Notes for October 31, 2000

1. Greetings and Felicitations!
   a. Why is homework program useful? If a program deletes an environment variable, which one?
   b. Current grades, *etc*. now on web page
2. Puzzle of the day
3. 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:
      $p = 5$, $q = 7$; $n = 35$, $f(n) = (5–1)(7–1) = 24$. 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 $M = C^{\mathrm{d}} \bmod n = 1811 \bmod 35 = 2$.
   d. Example: $p = 53$, $q = 61$, $n = 3233$, $f(n) = (53–1)(61–1) = 3120$. 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
4. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$.
   c. Keyed *vs*. keyless
   d. MD5, HMAC
5. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
6. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
   c. Key Escrow
7. Digital Signatures
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
   c. Key Escrow

Puzzle of the Day

The UNIX system reserves network ports numbered 1023 and below for *root*-owned processes only. User processes must use ports with higher numbers. So, if the source port from a remote host has a source port of 536, it must have originated with a process that was at one time *root*. This is a UNIX standard, **not** an Internet one.

What problems can this scheme cause in a heterogeneous network?