Notes for October 22, 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. Example of Flaw Hypothesis Methodology
   c. Go through Burroughs B6700 penetration
4. Intrusion Detection Systems
   a. Anomaly detectors: look for unusual patterns
   b. Misuse detectors: look for sequences known to cause problems
   c. Specification detectors: look for actions outside specifications
5. Anomaly Detection
   a. Original type: used login times
   b. Can be used to detect viruses, etc. by profiling expected number of writes
   c. Basis: statistically build a profile of users' expected actions, and look for actions which do not fit into the profile
   d. Issue: periodically modify the profile, or leave it static?
   e. User vs. group profiles
   f. Problems
6. Misuse Detection
   a. Look for specific patterns that indicate a security violation
   b. Basis: need a database or ruleset of attack signatures
   c. Issues: handling log data, correllating logs
   d. Problems: can't find new attacks
7. 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.
8. Cryptography
   a. Ciphers v. Codes
   b. Attacks: ciphertext-only, known plaintext, known ciphertext
9. 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