FINAL REVIEW

1. Overall Info

The exam is two hours, plus some extra time. There will be three proofs, some 'computational' problems needing to show work, and some 'just answer it' problems as before. Knowing the proofs and computations in the text (especially the proofs) and your homework will be most valuable. The exam covers everything we did in the course, including Chapters 0-4 and 6, and the parts of 5, 7, and 8 which we did, and the cryptography worksheets. Please refer to the other two handouts for review information for material prior to the second midterm.

2. Chapter 8

Know what it means for two sets to have the same cardinal number. Be able to show that two of them do. Know how to define an infinite set, and some examples. Be able to show that $\sqrt{2}$ is irrational, and general facts about irrationals. Know what *countable* and $\aleph_0$ are. Know the general processes behind showing that the rationals and the natural numbers have the same cardinal number and that the reals and the natural numbers do *not* have the same cardinal number (not every detail).

3. Cryptography

Understand how to compute $\phi(n)$, especially for product of two primes or a prime power; be able to use Euler's Theorem and the Chinese Remainder Theorem. Understand how the actual RSA algorithm (in section 5) works, especially the difference between the public and private keys.

4. Useful Review Problems

This section has the same purpose as on the previous handouts.
Practice Problems 8.3, 8.5, 8.7
Exercises 8.1, 8.15
Handout Exercises about Euler ϕ function and Euler's Theorem