Notes for October 28, 1998

1. Greetings and Felicitations!
   a. Office hours 3:00–4:00PM today.
   b. Security lab seminar 1:00–2:00PM in 1131 EU-II. We will talk about ongoing projects!
2. Puzzle of the Day
3. 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
4. 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
5. 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.
6. Cryptography
   a. Ciphers v. Codes
   b. Attacks: ciphertext-only, known plaintext, known ciphertext
7. Classical Ciphers
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE $\rightarrow$ UHQDLVVDQFH
   c. polyalphabetic: Vigenère, $f_i(a) = (a + k_i) \bmod n$
   d. cryptanalysis:do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. problem: eliminate periodicity of key