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

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 chapter 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 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 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 In-Class Exams	35%
Comprehensive Final Exam	20%
Problem Sets	45%

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 Friday mornings at 9:30 at the beginning of class. 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.

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 Susan Friedman or Kristine Smith, interim Accessibility Services Specialists, 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 Monday – 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.