Pure Mathematics 429 Cryptography – Design and Analysis of Cryptosystems

Review of basic algorithms and complexity. Designing and attacking public key cryptosystems based on number theory. Basic techniques for primality testing, factoring and extracting discrete logarithms. Elliptic curve cryptography. Additional topics may include knapsack systems, zero knowledge, attacks on hash functions, identity based cryptography, and quantum cryptography.
Course Hours: H(3-0)
Prerequisite(s): Pure Mathematics 329 or 418.

Syllabus

Topics	**Number of hours**
Review of Basic Algorithms and Complexity: The Big O notation and its properties. Computational complexity. Applications to the Euclidean algorithm. Extended Euclidean algorithm. Half-Extended Euclidean Algorithm, modular inverses. Lamé's Theorem, computational complexity of the GCD, and the Least Absolute Remainder Algorithm. Exponentiation and its complexity. Polynomial arithmetic, Finite Field arithmetic and complexity. Constructing Finite Fields.	6
Discrete Logarithm Based Cryptography: Brief review of discrete logarithm based public key cryptography and signature schemes. Diffie-Hellman key exchange protocol. The Discrete Logarithm Problem in finite fields, its relevance to DLP based cryptosystems/protocols (EIGamal public key system, EIGamal Signature Scheme, Digital Signature Algorithm). Generalized Diffie-Hellman key exchange in finite groups. Baby step giant step algorithm for computing discrete logs and its complexity. Pollard-rho and Pollard Kangaroo methods. Pohlig-Hellman algorithm.	9
Factoring Based Cryptography: Brief review of factoring based public key dryptography and signature schemes. Review of RSA. Fast Decryption for RSA and its complexity/cost savings. Variants of RSA. The Integer Factoring Problem and its relevance to RSA. Smooth numbers, Pollard's p-1 Algorithm, the p+1 algorithm, Dixon's Factorization Method and the Quadratic Sieve. Complexity of these algorithms.	6
Primality Testing and Prime Generation: True primality tests, proofs via converse of Fermat's Little Theorem and their complexity. Probabilistic primality test, pseudo-primes, strong pseudo-primes. Quadratic reciprocity, Jacobi and Legendre symbols. Solovay Strassen Test, Miller-Rabin-Selfridge Test. Prime number Theorem and method for generating primes (and complexity).	6
Elliptic curves and cryptography: Introduction to Elliptic Curves over $\mathbb{Q}$ and over Finite Fields. Elliptic Curve Cryptography. Complexity of the Elliptic Curve Discrete Logarithm Problem, security considerations. Comparison of public-key cryptosystems via NIST recommendations.	6
TOTAL HOURS	**33**

Additional Topics (if time permits):

Knapsack: The subset sum problem, the knapsack problem, superincreasing sequences. Merkle-Hellman knapsack cryptosystem, Chor-Rivest knapsack cryptosystem. Discussion of the complexity of knapsack systems and explanation of how they were broken.

Zero-knowledge: Bit commitment revisited. Interactive minimum disclosure proof systems. Zero-knowledge proofs of knowledge, computational and perfect zero-knowledge. Feige-Fiat-Shamir identification protocol, cut and choose protocol-cave analogy, zero-knowledge proofs via Hamiltonian cycles, basic zero-knowledge noninteractive protocol, and zero-knowledge proof of discrete logarithm.

Quantum Cryptography: Heisenberg's uncertainty principle, quantum key generation, and a brief discussion of the future implications.

One-Way Functions and Hash Functions: Review of one-way functions. Coin Flipping by telephone using one-way functions (such as exponentiation). Bit commitment using symmetric-key cryptography. Hash functions and their applications. One-way hash functions and compression, iterated hash functions, unkeyed hash functions, hash functions based on modular arithmetic. Speedy stream cipher MAC. Attacks on hash functions.

* * * * * * *

2010:08:12 Effective Fall 2010
RS:jml