Midterm

LBSC 690
October 11, 2009

Name: ________________________
by writing my name I swear by the honor code

Read all of the following information before starting the exam:

- Show all work, clearly and in order, if you want to get full credit. I reserve the right to take off points if I cannot see how you arrived at your answer (even if your final answer is correct).
- You have an hour and a half to complete this exam.
- This exam is closed book, but open notes. You may use a calculator, but you shouldn't need to.
- Justify your answers algebraically whenever possible to ensure full credit. Be sure to have units for all answers that call for them.
- Circle or otherwise indicate your final answers.
- Please keep your written answers brief; be clear and to the point. I will take points off for rambling and for incorrect or irrelevant statements.
- This test has eight problems, but you only need to complete **five** questions. If you answer more than five questions, I will grade the first five completed questions. (If you change your mind on which questions you want graded, be sure to clearly identify which questions shouldn't be graded.)
- Good luck!

1. Inspector Javert is going high-tech, and decimal designations are so nineteenth century. What would prisoner 24601 be in binary? In hexadecimal?

Power of 2	Value	Used?	Remainder
14	16384	1	8217
13	8192	1	25
12	4096	0	25
11	2048	0	25
10	1024	0	25
9	512	0	25
8	256	0	25
7	128	0	25
6	64	0	25
5	32	0	25
4	16	1	9
3	8	1	1
2	4	0	0
1	2	0	0
0	1	1	0

In binary:	0110	0000	0001	1001
In hex:	6	0	1	9

2. *Moby Dick* has about two hundred thousand words. If you stored the novel in 8-bit ASCII text, how large would the file be in KB? If you wanted to store fifteen million (the number of volumes in Harvard's library) books the size of *Moby Dick*, how much space would you need? How many DVDs (feel free to round to the nearest GB) would you need? (Use the power of 10 approximation for converting MB to KB.)

$$\frac{200 \cdot 10^3\text{words}}{1} \cdot \frac{1\text{byte}}{\text{word}} \cdot \frac{1\text{KB}}{10^3\text{byte}} = 200\text{KB} \tag{1}$$

$$\frac{15 \cdot 10^6\text{book}}{1} \cdot \frac{.2 \cdot 10^6\text{B}}{\text{book}} = 3 \cdot 10^12\text{B} = 3\text{TB} \tag{2}$$

If you use the 2^{10} conversion, you should get something like 195 KB and 2.8 TB.

Number of DVDs:

$$\frac{3000\text{GB}}{1} \cdot \frac{1DVD}{5GB} = 600DVDs \tag{3}$$

3. Explain how public-key cryptography works (at a very general level, but with sufficient detail to distinguish it from symmetric key cryptography). Explain why it is important, what weaknesses it has, and how these are often addressed in practice.

   Let say that Alice wants to send Bob information, but there's no secret channel between Alice and Bob. In public-key cryptography, Bob has a "private key" and publishes a "public key." Alice uses the public key to encode her information so that nobody else can understand it, and Bob uses his private key to understand it. In symmetric key cryptography, both Alice and Bob have a shared secret key they use to decode a message.

   Public key cryptography is important because it is used to protect online transactions and to secure file transfers. It is vulnerable to man in the middle attacks where someone pretends to be your communication partner and replaces the real public key with something else.

4. You have five computers in a library that share a DSL connection to the Internet. The computers are locked down so that files cannot be saved locally and that files cannot be transfered between computers. A tech vendor suggests that you should upgrade your 10 Mb ethernet LAN to gigabit. Is this a good idea? How could you check to see if it would be worth it?

   It probably isn't worth it. The computers only access the Internet, and the Internet connection is too slow to saturate the local network.

5. Write an HTML snippet (you don't have to create a full page) that would best replicate the following table:

Mötley Crüe	is certainly	a **very**
motley	crew,	but I like their use of *rock dots*

```
<TABLE>
  <TR>
       <TD ALIGN="left">M&ouml;tley Cr&uuml;e</TD>
       <TD ALIGN="right">is certainly</TD>
       <TD ALIGN="center">a <B>very</B></TD>
     </TR>
     <TR>
       <TD ALIGN="left">motley</TD>
       <TD ALIGN="right">crew,</TD>
       <TD ALIGN="center">but I like their use of <I>rock dots</I></TD>
     </TR>
</TABLE>
```

6. What is the difference between between a traditional hard drive and RAM? Adress issues such as: volatility, storage medium, latency, cost per byte, and the time it takes to access arbitrary data in an arbitrary order (as opposed to sequential access).

   Volatility The contents of RAM are erased when power is removed.

   Medium A hard drive is magnetic flakes on spinning discs. RAM is solid state circuits on a chip.

   Latency RAM has much lower latency.

   Cost Hard drives have much lower cost per byte.

   Order RAM allows you to get to any data at any time. Hard drives need to rotate discs and move the head over desired data to read it.

7. What is an affordance? Give (briefly) five examples of devices or designs that have good or bad affordances.

   Affordances are cues in a design that let you know you can or should do something.

   Good affordances

   - Toaster slots and button
   - Doors with a push bar on one side
   - Shredders
   - Staplers

Bad affordances

- Doors with no indication if you should push or pull
- Buttons that say “do not push”
- Remote controls

8. Explain what happens when you point your browser to `www.google.com` and hit enter on a computer with a working Internet connection. Include the following in your description: IP address, DNS, browser cache, packet, routing, port, HTML, and web server.

   (a) You hit enter, and the your keyboard sends and interrupt to the operating system

   (b) The operating system passes that event to the active program, the web browser

   (c) The web browser takes the text in the box and parses it into an http address

   (d) The web browser checks to see if the page already exists in the local cache; if it does, it displays the cached page

   (e) Since it does not, the web browser connects to DNS server, which tells it the appropriate IP address to use

   (f) The web browser uses the port fro HTTP to connect to Google’s web server and asks for its home page

   (g) The HTML of the web page is broken into IP packets, sent to the next computer in the web server’s routing table, and the packets make their way to your computer

   (h) The packets are assembled into a complete file and displayed on your computer