18.310 Exam 2 Take-Home

Due: Tuesday, November 28, 2006

You may use your codes and spreadsheets from previous homework assignments.

Problem 1: RSA (10 points)

The received message $r = 1598936$ is intercepted and you want to break the code. The RSA code used: message m is raised to the power M (Mod N), where $M = 125879$ and $N = 2044459$, so $r = m^M$ Mod N. Retrieve the original message m.

Problem 2: FFT (20 points)

Use the Fast Fourier Transform to multiply 8675301357902468 and 1812768642097531. (see attached notes on carrying)

Problem 3: Sequential Choice (20 points)

In this problem, you will work out the details of the problem (below) given in the in-class exam.

Suppose you have been observing the price of a stock for 10 days and want to buy it within the next 15 days. Assume you are permitted to buy only at noon each day at the current price. Assume that noon prices are randomly distributed in rank over this period without correlation. Suppose you earn a bonus if you purchase at the lowest or second lowest noon price during this period. What should your strategy look like if you seek only to earn this bonus?

Determine the best strategy available to you. (hint: There are 2 thresholds. Classify by the best rank up to the first threshold and second best up to the second threshold.)