Course Announcement: Mathematical Cryptography

http://math.colorado.edu/~kstange/teaching.html
Spring 2024, MATH 8174, Topics in Algebra I
Katherine E. Stange, kstange@math.colorado.edu

Course Description

The goal is to cover the mathematical underpinnings of cryptography at a graduate level, with an emphasis on the beautiful underlying mathematics[1], especially algorithmic number theory. My point of view is that cryptography is an excuse to do exciting mathematics.

I plan to cover the current post-quantum cryptography candidates that are most actively being researched. I plan to encourage you to program algorithms in Sage (math software based on Python), so this is a good course to take for some introductory mathematical programming experience, and some rudimentary introduction to algorithms and runtimes. It's also a good way to see more number theory, arithmetic algebraic geometry, and other algebra topics, whether or not you care for practical application.

Topics (aspirational, and subject to change especially in response to student interest):

1. Discrete log and Diffie-Hellman.
2. RSA and integer factorization, including state-of-the-art factoring algorithms.
3. Elliptic curve cryptography, including pairing-based cryptography and isogeny-based cryptography. Higher-genus considerations. (I will introduce elliptic curves at the level of Silverman, but will take some foundational results for granted after stating them.)
4. Quantum computers and Shor's algorithm. I will assume no knowledge of quantum computation, and will give a brief introduction in the language of Hilbert spaces and tensor products, etc. (Want to program a quantum computer? It's all just linear algebra!)
5. Lattice-based cryptography, including learning-with-errors and NTRU. LLL algorithm, Coppersmith.
6. Ideal lattices, ring-learning-with-errors.
7. Multivariate cryptography.
8. Coding-based cryptography.
9. Possibly some information theory, complexity, zero-knowledge proofs, etc. etc.

[1] did I say mathematics twice? yes I did

Pre-requisites

The course will be accessible to first-year math PhD students who are willing to work ahead in Dummit and Foote as needed. I will assume knowledge of finite fields, as usually covered in *Algebra 1* here at CU. Also some knowledge of ring theory, Hermite/Smith normal form, quadratic number fields, cyclotomic number fields, perhaps some other stuff.

Note: I will likely assign some programming, but won't teach programming per se; you can pick up Python by self-study.

Graduate students from other departments and undergraduates are encouraged to contact me to enroll, if they have approximately the above pre-requisites. Note: as a mathematics graduate course, this is a proof-based course.

Resources

Some relevant texts I will likely use:

1. *An Introduction to Mathematical Cryptography*, Hoffstein, Pipher, Silverman.
2. *Mathematics of Public Key Cryptography*, Galbraith.
3. *Quantum Computation and Quantum Information*, Nielsen and Chuang.
4. *The Arithmetic of Elliptic Curves*, Silverman.

There are few established texts for the mathematical perspective on the most up-to-date post-quantum cryptography.

Credit

I'll assign homework on a rolling basis (including using Sage). We'll have homework presentation days.

Students wishing to receive credit for the course shall attend lecture regularly, and show evidence of having done some homework competently, at a minimum. Students wishing to receive an A for the course shall, in addition, present homework solutions regularly.