Math 302 – Advanced Cryptography – Course Policies

PROFESSOR: Tommy Ratliff, Science Center 1309, x3968
EMAIL: ratliff_thomas@wheatoncollege.edu
HOME PAGE: http://tratliff.webspace.wheatoncollege.edu
OFFICE HOURS: Posted on webpage
And by appointment (Really!)
TEXT: *An Introduction to Mathematical Cryptography, 2nd Edition*
by Hoffstein, Pipher, and Silverman

Overview

This course is a follow-up to Math 202 Cryptography. During the first half of the semester, we will revisit a few of the topics from Math 202 to fill in some of the more mathematically sophisticated details, such as primality testing, attacks on the DLP, and considerations of computational complexity. After Spring Break, we will look at some new topics, including elliptic curve cryptography and lattice-based systems that are not susceptible to any known attack by quantum algorithms.

This is going to be a really fun semester!

Course Goals and Expectations

One of the primary goals of the course is that you improve your ability to communicate mathematics clearly and precisely, both in writing and verbally. Mathematics is a very personal discipline that is best learned by *doing* rather than by observing. Learning to write precise and complete mathematical arguments is a challenging endeavor, but the process will not only aid your mathematical development but can also greatly improve your clarity of thought in other disciplines and contexts as well.

One of the features that makes your Wheaton education so special is that we have face-to-face time in small classes to explore material together. You should look at the Tentative Daily Syllabus and the Detailed Reading Assignments on the course webpage before each class meeting. Because we covered some of the material in the text in a different context in Math 202, we'll be able to skip some parts of this semester's text. You will probably not completely understand all of the content from this first reading, but the class meetings will be much more valuable if you are already familiar with some of the basic ideas. The class meetings are not intended to be a complete encapsulation of the course material, but instead they will focus on the major concepts and clarifying the more subtle ideas in the course.

You should expect to put in at least 3 hours outside of class for each hour in class. In other words, expect to spend about 9 hours per week on Advanced Cryptography outside of class. There will be some weeks where you spend more time, and there may be some weeks where you spend slightly less.

The Honor Code

We operate under the Honor Code for all of your academic work at Wheaton. This carries certain freedoms and responsibilities for both you as a student and me as a professor. I take this quite seriously.

Most likely, no Honor Code issues will arise this semester. If you are uncertain about whether a particular situation falls under the Honor Code, then please consult with me. However, if an Honor Code issue does come up, I will assume that you are prepared for the full consequences. Remember that you should write out, and sign, the following statement on all course work:

> "I have abided by the Wheaton College Honor Code in this work."

Working with Other Students

I strongly encourage you to work with other students outside of class because I believe mathematics is best learned through collaboration. However, you should not turn in identical work to your partner(s); the answers that you give to the homework assignments should represent your own thinking about the solutions.

You should cite anytime that you work with another student on a Problem Set. If you fail to do this, it will be viewed as a violation of the Honor Code.

See the Guidelines for Problem Sets on the course webpage for complete details.

Evaluation

Your final grade will be determined by

Two In-Class Exams	35%
Comprehensive Final Exam	20%
Problem Sets	30%
Cryptanalysis Challenges	10%
Group Presentation	5%

Exams

The two exams during the semester will be given in the evening so that you are not constrained by the 50 minute class period. See the Tentative Daily Schedule on the course webpage for the dates of the exams. The comprehensive final exam will be given during the scheduled exam period.

Problem Sets

You will have a Problem Set due most Wednesday at 3:00 pm. I will not accept any homework after this time with one exception: I will allow you to turn in *one* homework assignment late during the semester. You do not need to give me any justification, but you must inform me via email before noon on the day that the homework is due that you intend to take advantage of your one late assignment. The late assignment is due at 3:00 pm on the following Monday.

The course webpage has the specific assignments, due dates, and details on the grading and expectations for the presentation of your assignments. We will use the same grading system for your problem sets as in Math 202.

Cryptanalysis Challenges

These assignments will take two forms: (Approximately) biweekly challenges and participation in a national undergraduate cryptanalysis contest during April 13–17. In both cases, you will be given a cipher text, and your goal is to recover the original English text. For the biweekly challenges, you will work in groups of two or three that I assign. For the contest, you will work in groups of two or three of your own choosing.

An important point to note about these challenges: *I do not expect that you will break every cipher!* It's great if you do, but you can receive full credit on these assignments even if you do not find the original text.

You should plan to spend approximately 3–4 hours working with your partner on each biweekly challenge. You will turn in a one to two page writeup that explains either the solution, if you found it, or the different approaches you attempted if you were unable to break the cipher. In the latter case, you will be evaluated on the quality of your failure.

I will give more details about the April contest as the time gets closer.

Group Presentations

There are many interesting applications of cryptography outside of the text that we should all know more about, and you'll get to explain one of these to the rest of the class! You will form groups of two or three of your own choosing, and your group will be responsible for a class meeting to discuss your topic. Some possible topics include applications of block chain schemes, quantum algorithms and quantum computing, tokenization in systems like Apple Pay, homomorphic encryption, etc. I've set aside three days during the semester for these class meetings, and I will work with you to find resources and to prepare for your presentations.

Class Attendance

Although class attendance is not a specified percentage of your grade, I will keep a class roll to help me determine borderline grades at the end of the semester. If you do miss class, you are responsible for the material that was covered.

Accommodations for Students with Disabilities

Wheaton is committed to ensuring equitable access to programs and services and to prohibit discrimination in the recruitment, admission, and education of students with disabilities.

Individuals with disabilities requiring accommodations or information on accessibility should contact Abigail Cohen, Disability Services Specialist at the Filene Center for Academic Advising and Career Services: cohen_abigail@wheatoncollege.edu or (508) 286-3794.

Getting Help

Please come see me during my office hours! If you have a conflict and cannot make my office hours, please email me and we can set up an appointment for another time.