CSC 464/564 Homework #3 Instructor: Jeff Ward
Due: Wednesday, September 12
Covers: RSA encryption; analysis of divide-and-conquer algorithms 30 points

Problem #1 (RSA calculation problem; 5 points) For this problem, you are free to use the modular exponentiation program that you wrote for Homework #2, Problem #3. Consider the RSA algorithm from Section 1.4.2.
Suppose Bob chooses $p = 131$, $q = 137$, and $e = 3$.
What is Bob's public modulus N?
What is Bob's secret exponent d?
Suppose Alice wishes to send Bob the message $x = 36$.
Derive the encoded message y that she actually sends.
Show the calculations by which Bob decodes the message.

Solve the following problems from the textbook:

2.4 (9 points) Show your work: If the result is a direct application of the Master Theorem, then say so, and give the values of a, b, and d. Otherwise, solve the problem by writing a sequence of inequalities as in Problem 2.3 (which we will do in class on September 5).

2.5 (16 points) Parts a-e, g-i. Show your work: If the result is a direct application of the Master Theorem, then you can just say "by MT". Otherwise, write a mathematical equation or two that shows how the problem reduces to a problem that you have already seen in class (say, Problems 0.2 or 2.3), or already solved in Homework 2, Problem 0.1.