



Pure Mathematics 529 Advanced Cryptography and Cryptanalysis

(see Course Descriptions under the year applicable: http://www.ucalgary.ca/pubs/calendar/)

Syllabus

Table with 2 columns: Topics and Number of Hours. Rows include Residuacity Based Cryptography (6), Factoring and Discrete Log Algorithms (9), Hyperelliptic Curve Cryptography (9), Pairing Based Cryptography (5), and Student Presentations (6). Total: 35.

Additional Topics (if time permits):

Provable Security: Formal notions of security against active and passive attacks, formal proofs of security.

Secret Sharing: Definition of a secret sharing scheme. Perfect secret sharing schemes. Shamir's scheme. Niederreiter's scheme. Access structures.

Code-Based Cryptography: Basic coding theory. McEliece cryptosystem. Goppa codes.

Lattice-Based Cryptography: Overview of lattices, shortest vector and closest vector problems. Reduction (LLL-algorithm). Ajtai-Dwork construction. NTRU. Possibly other lattice based schemes.

Multi-variate Cryptography: Hidden Field Equations. Matsumoto-Imai scheme. Possibly other MV based system. Groebner bases. Attacks on multi-variate polynomial based schemes.
