Outline for February 22, 2006

Reading: text, §9.3–9.4

1. Greetings and felicitations!
   a. Puzzle of the day
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 PKC for this)
4. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:

      Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \#(n) = 1$

      Proof: $M^{\#(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \#(n) = 1$

      Public key is (e, n); private key is d. Choose $n = pq$; then $\#(n) = (p-1)(q-1)$.
   c. Example: $p = 5$, $q = 7$; then $n = 35$, $\#(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \#(n) = 1$, so $e = 11$.

      To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.
   d. Example: $p = 53$, $q = 61$; then $n = 3233$, $\#(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$.
      To encipher M = RENAISSANCE, use the mapping A = 00, B = 01, ..., Z = 25, b = 26. Then: M = RE NA IS SA NC Eb = 1704 1300 0818 1800 1302 0426, so $C = (1704)^{71} \bmod 3233 = 3106$; etc. = 3106 0100 0931 2691 1984 2927
5. 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