Outline for November 15, 2006

Reading: §9.3

1. Greetings and felicitations!
   a. Puzzle of the day
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. Go through algorithm:
   Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \Phi(n) = 1$
   Proof: $M^{\Phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \Phi(n) = 1$
   Public key is (e, n); private key is d. Choose $n = pq$; then $\Phi(n) = (p-1)(q-1)$.
   c. Example: $p = 5$, $q = 7$; then $n = 35$, $\Phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \Phi(n) = 1$, 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 $n = 3233$, $\Phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$
   To encipher M = RENAISSANCE, use the mapping A = 00, B = 01, ..., Z = 25, b̸ = 26.
   Then: M = RE NA IS SA NC Eb̸ = 1704 1300 0818 1800 1302 0426
   So: $C = (1704)^{71} \bmod 3233 = 3106$; etc. = 3106 0100 0931 2691 1984 2927