Math/Cmsc 456, Jeffrey Adams

Review for Test 2, May 8, 2009

1. Chapter 7 (Discrete Logarithm)
   (a) Basics of discrete logarithms
   (b) Pohlig-Hellman
   (c) Baby Step, Giant Step
   (d) Diffie Hellman key exchange
   (e) ElGamal cryptosystem
2. Chapter 8 (Hash Functions)
   (a) Basics of hash functions
   (b) Birthday attacks
   (c) Birthday attack on discrete logarithms
3. 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
4. Chapter 12 (Secret Sharing)
   (a) Basic concept of secret sharing
   (b) (t, w)-threshhold schemes
   (c) Shamir threshold scheme
5. Chapter 14 (Zero Knowledge)
   (a) Basic concept of zero-knowledge
   (b) Square-root zero knowledge algorithm
6. 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