MATHEMATICS 4440
SPRING 2014
CODING AND CRYPTOGRAPHY

Instructor: Katherine Stange
kstange@math.colorado.edu
Math Office 308 ☛ (303) 492-3346

Monday, Wednesday, Friday 2:00-2:50 pm, FLMG 156.

http://math.colorado.edu/∼kstange/4440-Spring2014
It is your responsibility to notice online announcements, which will be posted under "Virtual Class".

Goals

(1) To learn the mathematical underpinnings of cryptography and coding theory.
(2) To learn to encipher, decipher, cryptanalyse and use cryptography securely.
(3) To learn to code and decode.
(4) To learn basic computer programming.
(5) To learn or improve your LaTeX skills.
(6) To improve your ability to communicate mathematics.
(7) To improve your ability to think mathematically.
(8) To have fun.

Prerequisites

I will not assume any particular mathematical knowledge beyond the ability to solve a system of linear equations, but the course will require a degree of *mathematical maturity*, meaning the ability to follow and communicate mathematical and logical argument.

Varying backgrounds and ability

This is a mixed course. There are undergraduate and graduate students. Some students will come to this course with more background and mathematical experience than others. There are two versions of this course: 4440 (undergraduate) and 5440 (masters). The masters students will do harder problems on homework and exams. Undergraduates with strong

Date: Last revised: January 4, 2014.

backgrounds may register for 5440 with permission in order to do the "advanced stream."

Laptops

Please bring a laptop to *every* class. We will frequently use them for groupwork, Sage demos, etc.

LaTeX

I require that you type your homework in the mathematical typesetting system LaTeX. (*There is no other reasonable way to type math on a computer.*) This takes a little time out of our course at the beginning, but having and knowing latex will be invaluable to you, especially if you are a math or cs major.

Programming

Part of the purpose of this course is to learn basic programming in the context of symbolic math software. We will be writing short routines and implementing algorithms in Sage. Resources are available on the webpage.

Textbooks and Resources

Please see the 'Resources' tab on the website, which includes many online resources. In addition, there are two paper texts at the bookstore and the library reserve (which may be more cheaply available as e-books).

Introduction to Cryptography with Coding Theory, 2nd ed. by Wade Trapp and Lawrence C. Washington. This is the mathematical textbook for the course, which we will use for readings, reference and exercises.

The Code Book by Simon Singh. This book is a highly readable and enjoyable account of the history of cryptography. The history and application of cryptography is deeply intwined with its mathematics, and the subject cannot be studied without a wider perspective.

Lecture Questions

Each day you will be given a notecard and will write upon it a question about that day's class. You can ask your question out loud in class if you like also, or you can just hand it in, but you have to have at least one question. A good question is designed to help clarify your understanding. This usually means that a precise question (e.g. 'Why does that definition require condition blah? Couldn't you define it without that?') is better than a vague one (e.g. 'What is the point of codes?'), but sometimes a vague question is the right way to go. The point is to ask a question that is useful to your understanding. I will do my best to address the questions next class. (This will not be graded.)

Course Schedule

On the course webpage there will be a course schedule. I will post homework assignments for each lecture period. Although only some will be designated for handing in, all of them are required (readings, etc.). It is your responsibility to check the schedule every day to see what is required.

In addition, there are two important dates:

Midterm	Thursday, February 27th, 5:15 - 6:45 pm.
Final Exam	Monday, May 5th, 1:30 pm - 4:00 pm.

Instructor's Office Hours

Since this is a small class, I will hold office hours per request. That means if you want to consult me, then email me to set up a time, and I will advertise the time to the rest of the class so other people can benefit also (unless it is a private matter). We may develop a regular schedule as the semester progresses.

Discussion Boards

Some assignments will require posting codes on the internet for each other. On the course website you'll find "Virtual Classroom" which is just a wordpress blog. Discussions will take place there.

Group Work

Some homework will involve working in groups, posting ciphertexts on the website for each other, etc. We will exchange contact information and you will work in groups both inside and outside of class.

Grading

Final Exam	30
Midterm	20
Classwork	50

The midterm will be designed to take one hour to complete, but you will be given one hour and a half to write it. The final exam will be cumulative. It will be designed to take two hours to complete, but you will be given 2.5 hours to write it.

Course Policy on Homework Help

In this course I strongly encourage you to work together. There are caveats about how you write up your solutions, however, as follows.

On graded work, you are encouraged to seek help through all the means available to you: instructors, resource center, internet, tutors, etc. The internet *can* do your homework for you, especially the computational parts.

However, it is your responsibility to seek only those means of help through which you *learn*. Don't just let others do the work for you. Specifically, when you write your solutions, **you must write them alone, in your own words, using your textbook and course notes if necessary, not copying from other notes, websites, friends, or any other source**. This means you can work on problems with your friends, your tutor, or your dog, but you must **not** copy answers during the discussion; instead, you must write in your own words, afresh from your own newly improved brain, *after* the discussing and working has been done. This is course policy, but it is also common sense study habits.

Furthermore, if you did work with others or receive help, I expect you to cite the sources clearly on your homework (URLs, books including page numbers, friends' names).

Failure to follow this policy may result in a grade of zero.

Special Requests

I am happy to accommodate disabilities or religious observances, or a request that I address you with a different name or pronoun than my roster indicates. Please contact me as soon as possible.

Missed or late work:

... receives a zero. The lowest 15% of homework scores are automatically dropped; this should cover any unexpected illnesses or other legitimate reasons to miss work. If you are missing more work than this, you must come talk to me.

If you have a religious exception or other legitimate reason to reschedule the midterm or final, please make arrangements with me **as soon as possible.** If you missed a midterm without permission, you must supply a note specifically excusing your absence (i.e. 'Jane Doe *could not* attend the midterm because she swallowed a cat / was abducted by militant Pastafarians') from a doctor or the Office of the Dean of Students. In that case, and only in that case, appropriate grading adjustments will be made.

University Policies

Please see the course website for University Policies concerning such matters as religious holidays, the Honour Code, harassment, etc.