QUALIFYING EXAM SYLLABUS

DAVID FREEMAN
DFREEMAN@MATH.BERKELEY.EDU

Committee: Bjorn Poonen (Chair); Kenneth Ribet; Edward Schaefer (Santa Clara University); Luca Trevisan (Computer Science)
Date: Thursday, 12 May 2005 at 10.00 am.

1. Major Topic: Cryptography (Applied Mathematics)

- Definitions of secrecy: Shannon secrecy, perfect secrecy, statistical secrecy, computational secrecy, implications
- Pseudorandomness
  - Pseudorandom generators, pseudorandom functions and permutations, definition of advantage
  - Constructions: PRP from PRF, PRF from PRG, PRG from one-way permutation
- Symmetric-key encryption
  - One-time pad, ECB mode, CBC mode, Counter mode
  - Security for symmetric-key cryptosystems: Real-or-random, left-or-right, find-then-guess, semantic security, equivalences (IND-CPA)
  - Attacks on ECB and CBC with counter IV
  - Security of CBC and counter modes
- Message integrity
  - Integrity of plaintext, integrity of ciphertext, definition of advantage
  - Hash functions, n-universality
  - Construction of message authentication codes
  - Combining MAC and encryption: good and bad methods
- Asymmetric encryption
  - Trapdoor permutations, definition of advantage, random oracle model
  - Hard-core bits, Goldreich-Levin theorem
  - Chosen-plaintext and chosen-ciphertext security
  - Construction of encryption schemes using trapdoor and hash functions: good and bad methods
  - Public-key primitives: RSA, Rabin trapdoor function, Diffie-Hellman key exchange, ElGamal cryptosystem
- Digital Signatures
  - Security against existential forgery
  - Good and bad protocols: Plain trapdoor function, hash-and-sign, full domain hash, probabilistic full domain hash
- Zero-Knowledge Proofs
  - Bit commitment: definition, construction from trapdoor function, construction from pseudorandom generator
  - Interactive proof system; completeness, soundness
  - Definition of zero-knowledge proof: perfect, statistical, computational
  - Graph 3-colorability proof: algorithm, proof of zero-knowledge

References: M. Bellare and P. Rogeway, *Introduction to Modern Cryptography* (online notes available at `http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html`); O. Goldreich, *Foundations of Cryptography,* v. 1-2.

2. Major Topic: Elliptic Curves (Algebra)

- Fundamentals
  - Weierstrass equations, change of coordinates
  - Discriminant, j-invariant
  - Group law: geometric definition, isomorphism with $\mathrm{Pic}^0(E)$
- Maps
  - Isogenies, dual isogeny, structure of m-torsion group
  - Tate module, Weil pairing
  - Structure of endomorphism ring and automorphism group
- One-dimensional formal groups
- Elliptic curves over finite fields
  - Hasse's theorem
  - Weil conjectures and proof for elliptic curves
  - Schoof's point-counting algorithm
- Elliptic curves over local fields
  - Minimal Weierstrass equation, reduction, good and bad reduction
  - Points of finite order: injectivity of reduction map, bound on height
  - Criterion of Néron-Ogg-Shafarevich
- Elliptic curves over global fields
  - Weak Mordell-Weil theorem
  - Descent procedure and heights
  - Proof of Mordell-Weil theorem over $\mathbb{Q}$
  - Torsion points

Reference: J. Silverman, *The Arithmetic of Elliptic Curves*, Chapters III-V, VII-VIII.

3. Minor Topic: Algebraic Number Theory (Algebra)

- Algebraic integers, ideals, Dedekind domains
  - Unique factorization into primes
  - Finiteness of class group
  - Dirichlet unit theorem
  - Behavior of primes in extensions: splitting, inertia, ramification
  - Hilbert's ramification theory: decomposition and inertia groups
  - Quadratic reciprocity
  - Cyclotomic fields
- Valuations and local fields
  - p-adic numbers and absolute value
  - Classification of valuations on $\mathbb{Q}$
  - Ostrowski's theorem on complete fields with archimedian valuation
  - Hensel's lemma
  - Classification of local fields
  - Structure of multiplicative group of a local field
  - Newton polygons and Henselian fields

Reference: J. Neukirch, *Algebraic Number Theory* Chapters I-II.