Math 445
Final exam review topics
May 5, 2004

The exam will cover the whole course. Review topics include those distributed for the midterm and the following:

Information Theory

- Basic probability theory
- Entropy and conditional entropy
- Shannon's definition of perfect secrecy
- Huffman encoding

More Number Theory

- Modular exponentiation
- Theorems of Fermat and Euler
- Primitive roots
- Square roots modulo n

Public Key Algorithms

- RSA
- El Gamal
- Diffie-Hellman
- Implementation issues
- Applications: treaty verification, bit commitment, key distribution, signatures

Primality and Factoring

- Primality test: Fermat, Miller-Rabin
- Factoring algorithms: Fermat, universal exponent, given exponent, Pollard p-1, quadratic sieve

Discrete Logarithms

- Pohlig-Hellman algorithm
- Index calculus
- Birthday attacks

Digital Signatures

- RSA, El Gamal, and DSA schemes
- Hash functions
- Birthday attacks

Key Distribution

- Public Key Infrastructures
- PGP
- Station-to-station protocol
- Blum key distribution scheme
- Kerberos

Quantum Computing

- Quantum key distribution
- Qubits
- Quantum parallelism
- Quantum Fourier transformation
- Shor's algorithm