

SYLLABUS
Fall 2002

Number Theory and Cryptography, V55.0103
Professor Mel Hausner

Text: *Elementary Number Theory with Applications* by Thomas Koshy

The class has two components: the lectures and the labs. As far as possible, we will attempt to correlate them, but you must expect times when one is ahead of the other. Part of the lab will clear up some of the lectures, go over homework problems, and do problems on the material of the lectures. The other part will be hands on work, usually in small groups, on the computer, and on various laboratory equipment designed for the course.

Topics include: Induction and recursion; number systems; prime and composite numbers; divisibility theory and the Euclidean algorithm; congruence; linear Diophantine equations; Pythagorean triples; Pell equation; security systems; cryptography.

There will be 2 **midterm exams** plus a **final exam**, which will be cumulative. **Homework** will be posted weekly after the Monday lectures, and will be handed in the following week to your recitation instructor. Late homework will not be accepted. The midterm exams are each worth 20% of your final grade and the final exam is worth 25%. The lab, including the homework, is worth 35%. There will be *no makeups* for the midterms.

Office hours are on Mondays, from 5:00 to 6:00, and by appointment. Homework assignments and notes (including this syllabus) will be put on my web site.

Office: Room 702, Warren Weaver Hall
E-mail: hausner@cims.nyu.edu
Web page: www.math.nyu.edu/faculty/hausner

Tel: (212)998-3162
Fax: 995-4121