Math 202 – 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:	*Understanding Cryptography* by Paar & Pelzl

Overview

Cryptography is the study of encrypting and decrypting messages in a way that keeps the information secure so that only the sender and receiver can understand the message. While there is a rich history of cryptography going back thousands of years, modern networks demand security on a level that was unimaginable even 50 years ago. We will focus on understanding the mathematics underlying many of the modern cryptosystems, including the symmetric key system AES and the public key systems RSA and Elgamal. In addition, we will also study digital signatures, hash functions, and the applications to blockchains, such as Bitcoin, Ethereum and Beefchain (yes, that's a real thing).

This is going to be a really fun semester!

Goals for a 200-level Mathematics Course

There are several primary objectives of any 200-level math course at Wheaton. By the end of this semester you should:

- Be able to formulate a concise, precise mathematical argument, 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:

- How the security of modern communication depends on sophisticated mathematical concepts
- When a theoretic result gives a practical real-world solution, and when it does not
- The distinction between theoretic and practical security
- The advantages, and disadvantages, of symmetric and asymmetric encryption systems
- The mathematics underlying AES, RSA, Diffie-Hellman key exchange, Elgamal encryption, and DSA
- The reason for digital signatures and message authentication codes
- How the methods discussed this semester fit together in the TLS and blockchain protocols

Structure of Class Meetings

This semester is going to be unlike any that we've experienced before, because, well, 2020.

- Some of us will be remote for the entire semester.
- Those who plan to be in-person for classes may need to be remote for some period of time due to self-isolation or quarantine, including me!
- Our classroom is not large enough to hold all on-campus students and maintain social distancing.
- We need to be prepared if circumstances require us to shift the class to be completely remote.

This makes it impossible for the entire class to meet in-person at once. As a result, we're going to need to adjust the structure of scheduled class meetings, office hours, exams, etc. to meet the realities of this semester. We'll follow the Hybrid Tutorial model for Cryptography. The goal is that much of the content delivery will occur asynchronously outside of class meetings via reading assignments and short videos. This will allow us to devote most of the class meetings to smaller tutorials of 10-13 students where you are collaborating in groups and working on problems to clarify concepts and delve deeper into the subtleties of the content.

The plan for class meetings is:

> Monday, 12:30 - 1:10: Entire class meets via Zoom
> Monday, 1:10 - 1:50: Tutorial Group A meets via Zoom
> Wednesday, 12:30 - 1:10: Tutorial Group B meets in SC 1314
> Wednesday, 1:10 - 1:50: Tutorial Group C meets in SC 1314

Remote students will be in Tutorial Group A, and Tutorial Groups B & C will meet mask-to-mask in the classroom. The tutorial group assignments for each week will be posted to onCourse.

As the term goes on, we might have to make some adjustments to the structure of the class, depending on how things are working. This means that you should not plan any other commitments during our scheduled class time.

Let's all be kind to each other, and we'll figure it out.

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 reading and clarifying the more subtle ideas in the course.

You will have a Pre-Class assignment due every Sunday at midnight that introduces the content for the week. The assignments will consist of reading sections from the text, possibly watching short videos, and posting answers to a few short questions to onCourse. It is **extremely** important that you complete the assignments on time. The purpose of the pre-class assignments is to shift some of the delivery of content outside the class meetings so that you can build your understanding more deeply during the interactions in class.

You should expect to put in at least 2-3 hours outside of class for each hour in class. In other words, expect to spend a roughly 8 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 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 and Partner Evaluation	40%
Three Take-home Exams	40%

Pre-Class Assignments

The purpose of reading the text *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 get 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 class meeting!

Notice that the Pre-Class Assignments are due at midnight on Sundays! This will give me enough time to review your responses before our Monday class meetings. 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 you working in small groups on problems that delve more deeply into the content introduced in the Pre-Class Assignments. In previous semesters, 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, I will set up a shared Google Jamboard for each class, 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 daily Jamboard, and you should post your work for the in-class problems 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. You may not complete all of the problems during your tutorial session, but your group should work to complete these after class and post them to your frame before Thursday at midnight. I will also grade this work using a binary scale: You made a serious effort or you didn't.

There may be some short additional assignments that you will post to the onCourse discussion boards that will count as part of your Class Participation grade.

Problem Sets

You will have a Problem Set due most Wednesdays at midnight. 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 of the Problem Sets on the course webpage.

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. Since we cannot meet together as a group this semester, all of 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 office hours! 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 students to have access to specific technologies in order to complete classwork successfully. Having trouble accessing the learning technologies outlined in this syllabus? Or reliable wifi or computer access? First, work with all your professors to clarify requirements. Next, reach out to your Student Success Advisor in Academic Advising for help with acquiring material or software. 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. Contact us 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 Learningsupports 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.