Outline for October 11, 2024

Reading: *text*, §10.3–10.6 **Due:** Homework 2, due October 23; Project progress report, due November 1

1. 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
2. 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)
3. RSA
   (a) Provides both authenticity and confidentiality
   (b) Based on difficulty of computing totient, $\phi(n)$, when n is difficult to factor
4. Cryptographic Checksums
   (a) Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   (b) Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$
   (c) Keyed vs. keyless
5. Digital Signatures
   (a) Judge can confirm, to the limits of technology, that claimed signer did sign message
   (b) RSA digital signatures: sign, then encipher, then sign
   (c) El Gamal digital signatures