Outline for October 29, 2003

**Reading**: Chapters 11.1, 11.3–11.4

**Discussion Problem**
Microsoft spent February, 2002, teaching its programmers how to check their code for security vulnerabilities and how to spot common security flaws. Yet many Microsoft programs have security vulnerabilities. What problems do you think Microsoft encountered, and will encounter, in trying to find and clean up the vulnerabilities in its systems?

**Outline for the Day**
1. Types of attacks
   a. Forward searches
   b. Misordered blocks
   c. Statistical regularities (repetitions)
2. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end encryption
3. Example protocol: PEM
   a. Design goals