MA/CSSE 473 – Design and Analysis of Algorithms

Homework 6

45 points total

When a problem is given by number, it is from the textbook. 1.1.2 means “problem 2 from section 1.1” .

Problems for enlightenment/practice/review (not to turn in, but you should think about them):

How many of them you need to do serious work on depends on you and your background. I do not want to make everyone do one of them for the sake of the (possibly) few who need it. You can hopefully figure out which ones you need to do.

4.1.1	(divide-and-conquer array max for unsorted array)
4.1.2	(divide-and-conquer array max/min for unsorted array)
4.1.7	(Mergesort stability)
4.1.9	(O(n log n) algorithm to count inversions in an array)

Problems to write up and turn in:

1. (3) 4.1.4 (logarithm base in the Master Theorem)
2. (6) 4.1.5 (Simple application of the Master Theorem)
3. (6) (RSA attacks) Read about various ways of attacking the RSA cryptosystem.

   Write about two attacks that interest you. Explain how they work.

   One place you can look is http://en.wikipedia.org/wiki/Rsa ,
4. (15) (Miller-Rabin test) Let N = 1729.
   (a) How many values of **a** in the range 1..1728 pass the Fermat test [i.e. $a^{1728} \equiv 1 \pmod{1729}$]?
   (b) For how many of those values does the Miller-Rabin test provide a witness that N is composite?
   (c) For N=1729, if we pick **a** at random, what is the probability that running the test on **a** will show that N is composite? Note: Rabin showed that for any N, the probability is at least 75%, what is it for this case?

   [**Hint**: writing a few lines of code my help you here].
5. (15) (RSA decoding). If small primes are used, it is computationally easy to "crack" RSA codes.

   Suppose my public key is N=703, e= 53. You intercept an encrypted message intended for me, and the encrypted message is 361. What was the original message? How did you get the answer?