Lecture 20 Outline (May 13, 2015)

Reading: §9.4, 10.1–10.4, 10.6 **Assignment**: Homework 3, due May 20, 2015

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

The PGP secure mailing system uses both RSA and AES (or a number of other ciphers, but we'll use RSA as the interchange key cipher and AES as the data encryption cipher here). When one installs PGP, the software generates two large (1000 bits or so) numbers, to produce a modulus of 2048 bits. Such a number is too large to be factored easily. The private and public keys are generated from these quantities. The private key is enciphered with a classical cipher using a user-supplied pass phrase as the key. To send a message, a 128-bit key is randomly generated, and the message enciphered using IDEA with that key; the key is enciphered using the recipient's public key, and the message and enciphered key are sent.

1. If you needed to compromise a user's PGP private key, what approaches would you take?
2. It's often said that PGP gets you the security of a key with length 2048. Do you agree?