Outline for February 17, 2006

Reading: text, §6.4, §9.1–9.3

1. Greetings and felicitations!
   a. Puzzle of the day
2. Clark-Wilson Certification and enforcement rules
   a. C1. All IVPs must ensure that all CDIs are in a valid state when the IVP is run.
   b. C2. All TPs must be certified to be valid, and each TP is assocated with a set of CDIs it is authorized to manipulate.
   c. E1. The system must maintain these lists and must ensure only those TPs manipulate those CDIs.
   d. 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.
   e. C3. The list of relations in E2 must be certified to meet the separation of duty requirement.
   f. E3. The sysem must authenticate the identity of each user attempting to execute a TP.
   g. C4. All TPs must be certified to write to an append-only CDI (the log) all information necessary to resonstruct the operation.
   h. 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).
   i. 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
3. Cryptography
   a. Codes vs. ciphers
   b. Attacks: ciphertext only, known plaintext, chosen plaintext
   c. Types: substitution, transposition
4. Classical Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE Þ UHQDLVVDQFH
   c. Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
   d. Cryptanalysis: first do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. Problem: eliminate periodicity of key
5. 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?
6. DES
7. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. Given public key, computationally infeasible to get private key;
      ii. Cipher withstands chosen plaintext attack;
      iii. Encryption, decryption computationally feasible [note: commutativity not required]
   c. Benefits: can give confidentiality or authentication or both