Lecture 19, May 13

Reading: §9.3–9.4 **Assignments due:** Homework #3, due May 13, 2013

Discussion Problem. What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

> Our ancestors, and those who were considered to be wise, were accustomed to say that it was necessary to control Pistoia by means of factions and Pisa by means of fortresses; so they fostered strife in various of their subject towns, so as to control them more easily. In those days, when there was stability of a sort in Italy, this was doubtless sensible; but I do not think it makes a good rule today. I do not believe any good at all ever comes from dissension. On the contrary, on the approach of the enemy, cities which are so divided inevitably succumb at once; the weaker faction will always go over to the invader, and the other will not be able to hold out.[1]

Lecture outline.

1. Project
   a. Penetration test of a computer system using the Flaw Hypothesis Methodology
   b. Need to select groups of 3 or 4; each group gets an account on the system
2. 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: $p = 5$, $q = 7$; then $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $d = 11$. Then $ed \bmod \phi(n) = 1$, so $e = 11$
   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: $p = 53$, $q = 61$; then $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Pick $d = 791$. Then $e = 71$
   To encipher $M =$ `RENAISSANCE`, use the mapping `A = 00`, `B = 01`, ..., `Z = 25`, ␣ = 26.
   Then: $M =$ `RE NA IS SA NC E␣` $= 1704\ 1300\ 0818\ 1800\ 1302\ 0426$
   So: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
3. 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
4. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks

[1] Niccolò Machiavelli, *The Prince*, George Bull trans., Penguin Books, New York, NY (1995), p. 67.