Outline for February 15/20, 2002

Reading: §9–9.3

1. Greetings and Felicitations!
2. Puzzle of the day
3. Classical
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. polyalphabetic: Vigenère, $f_i(a) = (a + k_i) \bmod n$
   d. cryptanalysis: first do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. problem: eliminate periodicity of key
4. Long key generation
   a. Running-key cipher: M=THETREASUREISBURIED; K=THESECONDCIPHERISAN; C=MOIL-VGOFXTMXZFLZAEQ; wedge is that (plaintext,key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)
   b. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   c. Only cipher with perfect secrecy: one-time pads; C=AZPR; is that DOIT or DONT?
5. DES
6. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. given public key, CI 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
7. 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:
      $p = 5$, $q = 7$; $n = 35$, $\phi(n) = (5–1)(7–1) = 24$. Pick $d = 11$. Then $de \bmod \phi(n) = 1$, so choose $e = 11$. 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: $p = 53$, $q = 61$, $n = 3233$, $\phi(n) = (53–1)(61–1) = 3120$. Take $d = 791$; then $e = 71$. Encipher M = RENAISSANCE: A = 00, B = 01, …, Z = 25, blank = 26. Then:
      M = RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426
      $C = (1704)^{71} \bmod 3233 = 3106$; *etc.* = 3106 0100 0931 2691 1984 2927