## 18.310 Homework Assignment #6: Due Friday, October 24, 2008

This homework is fairly short, since the first draft of the paper is due Monday. Please turn in your spreadsheets using Stellar. To make it easy for the graders, mark the sections of the problems clearly. Label the cells you use for input and output, and put them where they are easy to find.

1. Choose two primes P and Q between 1000 and 2000. (They are chosen this size so that multiplying two numbers less than N = PQ doesn't overflow your spreadsheet arithmetic. Find them any way you want.) Construct an RSA encoder and decoder based on the number N = PQ as follows.
    a. Find a suitable number c so that the encoded message r is found by taking the message m and raising it to the power c, so $r = m^c \pmod N$.
    b. Now construct a spreadsheet program that uses Euclid's algorithm to find d so that the decoding is done by taking $r^d \pmod N$.
    c. Construct an encoder on a spreadsheet that inputs the message, and outputs $r = m^c \pmod N$.
    d. Construct a decoder on a spreadsheet that takes the output from the encoder, and raises it to the $d^{th}$ power (mod N) to decode the message.
2. Build a primality tester, that is capable of showing that 561 is not prime based on raising a randomly chosen x to the n-1 power mod n, and examining the results (and some of the results before the last one.)