Written Assignment 5 – due Wednesday, Aug 8th at 9 am sharp.

Reading Assignment

Read chapters 10 and 11 in the textbook Explorations in Computing. Read chapter 5 and Appendix A of the book Blown To Bits.

Instructions

- Type or neatly write the answers to the following problems.
- Please STAPLE your homework before you hand it in.
- On the first page of your homework, include your name, andrew ID, date, and the assignment number. Number your pages.
- You must hand in your homework at the start of class on the given due date.

Exercises

1. At a university, a student club wants to send out an individualized invitation letter to 1000 faculty for an upcoming donor event. Each letter requires the following steps, in order:

   1. Write a personal message to the faculty member on the inside of a card (10 minutes).
   2. Hand draw a scene with the club logo on the cover of the card with colored pencils. (15 minutes)
   3. Cut out and form a special envelope for the card out of a sheet of premium paper. (3 minutes)
   4. Seal the card in the envelope with glue, look up and write the address of the faculty member, and put a stamp on the card. (2 minutes)

   a. If the club utilized the principle of pipelining and had four work stations, one for each step above, and one person to work at each workstation, how many minutes would it take to complete the 1000 invitations? How does this compare to one person completing the entire task? Show your work.
   b. Can this task be completed even faster with four people concurrently? If so, explain how and compute the total amount of time needed to complete the task. If not, explain why.
2. Consider the following sorting network you saw in class:

Assume each comparator (i.e. the circles) takes time $t$ to compare its two elements and output its results and that the time for a data value to go from one comparator to the next negligible. We wish to sort 1000 sets of 6 integers each.

a. If we sort one set of 6 integers completely before starting the next set, how long will it take to sort the 1000 sets in terms of $t$? Explain your answer. (Remember that some of the comparators are operating concurrently.)

b. If we use the principle of pipelining, how long will it take to sort the 1000 sets in terms of $t$? Explain your answer. (NOTE: To simplify the problem, assume there are some dummy comparators inserted into the network as shown below so that all results arrive at the output terminals at the same time.)
3. In your own words, explain the principles of circuit switching and packet switching. Which is used on the Internet? Why?

4. Using the original IPv4 addressing scheme, a computer at Carnegie Mellon University has the IP address 128.2.13.161.
   a. What type of address is this: class A, class B, or class C? Why?
   b. Based on your answer from part (a), what is the common prefix for all computers from this organization (i.e. what numbers of the IP address would be the same for all computers at this organization), and what is the maximum number of computers that this specific organization can connect to the Internet at one time? Explain your answers.

5. The Internet is based on a number of different communication protocols. Specifically, we saw that TCP/IP is used to send messages on the Internet from one device to another.
   a. What parts of the communication process is handled by IP (Internet Protocol)?
   b. What parts of the communication process is handled by TCP (Transmission Control Protocol)?
   c. Real Time Protocol (which streams voice/video data) is normally layered above UDP rather than TCP. What characteristics of TCP make it less desirable than UDP for streaming voice/video traffic?
6. Consider a public key encryption system using RSA encryption that starts with two prime numbers $p = 97$ and $q = 233$.
   a. Compute the public key pair $(e, n)$ and the private key pair $(d, n)$ for this system. Select the smallest value for $e$ that will work, and then select the smallest value for $d$ that will work given your value for $e$. Show your work.
   b. Consider the numerical message 15110 that is to be transmitted. What is the encrypted message that should be transmitted using this system? Show your work.
   c. Verify that the receiver can decode the message from part (b) using the private key pair. Show your work.

   You may use `irb` to help you with the large computations for this problem.

7. Based on your reading in Blown To Bits, Appendix A, answer the following questions:
   a. If you have ten computers at home all connected to the Internet via your ISP, how many unique IP addresses do you get? Briefly explain how traffic is routed to each computer.
   b. Suppose an ISP company starts a service to sell music downloads. As part of this new venture, the company examines packets being sent to its users and slows down a user's connection if they detect packets from a competing music provider. Does this violate the principle of net neutrality? Why or why not?

8. Based on your reading in Blown To Bits, Chapter 5, you learned that today's encryption methods allow anyone to encrypt email and other data securely before being sent. The U.S. Government was very concerned about this type of technology since terrorists could use it to communicate without revealing their messages. What did the U.S. Government try to do in the 1990s to control this situation, and why did they give up trying to regulate encryption technology in the 2000s, even after the attacks of 9-11?

9. For each of the following patterns, describe specifically what strings would match.
   a. $p1 = \text{Pattern.new("pirates")}$
   b. $p2 = \text{Pattern.new("Eggs and (bacon|sausage|ham) for breakfast")}$
   c. $p3 = \text{Pattern.new("t...e")}$
d. $p4 = \text{Pattern.new("t.*e")}$

10. The **Loebner Prize for Artificial Intelligence** is awarded each year to the computer application that holds a conversation that most closely passes the Turing Test.
   a. What is the Turing Test? Describe this in your own words.
   b. The Loebner Prize for Artificial Intelligence was awarded in 2009 to David Levy of Intelligent Toys Ltd for **Do-Much-More**, a chatbot that converses with a user much like the Eliza program. Read about the chatbot and observe some of its responses to the comments and questions from the judges of the competition. Were some answers better than others? Give an example of a good answer and why you think it was a good response (based on the principles of natural language processing), and give an example of a poor answer and why you think it was a poor response.

11. Visit the **IBM Watson** website and view the videos **A System Designed For Answers**, **The Science Behind An Answer**, and **How Watson Works**.
   a. How does Watson use concurrency?
   b. Outline the four main steps that Watson uses to answer a question on the Jeopardy! game show. Describe each step briefly in your own words.
   c. Watson also uses the principle of **machine learning** as it plays the game. Give an example of how Watson uses correct answers during a game to adjust its algorithms to improve its game play.