Outline for March 10, 2006

Reading: text, §15.1–15.3

1. Greetings and felicitations!
   a. Puzzle of the day
2. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
3. Capabilities
   a. Capability-based addressing: show picture of accessing object
   b. Show process limiting access by not inheriting all parent's capabilities
   c. Revocation: use of a global descriptor table
4. Privilege in Languages
   a. Nesting program units
   b. Temporary upgrading of privileges
5. Lock and Key
   a. Associate with each object a lock; associate with each process that has access to object a key (it's a cross between ACLs and C-Lists)
   b. Example: use crypto (Gifford). *X* object enciphered with key *K*. Associate an opener *R* with *X*. Then:
      OR-Access: *K* can be recovered with any D_i in a list of *n* deciphering transformations, so $R = (E_1(K), E_2(K), ..., E_n(K))$ and any process with access to any of the D_i's can access the file
      AND-Access: need all *n* deciphering functions to get *K*: $R = E_1(E_2(...E_n(K...))$
   c. Types and locks