General Information

Lectures: Wed 5-7pm, WWH (Courant) 201. Final: TBA.
Instructor: Prof. Yevgeniy Dodis; Email: dodis@cs.nyu.edu; Phone: 212-998-3084;
Office: WWH (Courant) 413;
Office hours: Wednesday 3-4pm and by appointment.
Teaching Assistant: Dario Fiore; Email: fiore@cs.nyu.edu; Phone: 212-998-3093; Office: WWH 408;
Recitation and Office Hours: Tuesday 7-8pm, room 512 WWH.


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/csci_ga_3210_001_sp12
To post a message to all the list members, send email to csci_ga_3210_001_sp12@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/TA.

Signup Sheet: Please fill it and return to me within the first week of the course.

Prerequisites

No advanced mathematics background is assumed. However, students are expected to be somewhat comfortable with mathematical proof techniques (“mathematical maturity”), be at ease with algorithmic concepts, and have elementary knowledge of discrete math, number theory and basic probability. A brief review of relevant topics will be given as needed during the course, making it possible to follow the material. “Mathematical maturity” means simply that you have had exposure to proofs and know what distinguishes a formal proof from a convincing argument. Although we will not do too many formal proofs in class, you should be comfortable with thinking about things in an abstract way. No programming will be required for the course.

Finally, learning cryptography involves a great deal of curiosity, creativity and originality. Please bring those along...

Grading

Grading will be based on the problem sets, the final exam and class participation. Tentative grade split is roughly 50% homework and 50% final exam, plus minus 10% for class participation.
**Problem Sets.** Problem sets will be due at the beginning of lecture. *Homework without priorly obtained extension will not be accepted.* I strongly prefer typed homework solutions. In fact, I encourage you to use Latex for your solutions. In addition to be legible and readable, such homework is not losable and can be submitted over e-mail. Additionally, in case you are not familiar with latex, this will you with the opportunity to learn this extremely useful tool. To encourage you even further, **we provide you with a self-explanatory Latex template together with each homework.** All you have to do is to fill in your solutions in the places marked! Finally, here is a brief Latex tutorial to get you started. Worst comes to worst, *if you write by hand*, write neatly!

**Final Exam.** Most likely, the final exam will be in class and will be closed book. I’m entertaining the option of giving a take-home final, and also giving the option to do a research project in place of the final exam. These will be decided later.

**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 is no text book for the course. However, a lot of the material can be found in the following excellent books:

- **Introduction to Cryptography**, by Jonathan Katz and Yehuda Lindell. This book is introductory, and I recommend that you purchase this book.

- **Graduate Course in Applied Cryptography**, by Dan Boneh and Victor Shoup (book in progress). More information about the book is available at [https://crypto.stanford.edu/~dabo/cryptobook/](https://crypto.stanford.edu/~dabo/cryptobook/). There is the latest pdf file at the bottom of the page. It requires secure access. The user name is crypto. I will tell the password in class. This book is more advanced.

Additionally, up to date Lecture Notes will be provided on the course’s web site. They will be based on similar (but modified) Notes from previous class, so feel free to look ahead to see what we will cover next. When needed, I might give additional handouts, or point to appropriate places on the web. I will send email to the class mailing list when this happens. Finally, try to take good notes! Please contact the Reading section on the web site for more detailed information and other suggestions.

**Problem Set Policies**

Some of the homework exercises will be routine, but others will be more challenging. I do not expect you to solve all of the homework problems, but I hope that you will benefit from working on the more difficult ones. A few hints on the homework assignments:

- **Start early.** Difficult problems are not typically solved in one sitting. Start early and let the ideas come to you over the course of a few days.

- **Be rigorous and precise.** Each problem has a (sometimes unwritten) requirement that you argue why your solution is correct, or that you justify your calculations. To obtain full credit for a problem, it is necessary to fulfill these requirements. Please, no ”hand waving”, or a long line of numbers coming from nowhere.
• **Be concise but not sloppy.** Express your solutions at the proper level of detail. Give enough details to clearly present your solution, but not so many that the main ideas are obscured.

• **Collaboration?** You are encouraged to solve all the homework questions on your own, but are permitted to brainstorm difficult problems in small groups (up to three students), as long as each of you writes the solutions individually and honestly acknowledges the cooperation. Needless to say, if you work with others but never come up with the solution on your own, you may do OK in the homework component of your grade, but you will suffer on the exam, so be careful. On the other hand, if I detect cheating, the consequences will be devastating, so I do not recommend it.

• **Bibles? Help?** More or less, you are only allowed to use the lecture notes and the textbooks suggested in the Reading section. In particular, the use of internet, course bibles, outsiders, and other clearly “cheating” resources is strictly prohibited. Please talk to me if you are having problems keeping up with the material.