Notes for January 10, 1997

1. Hello
   a. Remember, no section meeting this week
2. Puzzle of the day
   a. Key point: people problem; no amount of code fixing will solve this.
3. Can we determine if something is secure or not?
   a. Need to represent system in some way
   b. Need to represent changes to protections in some way
4. Background
   a. Protection State: (S, O, A)
   b. A Access Control Matrix (Graham/Denning); give examples
   c. Primitives: **enter** r **into** $A[s, o]$; **delete** r **from** $A[s, o]$; **create subject** s, **create object** o, **destroy subject** s, **destroy object** o
   d. Commands: **if** (r_1 **in** $A[x_{s1}, x_{o1}]$) **and** … **and** (r_n **in** $A[x_{sn}, x_{on}]$) **then** $prim_1$; … $prim_m$
   e. Unauthorized state Q: one in which a generic right could be leaked; in other words, a command c would execute a primitive operation entering r into some cell of A not previously containing r (if not possible, initial state Q_0 is safe or secure)
5. Basic results:
   a. There is an algorithm that decides whether a given mono-operational system and initial state is safe for a given generic right r. It is however **NP**-complete.
   b. It is undecidable whether a given state of a given protection system is safe (secure) for a given generic right. Reduce the halting problem to it.
   c. Implications: key word is “generic”; can’t get general algorithm, but if you focus on a specific system, you often can.
6. Cryptography
   a. Basic components of ciphers: substitution, transposition
   b. Classical v. public-key; note classical gives you either confidentiality (Alice & Bob keep plaintext secret) or authentication (Alice publishes both plaintext and ciphertext and Bob validates it using his key) but not both.
   c. Attacks: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext
   d. Best ciphers withstand all of these
7. Classical
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE -> UHQDLVVDQFH
   c.