Outline for February 20/22, 2002

Reading: §9.3–9.4, §10.2, §10.4.2-10.4.3, §10.5.1-10.5.1.1, §10.5.2, §10.6 except §10.6.2.2

1. Greetings and Felicitations
2. Puzzle of the day
3. 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
4. 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
5. 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
6. Key Exchange
    a. Needham-Schroeder and Kerberos
    b. Public key; man-in-the-middle attacks
7. Cryptographic Key Infrastructure
    a. Certificates (X.509, PGP)
    b. Certificate, key revocation
    c. Key Escrow
8. Digital Signatures