CSC 257/CSC 457
Problem Set 4
December 6th, 2001

This problem set is not a graded assignment. We will go through the solution in class on Tuesday, December 11th. You will benefit from doing it in advance since it will prepare you for the exam.

1. Encryption:

   (a) Suppose we wanted to encrypt a Telnet session with, say, DES. Telnet sends lots of 1-byte messages, while DES encrypts in blocks of 8 bytes at a time. Explain how DES might be used securely in this setting.

   (b) Cipher block chaining is used to increase the complexity of DES so that the same plain-text message will not result in the same ciphertext. How would you decrypt a CBC-encrypted message?

2. Authentication:
   Show how two-way authentication works using RSA.

3. Endianness:
   Problem 7.7 from Peterson and Davie.

4. QoS:
   Consider the receiving side of a video stream that has a long-term average rate of 100 Mbps.

   (a) What is the average interpacket gap if each packet is 1 KB in size? (The interpacket gap should be measured from the first bit of one packet to the first bit if the next packet.)

   (b) Suppose the largest possible interpacket gap is 500 msec. Where should the playback point be set to ensure that all packets (frames) arrive in time?

   (c) How much buffering is required to support this playback point?

5. Resource Reservation:
   A computer on a 6-Mbps network is regulated by a token bucket, initially filled to capacity with 8 Megabits, and being filled at a rate of 1 Mbps. How long can the computer transmit at the full 6 Mbps?

6. QoS:
   Problem 6.44 from Peterson and Davie, 2nd edition.

7. Domain Name System:
   Problem 9.12 from Peterson and Davie, 2nd edition. This problem involves using nslookup to familiarize you with the domain name system. I will not go over this problem in class.