first week of the course.

Prerequisites

This is an advanced course in cryptography. As such, it will assume basic familiarity with notions such as symmetric-key encryption, symmetric-key authentication (e.g., MACs), public-key encryption, digital signatures, pseudorandom functions, block ciphers, collision-resistant hash functions and commitments. However, we will review the needed notions as we move along. In particular, from past experience Math PhD students usually do well in the course, even without taking the Introduction to Cryptography class. However, it is a good idea to read the Lecture Notes for the basic cryptography course, to check (or learn!) the material we might use.

No programming will be required for the course. Finally, knowledge of LaTeX (which is easy to acquire; see LaTeX Tutorial) is essential for producing the scribe notes and, possibly, for the final project.

Grading

The grade will be composed from four factors:

- **Homework**: there will be one or two homework assignments. Each homework will be due no earlier than 2 weeks since it is assigned.

- **Scribe Notes**: each student will be expected to produce scribe notes for one (or two) lectures. Of course, I will help in the process to answer questions unclear from the lecture. The student is required to produce the first draft one week after the lecture, and the final draft two weeks after the lecture.

- **Final Project**: each student will be required to read one or two related research papers from a recent CRYPTO/Eurocrypt/TCC conference and write a 5-10-page summary of what was learned. The paper should be chosen at least 3 weeks before the end of the course.
• **Class Participation.** I want to keep this class interactive and you interested in the material. Therefore, questions (including “stupid questions”, whatever that means) and other constructive participation is encouraged. Also, feel free to tell me if I am going too fast or too slow.

**Textbooks**

There will be no textbooks. However, I will assign research papers for some lectures. Hopefully, scribe notes will also be available with little delay. Please consult the [Reading](http://cs.nyu.edu/courses/spring07/G22.3220-001/) section on the web site for more information. Another great resource are the notes from the last edition of this class: check [http://cs.nyu.edu/courses/spring07/G22.3220-001/](http://cs.nyu.edu/courses/spring07/G22.3220-001/).