Outline for October 5, 2022

Reading: *text*, §10.2.4–10.5 **Assignments:** Homework 1, due October 5; Project selection, due Oct 7

1. Product ciphers
   (a) DES
   (b) AES
2. 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
3. Use of public key cryptosystem
   (a) Normally used as key interchange system to exchange secret keys (cheap)
   (b) Then use secret key system (too expensive to use public key cryptosystem for this)
4. RSA
   (a) Provides both authenticity and confidentiality
   (b) Based on difficulty of computing totient, $\phi(n)$, when n is difficult to factor