Math 302 – Advanced Cryptography – Course Policies

Professor:	Tommy Ratliff
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 attacks on the Discrete Log Problem, primality testing, 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 Shanks Babystep-Giantstep algorithm, the Pohlig-Hellman algorithm, and 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

Expectations

One of the features that makes your Wheaton education so special is that we have time in small classes to explore material together. The class meetings are not intended to be a complete encapsulation of the course material, but instead will focus on the major concepts from the readings and videos to clarify the more subtle ideas in the course.

You should expect to put in about 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 the scheduled class meetings. 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 Wheaton 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

Pre-Class Assignments	10%
Class Participation	10%
Problem Sets, Group Presentation, & Kryptos Contest	40%
Three Take-home Exams	40%

Pre-Class Assignments

The purpose of reading the text and watching the assigned videos *before* class is that if you are familiar with the basic concepts and definitions, then the class meetings can be devoted to the major ideas and subtleties of the material. Mathematical understanding is built in stages, and you will absorb the material more quickly if the class meetings are your *second* exposure to the fundamental ideas.

The Pre-Class Assignments are posted on the course webpage and include three or so questions that you should be able to answer after you have completed the reading and viewed any videos. You will submit your responses through Wheaton onCourse.

I will grade the Pre-Class Assignments using a binary scale: If you make a serious attempt, you will get full credit, even if your answers are not completely correct. The purpose of these questions is to encourage you to engage with the material before class. If you've read the text and watched any videos but don't understand how to answer a question, it is perfectly fine to say "I did the prep work but don't see how to approach this question." You'll definitely understand by the end of the end of the week!

Notice that the Pre-Class Assignments are due at midnight on Sunday! This will give me enough time to review your responses before our class on Monday morning. You will be allowed to drop one Pre-Class assignment at the end of the semester.

Class Participation

The tutorial meetings will be devoted to working in small groups on problems that delve more deeply into the content introduced in the Pre-Class Assignments and Monday class meetings. In previous years, you would have worked in groups at the chalkboards. Since that's not an option this semester with social-distancing requirements and some of us being remote, for each tutorial meeting I will set up a shared Google Jamboard, which is a virtual whiteboard that you'll have access to via your Wheaton email account.

Each group will have their own "frame" on the Jamboard, and you should post your work at the end of the tutorial there. If you have a digital pen, you can write directly on it, or else you can take a photo of your paper and upload it to your frame. I will also grade your group's work using a binary scale: You made a serious effort or you didn't.

Problem Sets

You will have approximately five Problem Sets due during the semester. 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, or possibly three, 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 and expectations for your write-ups of the Problem Sets on the course webpage.

Group Presentation

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 three of your own choosing, and your group will give a 20 minute presentation during last week of class. I will give more details about the Group Presentation during the semester.

Kryptos Contest

You will participation in Kryptos 2021, a national undergraduate cryptanalysis contest held April 22–26. For this contest, you will work in groups of two or three of your own choosing. The idea of the contest is that you will be given a ciphertext, and your goal is to recover the original English plaintext. I will also give you several problem in your Problem Sets to help you practice for Kryptos.

An important point to note about these problems: *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 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.

Take-home Exams

The purpose of the exams is for you to demonstrate your understanding of the course material and, just as importantly, to give you feedback on where your understanding is strong and where you may need more work. Similar to last fall, the exams will be open-note take-home exams where you will have several days to work on them. See the *Tentative Daily Syllabus* on the course webpage for dates of the exams. I will provide more details about the structure of the exams as the time gets closer.

I know that exams can be stressful, especially with the other academic, extracurricular, and family commitments that you may have. To try to reduce some of this stress concerning your grade, I will weight your exam scores by differing amounts: Your lowest exam score will count 20% of your exam grade, the second lowest will count 30%, and the highest will count 50% of your exam grade. For example, if your four exam scores are 71, 82, and 93, then your overall exam average will be 85.3.

Getting Help with Cryptography

Please come see me during my drop-in office hours! No appointment necessary! All office hours this semester will be remote, and the Zoom link is posted to onCourse. If you have a conflict and cannot make my office hours, please email me and we can set up an appointment for another time.

Having difficulty accessing the tech you need?

The Hybrid Tutorial Model and its remote components require you to have access to specific technologies in order to complete your classwork successfully. If you are having trouble accessing the learning technologies for this class or reliable wifi or computer access, please let me know and then reach out to your Student Success Advisor in Academic Advising for help with acquiring material or software. You can use this form to report your technology needs - Learning Technology request form:
https://forms.gle/hMXJdBkBQtU1NzzU8

Accessibility at Wheaton

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

Wheaton Student Support & Wellness Resources

The Counseling Center is the confidential and free mental health resource on campus for all students. To learn about services, check out the website, or give the office a call at 508-286-3905. Even when the Counseling Center is closed, or staff are unavailable, *After Hours Mental Health Support* is available by calling the front desk 508-286-3905 and following voicemail prompts to be connected to a clinician (24/7, available in languages other than English, and accessible from anywhere you are in the world).

The Filene Center strives to support your learning pathway by fostering successful academic, career, and personal development. The academic advising staff will work collaboratively with you, faculty and campus resources to ensure that you have the access and guidance to become a confident and reflective learner at Wheaton and beyond. You may contact them at advising@wheatoncollege.edu.

Many other offices on campus can also help support the holistic wellness of students. For students who identify as low-income, first-gen, LGBTQ+, or have a faith or spiritual practice they adhere to, the Center for Social Justice and Community Impact and Center for Religious and Spiritual Life (the Base) are good places for support and engagement. The Marshall Center for Intercultural Learning supports BIPOC students and those working towards breaking down barriers across difference, and the Center for Global Education supports international students, and students seeking educational opportunities abroad. We encourage you to reach out to any and all of these offices for support.

Health Services through Norton Medical Center is available to support students with a variety of physical health needs including specialty support for GYN and STI care. Contact the office at 508-286-4500 to make an appointment for care. There is no copay for visits and most services are free, with select procedures and labs billed to insurance.