Notes for October 25, 1999

1. Greetings and Felicitations!
   a. Bibliography: I'll have copies made for Monday or Wednesday of next week
   b. Program hints: see newsgroup. Should I extend homework due date to Wednesday?
2. Puzzle of the Day
3. Specification Detection
   a. Look for violations of specifications
   b. Basis: need a representation of specifications
   c. Issues: similar to misuse detection
   d. Advantage: can detect attacks you don't know about.
4. Cryptography
   a. Ciphers v. Codes
   b. Attacks: ciphertext-only, known plaintext, known ciphertext
5. 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
6. 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. Enigma/rotor systems; wheels, 3 rotors and a reflecting one. Go through it; UNIX uses this for *crypt*(1) command.
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   d. Only cipher with perfect secrecy: one-time pads; C=AZPR; is that DOIT or DONT?
7. DES
   a. Go through the algorithm
8. 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 authentiction or both
9. Use of PKC
   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)