Math 445
Midterm review topics
March 1, 2004

Basic Cryptography

Basic framework for a cryptosystem
Ciphers and codes
Block and stream ciphers
Modes for a block cipher: ECB, CBC, CFB
Kerckhoff's principle
Types of attacks
Importance of the key size
Applications beyond confidentiality

Classic Cryptosystems

Shift cipher
Affine cipher
Substitution cipher
Vignère cipher
Playfair cipher
Hill cipher
One-time pad

Basic Number Theory

Divisibility, primes
GCD, extended Euclidean algorithm
Congruences and modular arithmetic
Solving linear congruences
Chinese remainder theorem
Polynomials modulo p and finite fields

DES

Feistel systems
Specification of DES
Basic idea of differential crytpanalysis
Current status of DES

AES

Computations in the field of 128 elements
Overview of the AES algorithm
Specification of the layers
Decryption vs. encryption