

PURE MATHEMATICS 429 "CRYPTOGRAPHY -- The Design of Ciphers"

Calendar Description: H(3-0)

Review of basic algorithms and complexity. Symmetric key cryptography. Discrete log based cryptography. One-way functions and Hash functions. Knapsack. Introduction to primality testing. Factoring. Other topics may include elliptic curves, zero-knowledge, and quantum cryptography.

Prerequisite: Pure Mathematics 315 and 329.

Syllabus

<u>Topics</u>	<u>Number of hours</u>
Review of Basic Algorithms and Complexity: The Big O notation and its properties, Computational complexity, applications to the Euclidean algorithm, Extended Euclidean algorithm, Lamé's Theorem, Computational Complexity of the GCD, and the Least Absolute Remainder Algorithm. Exponentiation and its complexity.	5
Symmetric Key Cryptography: Review of symmetric key cryptography. Overview of Rijndael, the Advanced Encryption Standard. Pohlig-Hellman Symmetric Key Exponentiation Cipher, Massey-Omura cryptosystem (lead into Discrete Log). Complexity analysis of both these systems.	4
Discrete Log Based Cryptography: Brief review of public key cryptography and signature schemes. Review of the Diffie-Hellman key exchange protocol. The Discrete Logarithm Problem in finite fields, its relevance to Diffie-Hellman, Pohlig-Hellman, Massey-Omura. Other DLP based cryptosystems/protocols (ElGamal public key system, ElGamal Signature Scheme). Generalized Diffie-Hellman key exchange in finite groups. Baby step giant step algorithm for computing discrete logs and its complexity.	6
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. Review of trap-door one-way functions, their use in public key cryptography, examples (RSA public-key cryptosystem, Elgamal cryptosystem). Hash functions and their applications: data integrity, symmetric data origin	7

authentication. One-way has functions and compression, iterated has functions, unkeyed hash functions, hash functions based on modular arithmetic. Speedy stream cipher MAC.

Knapsack: The subset sum problem, the knapsack problem, Superincreasing sequences, the Merkle-Hellman knapsack cryptosystem, the Chor-Rivest knapsack cryptosystem. A brief discussion of the complexity of knapsack systems and explanation of how they were broken. 2

Introduction to Primality Testing: True primality tests, including Pocklington's theorem, Proth's theorem, Pepin's primality test, Proofs via the converse of Fermat's little Theorem, Complexity of these tests. 3

Factoring: Smooth numbers, Pollard's p-1 factoring algorithm 2

Advanced topics:

Elliptic curves and cryptography: The Elgamal public-key elliptic curve cryptosystem, and the Menezes-Vanstone elliptic curve cryptosystem. Diffie-Hellman key exchange using elliptic curves. 4

Zero-knowledge: Bit commitment revisited. Interactive minimum disclosure proof systems, zero-knowledge proofs of knowledge, computational and perfect zero-knowledge, the Feige-Fiat-Shamir identification protocol, the cut and choose protocol-cave analogy, zero-knowledge proofs via Hamiltonian cycles, basic zero-knowledge noninteractive protocol, and zero-knowledge proof of discrete log 4

Quantum Cryptography: Heisenberg's uncertainty principle, quantum key generation, and a brief discussion of the future implications 1

TOTAL HOURS 36

* * * * *

2003:12:23 Effective Winter 2004
JL:jml
Prereq change, coreq deletion Fall 2009