MATH/CMSC 456, Jeffrey Adams

Review for Final, May 18, 2009 (8-10 AM, Math B0429)

1. Chapter 2
   (a) Shift and affine ciphers
   (b) Vigenère cipher
   (c) Block ciphers, Hill cipher
   (d) One-time pads
   (e) Linear feedback shift registers
2. Chapter 3
   (a) Prime numbers
   (b) Euclidean algorithm, greatest common divisor, extended Euclidean algorithm
   (c) Chinese Remainder Theory
   (d) Congruences
   (e) Inverses $\pmod{n}$, solving $ax = b \pmod{n}$
   (f) Fermat's and Euler's theorems
3. Chapter 4 The main thing to understand is the idea of Feistel systems. Also DES is not a group, triple DES, meet-in-the-middle attacks.
4. Chapter 6
   (a) Public Key Cryptography
   (b) Definition of RSA
   (c) Primality testing and factoring:
      i. the Basic Principle (page 176)
      ii. Fermat test
      iii. p-1 factoring algorithm
      iv. Miller Rabin and Universal Exponent method
      v. Quadratic Sieve
5. Chapter 7
   (a) Basics of discrete logarithms
   (b) Pohlig-Hellman
   (c) Baby Step, Giant Step
   (d) Diffie Hellman key exchange
   (e) ElGamal cryptosystem

6. Chapter 8 (Hash Functions)
   (a) Basics of hash functions
   (b) Birthday attacks
   (c) Birthday attack on discrete logarithms
7. Chapter 9 (Digital Signatures)
   (a) Basic idea of digital signatures
   (b) RSA signatures
   (c) ElGamal signatures (you don't need to remember the formula)
   (d) Hashing and signatures
   (e) Birthday attacks on digital signatures
8. Chapter 12 (Secret Sharing)
   (a) Basic concept of secret sharing
   (b) (t, w)-threshhold schemes
   (c) Shamir threshold scheme
9. Chapter 14 (Zero Knowledge)
   (a) Basic concept of zero-knowledge
   (b) Square-root zero knowledge algorithm
10. Chapter 16 (Elliptic Curves)
   (a) Basic concepts of elliptic curves
   (b) Addition law on an elliptic curve
   (c) Hasse's theorem
   (d) Discrete logarithms on elliptic curves
   (e) Representing plaintext
   (f) Factoring with elliptic curves
   (g) ElGamal on elliptic curves
   (h) Diffie-Hellman on elliptic curves