Tom Roby's Math 3094 Home Page (Spring 2010) Cryptography



Questions or Comments?

- Send me email (click here and delete "QQQ")
- Homepage: http://www.math.uconn.edu/~troby
- Offices: MSB M212 and CUE 123: phone: 860-486-8385
- Office hours are Tuesdays 2-2:50 and Thursday 11-11:50 in CUE 123 and by appointment. My office in the math department is MSB 212. Whichever office you look for me in, I'm likely to be in the other one, or in a meeting, so it's best to call or email first (see coordinates below). Email is generally the best way to reach me. I try to block out most mornings for research and writing (or it languishes).

Class Information

COORDINATES: Classes meet Tuesdays and Thursdays 12:30-2:00 in CUE 321. The registrar calls this Section 001, #19187.

PREREQUISITES: Consent of Instructor, excellent performance in previous math courses, linear algebra (at the level of Math 2210Q), and experience with mathematical reasonsing (at the level of Math 2710). This is a Math Scholars course.

TEXT: Wade Trappe and Lawrence C. Washington: *Introduction to Cryptography with Coding Theory, 2nd Edition* (July, 2005). The ISBN is 0-13-186239-1. **You will need to purchase this through some (probably online) source other than the UConn Co-op.** Let me know if you have any trouble getting it.

WEB RESOURCES: The homepage for this course is http://www.math.uconn.edu/~troby/Math3094S10/. The second author also has a useful site with errata and downloadable programs at: http://www-users.math.umd.edu/~lcw/book.html.

SOFTWARE The authors provide programs that do cryptographic computations in each of the the three major commercial symbolic algebra packages: Maple, Mathematica, and Matlab. Unfortunately, these all cost significant amounts of money. I just learned more about a possible free open-source alternative called Sage, which we may try using for computations.

GRADING: Your grade will be based on one midterm exam, homework & (possible quizzes), and a final presentation.

The breakdown of points is:

HW (& Quizzes)	Midterm	Project
35%	35%	30%

MIDTERM EXAM: Will cover all the material to that point in the term. It is currently scheduled for **6 April**. Please let me know immediately if you have a conflict with that date (the Tuesday after Easter). This class is small enough that if we can agree on an alternate date, that's OK--I just want to avoid giving makeup exams at all costs.

QUIZZES: Quizzes will only be given if it seems to be pedagogically preferable. For this group, I suspect that HW might be enough. But I'm not ready to rule out the possibility entirely yet.

HOMEWORK: Homework for the sections scheduled for a given week are due the following Thursday. I will not be able to check your homework thoroughly, but may grade a random sample of problems carefully. Please provide clear and complete solutions, not just correct answers. The quality of your writing is important.

You may find some homework problems to be challenging, leading you to spend lots of time working on them and sometimes get frustrated. This is natural. I encourage you to work with other people in person or electronically. The HuskyCT site for this class has discussions boards you can use for this purpose (though I may not check them regularly). It's OK to get significant help from any resource, but in the end, please write your own solution in your own words. Copying someone else's work without credit is plagiarism and will be dealt with according to university policy. It also is a poor learning strategy.

PROJECTS: are described in the link. Please select your research topics by 9 February. First drafts of papers are due 10 April. Presentations will start shortly thereafter.

CONTENT: Cryptography is a fascinating subject, with venerable history and many ties to modern mathematics. The fates of monarchs (e.g., Mary Queen of Scots) and empires have been determined by whether a cipher was sufficiently strong to withstand attack. Today the widespread use of electronic communication, and the ease with which such information can be captured, has made the use of cryptographic systems essential in everyday commerce. The distinction between "http" and "https" is one of whether a Secure Socket Layer (SSL) of encryption (whose details are invisible to those using them) prevents someone's credit card number or identity being stolen.

DISABILITIES: If you have a documented disability and wish to discuss academic accommodations, or if you would need assistance in the event of an emergency, please contact me as soon as possible.

LEARNING: **The only way to learn mathematics is by doing it!** Complete each assignment to the best of your ability, and get help when you are confused. Come to class prepared with questions. Don't hesitate to seek help from other students. Sometimes the point of view of someone who has just figured something out can be the most helpful.

We will often spend classtime doing things in groups, presenting mathematics to one another, or having interactive discussions. There will not be time for "cover" all material in a lecture format so you will need to read and learn some topics on your own from the book, web sources, (or otherwise).

HONORS CONVERSIONS If you are in the Honors Program and perform at the level of a **B** or better, then this course will automatically convert to an honors course. You don't need to fill out the paperwork yourself.

SCHEDULE: The following is a the start of a tentative schedule, that I will update throughout the semester.

3094 (STILL BEING REVISED) LECTURE AND ASSIGNMENT SCHEDULE

Section	Date	Topics	HW Problems
Ch.1	1/19 T	Overview of Cryptography	
§3.1-3	1/19 T	Divisibility & Modular Arithmetic	
§2.1-2	1/21 R	Shift & Affine Ciphers;	HW #1: p. 55: #1, 2, 4, 6, 7, 8, 11; p. 59: #2, 3, 7, 9
§2.3, 2.12	1/26 T	Cracking Viginere; Exponents in Mods	HW#2: p. 55: #13,16,18,19,22,23,25; p. 61: #12,12
§2.6-11	1/28 R	Hill Cipher & LFSR	HW#2 (cont.): p. 104: #1, 3, 5, 6, 12
§3.1-4	2/2 T	NT: (Simultaneous) linear congruences, primitive roots	HW #3: p. 104: #2,10,16,20,23,25,26,27
§3.5-7	2/4 R	NT: Discrete exponentials & logs	p. 111: #3,9
§3.9	2/9 T	NT: Solving quadratic equations	
§3.10	2/11 R	NT: More quadratics in mods	HW #4: pp. 104ff: #9,14,17,21,29,30,31,32,39
§6.1,7	2/16 T	Public Key & RSA	Choose Project Topic by today
§6.2	2/18 R	RSA 2	HW #5: p. 192: #3,6,7,8,10,13,17,19,21,23; p. 199: 12,13,14
§6.3	2/23 T	(Probablistic) Primality Tests;	
§6.3	2/25 R	Solovay-Strassen Test	HW#6A: §7.6 (p.215) #6, 8; Sec. 7.7 (p. 216) #4
§8.1-4	3/2 T	Discrete Log:	HW #6B: §8.8 (p. 239) #1,2,3,4,6,9a,10; §8.9 (p.242) #1,2;
§	3/4 R	Hash Functions	**Project Outlines due 3/5.**
		8-12 MARCH SPRING BREAK NO CLASSES	
§ 18.1	3/16 T	Intro. to ECC	**HW6 due today (or Wed. by 2:50p.m.) in CUE 123.**
	3/18 R	Dr. Conrad: Check Sum Digits	
§ 18.2	3/23 T	[DL] ECC	
§ 18.3	3/25 R	[DL] Bounds on General ECC	
§ 18.4	3/30 T	Linear Codes	**First drafts of papers due**
§ 3.11	4/1 R	Finite fields	HW7: WT §18.12 #1-10; §3.13 #33,34

§ 18.7	4/6 T	Cyclic codes	
§ 18.8-9	4/8 R	BCH & Reed-Solomon Codes	
§	4/13 T		
§	4/15 R	Projects: *Atif* & *Nikhaar*: NTRU Encryption	HW8: WT §18.12 #11-15,17-19; §18.13: #2
§	4/20 T	DL	
§	4/22 R	Projects: *Mike* & *Jon*: Braid Group Crypto	
§	4/27 T	Projects: *Jakob* & *Tiff*: Quantum Crypto	
§	4/29 R	Projects: *Yehven* (TBD) & *Briana* (DRM & stream ciphers)	

Web Resources

Web Resources abound for cryptography, and a careful google search will often reveal useful slides, handouts, write-ups, and applets that are outside your instructor's knowledge. As you find such things, please share them with me, and I'll make sure they get out to the whole class.

- Keith Conrad has an Expository paper website with lots of useful handouts, which I'm using without compunction (but with attribution).
- Cristina Nita-Rotaru has a website for her CS 355 Cryptography course at Purdue University, with links to slides for her lectures. We may use some of these to frame class discussions.
- Tom Linton has a Cryptography webpage with links to Java applets

---

NEWS & NOTES

Thanks to Professor Conrad, here's a copy of the original paper on RSA encryption by Rivest, Shamir, and Adelman.

The Wikipedia article on the Pohlig-Hellman technique for finding discrete log (mod p) when p-1 is smooth is stubby, but has a link to the original article. Here's a fully worked out example from a page of Bill Cherowitzo.

Back to my home page.
