Lecture 26, May 31

Reading: §22 (*not* 22.6), 26.3, [Nac97][1] **Assignments due:** Homework #5, due June 6, 2013 at 11:55pm

Discussion Problem. It has often been said that the only way to decipher a message that has been enciphered using RSA is to factor the modulus n used by the cipher. If you were told that an enciphered message was on a computer that you controlled, and that the message was enciphered using RSA with an n of 1024 bits (about 309 decimal digits), how would you find the encrypter's private key?

Lecture outline.

1. Greetings and Felicitations!
   a. Review session: Friday, June 7, at 11:00am–12:00pm in room 184 Young (this room!)
2. Types of malicious logic (*con't*)
   a. Computer worm
   b. Bacterium, rabbit
   c. Logic bomb
3. Ideal: program to detect malicious logic
   a. Can be shown: not possible to be precise in most general case
   b. Can detect all such programs if willing to accept false positives
   c. Can constrain case enough to locate specific malicious logic
4. Defenses
   a. Type checking (data vs. instructions)
   b. Limiting rights (sandboxing)
   c. Limiting sharing
   d. Preventing or detecting changes to files
   e. Prevent code from acting beyond specification (proof carrying code)
   f. Static signature checking
   g. Behavioral analysis
   h. Check statistical characteristics of programs
5. Network security
   a. Firewalls
   b. Network organization, DMZ
   c. Hiding internal addresses

[1] This is available in the Resources area of SmartSite; look in the folder "Handouts"