Lecture 23 Outline (May 20, 2015)

Reading: §11.4.1, 14.6.3, 12 **Assignment**: Homework 3, due May 20, 2015

1. Greetings and felicitations!
2. TOR
   a. Overall ideas
   b. Entry, middle, exit nodes
   c. Directory servers
   d. cells and circuits
3. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conforment MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs
4. Anonymous mailings
   a. Cypherpunk remailer
   b. Mixmaster remailer
5. Authentication
   a. Validating client (user) identity
   b. Validating server (system) identity
   c. Validating both (mutual authentication)
   d. Basis: what you know/have/are, where you are
6. Passwords
   a. Problem: common passwords
   b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   c. Other ways to force good password selection: random, pronounceable, computer-aided selection

---

Today, TechWorm has a story entitled "Two Security Researchers Break RSA 4096 Bit Keys with 'Phuctor'." They did so by finding a common factor of the (different) moduli of two public keys. (See the extra credit of homework 3 for more details of how this can be done.) As these factors p and q are generated randomly, and are on the order of 2096 bits big, why might two of these factors be the same even when they are generated on two, often geographically widely separated, systems?

The URL of this story is:

`http://www.techworm.net/2015/05/two-security-researchers-break-rsa-4096-bit-keys-with-phuctor.html`