Math 5248
Crypto and Number Theory

Prof. Paul Garrett

3:35-5:00 MW in Fraser 102

Course web page:
http://www.math.umn.edu/~garrett/crypto/
Announcements will appear there, so please check that page often.

Text: My book *Making and Breaking Codes, an Intro to Cryptology*, **second printing**, available in the bookstore. (The second printing corrected many errors in the first printing.)

Errata:

http://www.math.umn.edu/~garrett/crypto/Errata.html
and
http://www.math.umn.edu/~garrett/crypto/Errata2.html

Introduction to cryptology, number-theory, algebra, and algorithms. Protocols. Symmetric versus asymmetric systems. Stream, block ciphers. One-way functions, signatures. Key management issues. DES, AES (Rijndael). (Pseudo-) random number generation. Permutation groups, primes, Euclidean algorithm, finite fields, quadratic reciprocity. Discrete logs, RSA, pseudoprimes, rho method. Elliptic curve methods. And so on.

Grading:

• take-home quiz each week (given out Monday, collected Wednesday)

• three 85-minute **midterms** on Wed Oct 8, Wed Nov 12, and Wed Dec 10

• a term project due Dec 10.

The midterms are reviews of previous quizzes. All exams are open-book, open-notes, open-calculator, etc. The quiz scores and project scores will *not* be curved: if everyone does well, everyone gets a good grade. Of the course grade each midterm is 15%, project is 20%, and the take-home quizzes are 35%. Late take-home quizzes (without prior arrangments) lose 10 points per 24 hours late, out of 100.

The content of the project is flexible, and can be done either individually or in groups. It should be at least 10 pages typed (1.5 spaced with at most 11-point font), with bibliography.

Gradeline ranges:

A : 93.00-100.0	A– : 90.00-92.99	
B+ : 86.67-89.99	B : 83.34-86.66	B– : 80.00-83.33
C+ : 76.67-79.99	C : 73.34-76.66	C– : 70.00-73.33
D+ : 65.00-69.99	D : 60.00-64.99	

Of course **plagiarism** of text or images or other IP is prohibited.

In particular, verbatim or nearly-verbatim copying from **my solutions** from homeworks or exams from prior years is **prohibited** on homework or exams.

You certainly **may** copy from **your own** stuff.

And cutting-and-pasting of text and/or images from the internet without giving credit or in violation of copyright or other IP laws is prohibited.

Office hours: 2:45-3:30 MW in Vincent 353, and 5:00-5:30 MW (in the classroom), and 3:30-5:00 Tuesday (in Vincent 353).

email is by far the best way to reach me

Office: Vincent 353 (north stairwell), phone (612) 624-5012. **EMAIL IS BEST**.

Please do not drop by my office at non-office hour times and ask whether I'm busy or not... **Sending email is ok anytime**, because I can reply when I have a spare moment.

We will follow IT/CLA policies on incompletes, scholastic misconduct, etc.

Incompletes can be given only if you've completed a majority of the course with a passing grade and agree to complete the incomplete within a short time after the end of the semester. You **cannot** complete an incomplete by retaking the course in the future.

Writing: All answers on homeworks and midterms should be in complete sentences, with reasonably good grammar and spelling. What you have on the page should make sense when read out loud.

Getting a **final answer** is probably necessary, but is not the whole point.

Showing computations/work necessary, but is not the whole point.

Following an algorithm is often the right thing to do, but is the not the whole point.

Also *explain what is happening well enough so that someone else could redo what you have done without prior knowledge.*

That is, give a **narrative** that tells what is happening, what is not happening, and why. What branches in an algorithm were *not* taken? What criteria *were* met leading you to do a particular thing? What would you have done *otherwise*?

Do not use *abbreviations* which reduce readability.

Format writing on the page in logical order.

Do not require the reader to *solve a puzzle* to figure out your intent.

Bad grammar and bad spelling are undesirable because they weaken the sense of your writing.

Do not write in a manner so that the reader must already know the answer and method to understand what you've written.

On the other hand, don't tell everything you know on every question, regardless of the relevance. Yes, *figuring out what to say and what not to say is part of every question. What is the proper context? What is relevant? What is irrelevant?*

What are the primary issues? Secondary? Subordinate? Deciding this is always the most important item.

My grader has worked with me for more than a year, and follows my instructions.

Of course if the grader has blundered, I am more than happy to repair the mistake and apologize for it.

However, you should look at what the grader has written before presuming that the grader blundered.

In particular, choice of numbers of points to deduct is a judgement call which the grader has usually discussed with me beforehand. The grader is careful to be *uniform* in grading.

• Do *not* copy your friend's 5248 homework sheet: the papers are *numbered*, and each paper has different data.

• *Instead*, send me email if you need to get a homework paper. I will make one for you and send you the URL of the PDF file.

• Put '5248' in the subject line of email, to not get *spam-filtered*.

• I do email as fast as I can. If I have not responded to your email it means I've been veeeerrrrry busy, too busy to answer all my email! *Sending multiple copies or coming to my office will not solve that problem...* :-)