Brown Math 1580 Fall 2011 Syllabus

Instructor: Chris Kottke
Office: #303 Kassar-Gould House
Email: ckottke@math.brown.edu

Course website: http://math.brown.edu/~ckottke/1580/

Office hours: WF 2-3pm, or by appointment.

Text: *An Introduction to Mathematical Cryptography*, by Hoffstein, Pipher, & Silverman. Springer. ISBN: 978-0-387-77993-5.

Exams:

- Midterm: Friday Oct. 21, in class.
- Final: Tuesday, Dec. 13, 9am.

Grading: Your final grade will depend on weekly homework scores and exams (1 midterm and 1 final), weighted as below. Your lowest homework score will be dropped. The final will be about 1/3 cumulative material and 2/3 new material.

Homework	30%
Midterm	30%
Final	40%

Description: This class will be an introduction to the theory of mathematical cryptography. While we will discuss symmetric key cryptography, the main focus is on the difficult mathematical problems which underlie asymmetric (public key) cryptography.

These problems include the discrete logarithm problem (ElGamal & Elliptic Curve Cryptography), integer factorization (RSA) and the Shortest Vector Problem (NTRU).

In the course of studying these problems, we will consider what it means for a mathematical problem to be considered difficult, what are some of the best known algorithms for solving such problems, and how they may be exploited for cryptographic purposes.

Topics will include modular arithmetic, finite fields, discrete logarithms, Diffie-Hellman key exchange, ElGamal, integer factorization, RSA, an introduction to probability and information theory, elliptic curves, lattices, and digital signatures.

Course Policies:

- **Homework:** Homeworks may be turned in during class, or turned in to the appropriate box in the math department mailroom, **by 4pm on the due date.** Collaboration on homework assignments is allowed, and indeed encouraged. This means discussing problems, solution techniques, and comparing individual answers, **not copying answers.** Each student must write up their own homework individually. **Please cite your collaborators and references used (apart from the textbook) on your homework assignments.**
- **Missed/Late assignments and exams:** Late homework will not be permitted, except in cases of emergency accompanied by a note from the Dean's office. If you have a conflict, please arrange to turn in your assignment early, or use it as your lowest homework score to be dropped. A missed exam may be made up only in the case of an emergency; the make up will be an oral exam and may be more difficult than the original.
- **Grade disputes:** Please check over your exams and assignments when they are returned to you for any grading mistakes and I will correct them. **Grade disputes will be considered for one week following the return of an assignment.** After one week, the grade is set.
- **Calculators:** You may use a basic calculator (limited to addition, subtraction, multiplication and division) on exams if you wish. **No scientific or graphing calculators or smartphones permitted.** However, the exams will be designed so that any computation can be reasonably done by hand, and arithmetic mistakes will not be unfairly punished when grading.

Tips for success:

- **Read the relevant material before class.** I will put sections of the book corresponding to each lecture on the website a day or so beforehand. You do not need to fully understand everything, however, having some familiarity with the subject of the lectures beforehand is extremely valuable. You will definitely get more out of each lecture this way.
- **Come to office hours.** Identify anything you don't understand very well, and ask me about it. This is an invaluable time to address individual questions that you have; there are no stupid questions! Also, if you have any questions or interests that go beyond the scope of this course, I'm more than happy to discuss these in office hours as well.
- **You are your own teacher.** You are ultimately responsible for your own learning, and you know best what material you understand well and what material you feel a little hazy about. Don't let yourself get away with the latter! While you're encouraged to work on homework assignments in groups, it is your responsibility to make sure you're not just leaning on your friends.
- **Think about and do math!** Really understanding mathematics takes time and practice. The homework assignments are not just for grading purposes, they're meant to give you an opportunity to dig into the material and develop your skills and intuition. While I'll drop your lowest homework grades (because once in a while you'll have a bad and/or crazy week), not spending any time working on a particular assignment is a Very Bad Idea. So too is waiting until Thursday night to begin the assignment. You will get the most out of each homework by starting early and letting the problems roll around in your brain for a while.