# Outline for October 15, 2003

**Reading**: Chapters 6.4, 9.1–9.2

## Discussion Problem

Bureaucracies have their own version of the English language with which you must become familiar. To help you do so, here are some common phrases. See if you can translate them.

1. Scintillate, scintillate, asteroid minikin.
2. Members of an avian species of identical plumage congregate.
3. Surveillance should precede saltation.
4. Pulchritude possesses solely cutaneous profundity.
5. It is fruitless to become lachrymose over precipitately departed lacteal fluid.
6. Freedom from incrustations of grime is contiguous to rectitude.
7. The writing implement is more potent than the rapier.
8. It is fruitless to attempt to indoctrinate a superannuated canine with innovative maneuvers.
9. Eschew the implement of correction and vitiate the scion.
10. The temperature of the aqueous content of an unremittingly galled saucepan does not reach 212 degrees Farenheit.
11. Upon vacating these premises all illuminations are to be extinguished.

## Outline for the Day

1. Clark-Wilson (*con't*)
   a. Certification and enforcement rules:
      C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run
      C2. All TPs must be certified as valid; each TP is assocated with a set of CDIs it is authorized to manipulate
      E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs
      E2: The system must maintain a list of User IDs, TP, and CDIs that that TP can manipulate on behalf of that user, and must ensure only those executions are performed.
      C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
      E3. The sysem must authenticate the identity of each user attempting to execute a TP.
      C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to resonstruct the operation.
      C5. Any TP taking a UDI as an input must be certified to perform only valid transformations, else no transformations, for any possible value of the UDI. The transformation should take the input from a UDI to a CDI, or the UDI is rejected (typically, for edits as the keyboard is a UDI).
      E4. Only the agent permitted to certify entities may change the list of such entities associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity
2. Cryptography
   a. Codes vs. ciphers
   b. Attacks: ciphertext only, known plaintext, chosen plaintext
   c. Types: substitution, transposition
3. Classical Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. Polyalphabetic: Vigenère, $fi(a) = (a + k_i) \bmod n$
   d. Cryptanalysis: first do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. Problem: eliminate periodicity of key
4. Long key generation

a. Running-key cipher: M=THETREASUREISBURIED; K=THESECONDCIPHERISAN; C=MOILVGOFXTMXZFLZAEQ; wedge is that (plaintext,key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)

b. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext

c. Only cipher with perfect secrecy: one-time pads; C=AZPR; is that DOIT or DONT?

5. DES