Outline for November 13, 2006

Reading: §9.2–9.3

1. Greetings and felicitations!
   a. Quick discussion of midterm
2. Product ciphers: DES
3. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption computationally feasible [note: commutativity not required]
   c. Benefits: can give confidentiality or authentication or both