Lecture 18, May 10

Reading: §9.2–9.4 **Assignments due:** Homework #3, due May 13, 2013

Discussion Problem. During a six month period, a number of computer installations were attacked by an intruder who broke in and simply looked at the data on the system. After repeated investigations, it was determined the intruders were from the Netherlands. The Dutch police were asked to investigate, because one of the computers was at a military site, and there was considerable belief that espionage against the United States was being committed.

After a thorough investigation, the Dutch authorities found that the intruder was a high school student who had no previous record of trouble, and they determined he was not spying; he was simply amusing himself. They declined to proceed any further as (then) attacking computer systems was not a crime under Dutch law.

The intruder continued to break into these systems despite efforts to stop him. While he caused no damage, he tied up lots of the system programmers' time.

1. What would you suggest they should try to solve the problem? Bear in mind the attacker is under Dutch, and not American, jurisdiction.
2. Someone finally hit upon the perfect solution. They implemented it and the problem ended. What was it?

Lecture outline.

1. Product ciphers: DES, AES
2. 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
3. Use of public key cryptosystem
   a. Normally used as key interchange system to exchange secret keys (cheap)
   b. Then use secret key system (too expensive to use public key cryptosystem for this)
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: $p = 5$, $q = 7$; 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: $C = (1704)^{71} \bmod 3233 = 3106; \ldots = 3106\ 0100\ 0931\ 2691\ 1984\ 2927$
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