Notes for January 24, 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. Password Storage
   a. Hashed; present idea of one-way functions using identity and sum
   b. Show UNIX version
4. 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)
   c. Random guessing: can't defend against it; bad login messages aid it
   d. Scavenging: passwords often typed where they might be recorded (b\as login name, in other contexts, *etc*.
   e. Ask the user: very common with some public access services
   f. Expected time to guess
5. Password aging
   a. Pick age so when password is guessed, it's no longer valid
   b. Implementation: track previous passwords vs. upper, lower time bounds
6. Ultimate in aging: One-Time Pads
   a. Password is valid for only one use
   b. May work from list, or new password may be generated from old by a function