UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

PURE MATHEMATICS 529
"ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS"

Calendar Description: H(3-0)

Probability and perfect secrecy. Provably secure cryptosystems. Prime generation and primality testing. Cryptanalysis of factoring based cryptosystems. Discrete log based and elliptic curve cryptography and cryptanalysis. Other advanced topics may include hyperelliptic curve cryptography, other factoring methods and other primality tests.

Prerequisite: Pure Mathematics 429.

Syllabus

Topics	**Number of Hours**
Probability and Perfect Secrecy: Overview of probability distributions, conditional probability, and Bayes' Theorem. The Birthday Paradox. Perfect Secrecy/unconditional security, Shannon's Theorem on unconditionally secure cryptosystems and its proof.	4
Provably secure cryptosystems: Notion of computational security. Brief review of RSA, its security and its complexity. Equivalence between factoring the modulus n, computing phi(n), and finding the secret key d. Review of Rabin's signature scheme. Review of the Legendre/Jacobi symbol, law of reciprocity and complementaries, algorithm for computing Jacobi symbols. The Rabin-Williams cryptosystem and its proof of security. Chosen plaintext attack on provably secure systems.	5
Prime Generation and Primality Testing: Review of Fermat's Little Theorem, Fermat test, pseudoprimes, Fermat liars and witnesses, Carmichael numbers and their properties. Review of Euler's Theorem, Euler Criterion, Solovay-Strassen test, Euler pseudoprimes, Euler liars and witnesses, relationship to primes and pseudoprimes. Strong pseudoprimes, relationship to Euler pseudoprimes, Miller-Rabin-Selfridge test. For all those probability tests, we analyze the probability of success. Mention Riemann hypothesis, extended Rieman Hypothesis (ERH), Bach's theorem and how it makes primality testing deterministic polynomial time under ERH. Generation of random primes for cryptographic purposes, the Prime Number Theorem (without proof).	6
Cryptanalysis of Factoring-Based Cryptosystems: Trial division. Power testing. Smooth numbers and review of Pollard p-1 factoring method. Pollard rho factoring method and its expected run time. Factoring via difference of squares. Fermat's algorithm. The Quadratic Sieve, overview of the run time of the QS. Brief mention of the Number Field Sieve and its complexity in comparison to the QS.	8
Discrete Log Based Cryptography and Cryptanalysis: Brief review of Diffie-Hellman key exchange, ElGamal cryptosystem, and the discrete logarithm problem in finite field. Relationship between the El-Gamal problem, the Diffie-Hellman problem, the DLP, and the problem of breaking the ElGamal/DH systems. Review of baby step giant step DL algorithm. Pollard rho method and overview of expected run time. Pohlig-Hellman algorithm and run time. Index calculus method and overview of run time analysis.	8
Elliptic Curve Cryptography and Cryptanalysis: Elliptic curves over finite fields, addition of points and the group of points, Hasse bound on the number of points (without proof). Diffie-Hellman key exchange using elliptic curves, ElGamal cryptosystem using EC, digital signatures using EC. Why the index calculus algorithm doesn't seem to work for ECs.	5
Additional Topics (as time permits): Hyperelliptic Curve Cryptography, Other Factoring Methods; Other Primality Tests.	
TOTAL:	**36**

* * * * * * * * * * *

2004:07:23
JL:jml
Prerequisite change Fall 2009