Outline for February 11, 2002

Reading: §6.4, §9–9.3

1. Greetings and Felicitations!
2. Puzzle of the day
3. Clark-Wilson
   a. Theme: military model does not provide enough controls for commercial fraud, *etc*. because it does not cover the right aspects of integrity
   b. Data items: "Constrained Data Items" (CDI) to which the model applies, "Unconstrained Data Items (UDIs) to which no integrity checks are applied, "Integrity Verification Procedures" (IVP) that verify conformance to the integrity spec when IVP is run, "Transaction Procedures" (TP) takes system from one well-formed state to another
   c. 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 to be valid, and 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
4. Classical
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE → 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=MOIL-VGOFXTMXZFLZAEQ; 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, CI 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

8. RSA

a. Provides both authenticity and confidentiality

b. Go through algorithm:

Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$.

Proof: $M^{\phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \phi(n) = 1$.

Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p–1)(q–1)$.

c. Example:

$p = 5$, $q = 7$; $n = 35$, $\phi(n) = (5–1)(7–1) = 24$. Pick $d = 11$. Then $de \bmod \phi(n) = 1$, so choose $e = 11$. To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.

d. Example: $p = 53$, $q = 61$, $n = 3233$, $\phi(n) = (53–1)(61–1) = 3120$. Take $d = 791$; then $e = 71$. Encipher M = RENAISSANCE: A = 00, B = 01, …, Z = 25, blank = 26. Then:

M = RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426

$C = (1704)^{71} \bmod 3233 = 3106$; *etc.* = 3106 0100 0931 2691 1984 2927