Syllabus and Information for Math 110
Applied Number Theory and Field Theory

Spring 2019

Instructor: Jacob Fox
jacobfox@stanford.edu,
Office: Building 380, Room 383-K

CA: Rodrigo Sanches Angelo
rsangelo@stanford.edu
Office: Building 380, Room 384-M

Time: Monday, Wednesday, Friday
10:30am - 11:20am

Location: Building 380, Room 380-F

Office hours: Fridays 3:00pm - 5:00pm (Jacob)
Wednesday, Thursday 2:00 - 3:30 (Rodrigo)
or by appointment

Textbooks: "An Introduction to Mathematical Cryptography"
by Hoffstein, Pipher, and Silverman (Required)

Introduction to Cryptography (with Coding Theory) by Trapp and Washington (Not required)

Grades: Take-home Midterm 20%, Homework 20%, Final exam: 30%, WIM paper 30%

Objective: To learn and appreciate number theory and field, and its applications in cryptography and coding theory.

Description:

Math 110 will cover basic concepts in number theory, field theory, and applications, mostly to cryptography and coding theory. Topics include: primes, factorization, modular arithmetic, finite fields, symmetric key cryptosystems, RSA, Diffie-Hellman, elliptic curves, and some additional topics to be decided based on student interest.

Math 110 is a Writing in Major (WIM) course so a significant amount of emphasis will be put on learning clear mathematical exposition. Students will be expected to write clear solutions on homeworks and exams. Additionally, there will be a writing assignment for which students will be expected to provide context and set up for a piece of mathematical exposition.

Suggestions: Class participation and discussion are highly encouraged.

Course page: stanford.edu/~jacobfox/110Spring2019.html
Homework: 4 homeworks (about one every two weeks)

The homework problems form an integral part of the course; they are easily the most reliable check of your progress in assimilating the material in a manner which is sufficiently deep to allow you to solve problems which are at least one level removed from routine application of definitions and formulae. While it is quite O.K. (and even encouraged) for you to discuss the problems in general terms with your peers, it is expected that what you hand in is your own work, and not a joint project of several people; i.e. you may NOT systematically work together with others on writing up solutions to the homework problems, and such behavior would constitute a violation of the Honor Code.

Honor Code: Please be sure you are aware of the requirements of the Stanford Honor Code and your responsibilities under the code.

Tentative Schedule:

Week 1, 4/1: Introduction to Cryptography and Modular Arithmetic, 1.1-1.4

Week 2, 4/8: Introduction to Cryptography and Modular Arithmetic, 1.5-1.7
Homework 1 due

Week 3, 4/15: Discrete Logarithms and Diffie-Hellman, Chapter 2

Week 4, 4/22: Integer Factorization and RSA, Chapter 3
Paper outline
Homework 2 due

Week 5, 4/29: Digital Signatures, Chapter 4
Take home midterm

Week 6, 5/6: Combinatorics, Probability, and Information theory, Chapter 5
Homework 3 due

Week 7, 5/13: Error correcting codes
First draft of paper

Week 8, 5/20: Elliptic curve cryptography, Chapter 6
Homework 4 due

Week 9, 5/27: Elliptic curve cryptography continued, Chapter 6
(No class 5/27 - Memorial Day)

Week 10, 6/3: Additional topics
Take home final
Final paper

Students with Documented Disabilities
Students who may need an academic accommodation based on the impact of a disability must initiate the request with the Office of Accessible Education (OAE). Professional staff will evaluate the request with required documentation, recommend reasonable accommodations, and prepare an Accommodation Letter for faculty dated in the current quarter in which the request is being made. Students should contact the OAE as soon as possible since timely notice is needed to coordinate accommodations. The OAE is located at 563 Salvatierra Walk (phone: 723-1066, URL: http://oae.stanford.edu).

Affordability of Course Materials
Stanford University and its instructors are committed to ensuring that all courses are financially accessible to all students. If you are an undergraduate who needs assistance with the cost of course textbooks, supplies, materials and/or fees, you are welcome to approach me directly. If would prefer not to approach me directly, please note that you can ask the Diversity & First-Gen Office for assistance by completing their questionnaire on course textbooks & supplies: http://tinyurl.com/jpqbarn or by contacting Joseph Brown, the Associate Director of the Diversity and First-Gen Office (jlbrown@stanford.edu; Old Union Room 207). Dr. Brown is available to connect you with resources and support while ensuring your privacy.