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 part 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. Later in the semester, 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!

Goals for a 300-level Mathematics Course

There are several primary objectives of any 300-level math course at Wheaton. By the end of this semester you should:

- Be able to formulate a concise, precise mathematical arguments and proofs, including recognizing when it is complete or when further justification is needed
- Be able to read and communicate advanced technical concepts
- Be willing to approach a problem even if you do not know whether or not your approach will be successful. If it doesn't work out, try something else!
- Appreciate the necessity of rigorous mathematical arguments
- Continue in your development from being a *consumer* of mathematics to being a *producer* of mathematics

Goals Specific to Cryptography

You should gain a deeper understanding of:

- The distinction between a theoretic solution and a practical solution
- The interplay between applications and theoretical mathematical results
- How to generate parameters, including large prime numbers, used for RSA, DHKE, and DSA
- Attacks to solve the Discrete Log problem, including Pollard's ρ method
- The underlying group structure of elliptic curves and how this is used in elliptic curve cryptography
- The basic theory underlying lattice-based systems such as GGH and NTRU

Expectations

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 on the course webpage and skim the section(s) from the text before each class. 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 a roughly 9 hours per week on 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."

Evaluation

Your final grade will be determined by

Two Mid-Semester Exams	35%
Comprehensive Final Exam	20%
Problem Sets	30%
Cryptanalysis Challenges, Kryptos 2019, And Group Presentation	15%

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 afternoons at 3:00 at the end of my office hours. I firmly believe that one of the best ways to build your understanding of mathematics is to explore the ideas with other students. Therefore, you will work on the Problem Sets in groups of two, and each group will turn in a single set of solutions. I will randomly assign new groups for every problem set. There are more details about the logistics of the Problem Sets on the course webpage.

Cryptanalysis Challenges and Kryptos Contest

There will be three Cryptanalysis Challenges during the semester, and you will participation in Kryptos 2019, a national undergraduate cryptanalysis contest during April 4–8. In both cases, you will be given a ciphertext, and your goal is to recover the original English plaintext. For the Cryptanalysis Challenges, you may work alone, or in groups of two or three of your choosing. For the Kryptos 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 plaintext. You should plan to spend approximately 3–4 hours on each Cryptanalysis Challenge. You may certainly use computing tools to help in your analysis, but you should thoroughly explain the process for breaking the cipher.

Each group will turn in a one to two page writeup that explains your analysis that allowed you to find the plaintext 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 Kryptos 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 give a 15–20 minute presentation during the week of April 22. Some possible topics include applications of block chain besides cryptocurrencies, Shor's algorithm, quantum computing, tokenization in systems like Apple Pay, homomorphic encryption, etc. I'll give more details about the presentations during the semester.

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.

Getting Help with Cryptography

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. It's best if you look at my schedule on my webpage and suggest a couple of times that we both have free.

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 Autumn Grant, Associate Director for Accessibility Services at the Filene Center for Academic Advising and Career Services: accessibility@wheatoncollege.edu or (508) 286-8215.

Campus Counseling Center

The Counseling Center is a confidential resource on campus for all students, providing short term solution focused therapy, case management, emergency services and support. The Counseling Center is open Mon-

day – Friday, 8:30 - 12:30 and 1:30 - 4:30. Students can call (508-286-3905) or stop by 42 Howard Street (the white building between Beard and Art Haus) to make an appointment or seek emergency services during office hours.

Counseling Center staff is available to support students with a wide range of challenges including, but not limited to, anxiety, depression, sleeping and eating concerns, identity exploration, substance use and concentration challenges. The Center welcomes any student to come and have a discussion regarding what their needs are, and the Center will help with next steps of care, whether here on campus, or locally off campus. Outside of office hours, mental health concerns and emergencies should be directed to the Area Coordinator On Call via calling Public Safety at x3333 or 508-286-3333.