Math 5248: Cryptology and Number Theory

Course Syllabus

Instructor: Gregg Musiker, Office in Vincent Hall 251,

Telephone (with voice-mail): 624-7073, E-mail: `musiker@math.umn.edu`

(To ensure faster responses to emails, please include the course number 5248 in the subject line.)

Meeting time: This class will meet on Mondays and Wednesdays 1:00-2:15 in Vincent Hall 113.

Office hours: Monday and Wednesdays 2:30-3:20 or by appointment.

Course Webpage: `http://www.math.umn.edu/~musiker/5248/`

Course Content: This is an introductory course in the mathematics of cryptography, the subject of how to make ciphers and break them, and related areas of number theory. Both symmetric and public key cryptosystems will be introduced. The math used in this course will be heavy on modular arithmetic, which will be introduced and covered in some depth. It also makes some use of elementary counting and probability, plus a tiny bit of linear algebra and matrices.

Prerequisites:

Two semesters of sophomore level mathematics (or the equivalent). Students will be expected to have some familiarity with proof techniques, such as mathematical induction.

Textbook:

Cryptology and Number Theory, by Paul Garrett, available at Alpha Print in Dinkytown (next to McDonald's), 1407 4th St SE., 612-379-8535. Used copies from previous years, produced by Alpha Print, are fine to use, as they are the same. However, the first edition, printed by the publisher, has substantial differences, and would not suffice.

Other useful texts (available freely and legally online):

A Computational Introduction to Number Theory and Algebra, by Victor Shoup.

Elementary Number Theory: Primes, Congruences, and Secrets, by William Stein.

(See links from the course webpage.)

Computer algebra systems (very helpful, but not essential and not required):

Sage, Maple, Mathematica, available in Math computer labs, and also (for CSE undergrads) for free downloads at CSE Labs. Some systems available online, the Sage Cell Server (`http://sagecell.sagemath.org/`) and Wolfram Alpha (`http://www.wolframalpha.com/`), are sufficient. A calculator is advisable, even if you use a computer algebra system, to reduce the tedium of computations.

Homework (25%): There will be 6 homework assignments due approximately every other week (tentatively) mostly of Wednesdays. The first homework assignment is due on February 4th.

I encourage collaboration on the homework, as long as each person understands the solutions, writes them up in their own words, and indicates on the homework page their collaborators. Late homework will not be accepted. Early homework is fine, and can be left in my mailbox in the School of Math mailroom in Vincent Hall 107. Homework solutions should be well-explained– the grader is told not to give credit for an unsupported answer. Complaints about the grading should be brought to me.

Three Exams (approx. 25% each): There will be 3 in-class exams (the first one is worth 20%, the second is worth 25%, the third is worth 30%) on Monday February 16th, Monday April 6th, and Wednesday May 6th. Each exam is open book, open notes, and with scientific or graphing calculators allowed, but no smart phones, iPads, or other communication devices can be used, and you have to do all the work yourself. Missing an exam is permitted only for the most compelling reasons. You should obtain my permission in advance to miss an exam. Otherwise you will be given a 0. If you are excused from taking an exam, your other exam scores will be prorated.

There is no final exam although the material in this course build on each other so while the third exam is not comprehensive, it will involve most of the topics from the course.

Class Participation: Participation in class is encouraged. Please feel free to stop me and ask questions during lecture. Otherwise, I might stop and ask you questions instead.

University Policy Statements: The University Senate statements regarding academic dishonesty, credit, and workload expectations, and grading standards are at

`http://policy.umn.edu/Policies/Education/Education/GRADINGTRANSCRIPTS.html` and

`http://policy.umn.edu/Policies/Education/Education/STUDENTWORK.html`.

Scholastic Misconduct: You must do your own work on all portions of the exams. Academic dishonesty in any portion of the academic work for this course will be grounds for awarding a grade of "F" for the entire course.

Workload: One credit is defined as equivalent to an average of three hours of learning effort per week (over a full semester) necessary for an average student to achieve an average grade in the course. This course is a 4 credit course that meets 3 hours per week. Therefore, you should expect to spend an additional 9 hours per week on coursework outside the classroom.

Tentative Homework and Exam Schedule:

HW 1	Wednesday	2/4
Exam 1	Monday	2/16
HW 2	Wednesday	2/25
HW 3	Wednesday	3/11
HW 4	Wednesday	4/1
Exam 2	Monday	4/6
HW 5	Wednesday	4/22
HW 6	Monday	5/4
Final Exam	Wednesday	5/6

First Homework Assignment (Problems from Garrett Text):

1.1 # 5, 10
1.2 # 4
1.3 # 3
1.5 # 2, 7, 9
1.6 # 4, 12, 15
1.7 # 3, 7, 14
4.2 # 3, 8
6.2 # 3

Check the Course Webpage `http://www.math.umn.edu/~musiker/5248/`

for Other Homework Assignments.