CS 503 Discrete Mathematics for Cryptography Syllabus

The syllabus below describes a recent offering of the course, but it may not be completely up to date. For current details about this course, please contact the course coordinator. Course coordinators are listed on the course listing for undergraduate courses and graduate courses.

Text Books

Required
Lecture Notes , *6 Modules* , (prepared by instructor).

Recommended
A.J. Menezes et al. , *Handbook of Applied Cryptography*, CRC Press, 1996

Week-by-Week Schedule

Week	Topics Covered	Reading	Assignments
1	Divisibility in Z, Division algorithm, Euclidean algorithm	Module I, pages 1-7.	Exercises in module.
2	Extended Euclidean algorithm, Prime numbers and Prime number theorem, Euler phi function	Module I, pages 8-14.	Exercises in module.
3	Basic abstract algebra, Mod n arithmetic, Ring of integers mod n, Chinese remainder theorem	Module II, pages 1-7.	Exercises in module.
4	Finite groups, Euler's and Fermat's theorems, square and multiply algorithm	Module II, pages 8-14.	Exercises in module.
5	Finite cyclic groups, cyclic mod n units	Module III.	Exercises in module.
6	Midterm		
7	Introduction to quadratic residues	Module IV, pages 1-7.	Exercises in module.
8	Quadratic residues and the Legendre symbol, Gauss Reciprocity theorem for the Legendre symbol	Module IV, pages 8-15.	Exercises in module.
9	Quadratic residues and the Jacobi symbol, Gauss Reciprocity theorem for the Jacobi symbol	Module IV, pages 16-28.	Exercises in module.
10	Polynomial rings, division algorithm for polynomials, quotient rings and fields	Module V.	Exercises in module.
11	Finite fields, characteristic of a finite field	Module VI, pages 1-6.	Exercises in module.
12	Vector spaces and finite fields	Module VI, pages 1-6.	Exercises in module.
13	Minimal polynomials, uniqueness of finite fields	Module VI, pages 7-12.	Exercises in module.
14	Mobius inversion and the existence of finite fields	Module VI, pages 13-20.	Exercises in module.