

Math 445
Final exam review topics

- Basic Cryptography
 - Basic framework for a cryptosystem
 - Kerckhoff's principle
 - Types of attacks
 - Importance of the key size
 - Applications beyond confidentiality
- Classic Cryptosystems
 - Shift cipher
 - Affine cipher
 - Substitution cipher
 - Vigenère cipher
 - Playfair cipher
 - ADFGX cipher
 - Hill cipher
 - One-time pad
 - Linear feedback shift register sequences
- Basic Number theory
 - Divisibility, primes
 - GCD, Extended Euclidean Algorithm
 - Congruences and modular arithmetic
 - Chinese Remainder Theorem
 - Solving linear congruences
 - Matrices modulo n
 - Finding square roots modulo n
 - Concept of a group, notion of the order of an element
 - Fermat's little theorem, Euler's theorem, Lagrange's theorem
 - Polynomials modulo p , construction of finite fields
 - generating LFSRs with long period, characteristic polynomial
- Public Key Cryptosystems
 - RSA cryptosystem
 - Attacks on the RSA cryptosystem
 - Primality Testing algorithms
 - Methods for factoring integers
 - The public key concept
- Discrete Logarithms
 - Definition of discrete logarithms
 - The Methods for computing discrete logarithms
 - The ElGamal Public key cryptosystem
- Digital Signatures and Hash functions
 - The RSA and the ElGamal Signature schemes
 - Definition of a cryptographic hash function
 - Examples of cryptographic hash functions
 - Applications of hash functions
 - The Birthday attack on hash functions and discrete logarithms
 - The Digital Signature Algorithm
- Elliptic Curves (turn page)

2

- Definition of an elliptic curve and the addition law
 - Hasse's Theorem
 - Elliptic Curve Cryptosystems
- AES
 - Definition of AES