CS 434/534 Homework | Week 4
February 12, 2008 | **DUE: Feb 19**

1. Below is a list of network attacks, followed by a list of security techniques. For each security techniques, list the attacks it defends against (use the letters).

   a) IP spoofing
   b) DOS
   c) packet sniffing
   d) person-in-the-middle
   e) SYN flood
   f) Stack smashing

   - Digital signatures
   - Firewall
   - Public key cryptography
   - Certification authority
   - SSL
   - Secure email (secret, authenticated)
   - Java

2. All security systems are based on trust. What do you have to trust to believe an SSL connection is secure?

3. Alice wants to download a file written by Bob from Trudy's ftp server. Alice wants to verify that the file is indeed written by Bob. Trudy wants to verify Alice's identity. Bob and Alice do not want Trudy to be aware of the contents of the file. All involved will use public key cryptography. Describe how this can be accomplished, including who does what with which keys. A combination of pictures and words may be best. (use the back if necessary)