UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

Pure Mathematics 649 Advanced Cryptography and Cryptoanalysis

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

Syllabus

Topics	**Number of Hours**
Residuacity Based Cryptography: Miller-Rabin signature scheme, Rabin-Williams cryptosystem. The quadratic residuacity problem, Blum-Blum-Shub pseudorandom number generator, Goldwasser-Micali cryptosystem.	6
Factoring and Discrete Log Algorithms: Number Field Sieve, Function Field Sieve, Adleman-DesMarrais algorithm and their respective complexities.	9
Hyperelliptic Curve Cryptography: Introduction to hyperelliptic curves. Divisors and the Mumford representation. Divisor addition, reduction and Cantor's algorithm. Hyperelliptic curve based cryptographic protocols. The Hyperelliptic Curve Discrete Logarithm Problem. If time permits: the real model of a hyperelliptic curve; principal infrastructure, infrastructure discrete logarithm problem.	9
Pairing Based Cryptography: Divisors revisited. The Weil and Tate pairings. Miller's algorithm. MOV and Frey-Ruck attacks. ID based cryptography using pairings. Tripartite key exchange via pairings.	5
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.

* * * * * * * * * *

2010:08:12 Effective: Fall 2010
RS:jml
Name change/description change/combined with PMAT 529: 2011:07:01
WEC