Notes for January 22, 1997

1. Hello
   a. Project comments will be out by Friday
   b. Want to post a 1-line description of projects being done; please use handin to hand it in (or I will summarize what you sent, and may get it wrong!)
2. Puzzle of the day
   a. Key point: real problem, no really good answer; a good project would be to analyze the options thoroughly, esp. with regard to ethics and practicality.
3. Authentication
   a. validating client (user) identity
   b. validating server (system) identity
   c. both (“mutual authentication”)
4. Basis
   a. What you know
   b. What you have
   c. What you are
   d. (proposed) Where you are
5. Passwords
   a. How UNIX does selection
   b. Problem: common passwords
   c. May be pass phrases, etc.; goal is to make search space as large as possible AND password distribution as uniform as possible
   d. Go through Morris and Thompson study; augment with Klein, mine, *etc*.
   e. Other ways to force good password selection: random, pronounceable, computer-aided selection
   f. Go through problems, approaches to each, *esp*. proactive
6. Password Storage
   a. In the clear (MULTICS story)
   b. Enciphered (key must be on line somewhere; get it and it’s all over)
   c. Hashed; present idea of one-way functions using identity and sum
   d. Show UNIX version
7. Attack Schemes Directed to the Passwords
   a. Exhaustive search: UNIX is 1-8 chars, say 96 possibles; it’s about 7e16
   b. Inspired guessing: think of what people would like (see above)