Lecture 21 Outline (May 15, 2015)

Reading: §10.1–10.4, 10.6 **Assignment**: Homework 3, due May 20, 2015

1. Greetings and felicitations!
2. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
3. Key Generation
   a. Cryptographically random numbers
   b. Cryptographically pseudorandom numbers
   c. Strong mixing function
4. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
5. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher

During the depths of the Great Depression, Grouch Marx and his brothers went to Central Park in New York City. They tried to sell money, asking everyone they met to purchase a $5 bill for $1. No-one bought; everyone they asked looked at them like they were crazy, or asked what was wrong with the $5 bill. Eventually, a policeman came over and, when they made him the same offer, arrested the brothers on suspicion of counterfeiting.

Why do you think the Marx brothers couldn't find a buyer? What does this inability say to an attacker who is planning how to attack a computer system? What does it say to a system administrator seeking to defend her system?