Math 4753-503: Introduction to Cryptography

Professor: Paul Fili
E-mail: paul.fili@okstate.edu (e-mail me with questions at any time)
Lecture: MWF 12:30-1:20 in HSCI 029. Lecture videos will be available online.
My Office: 532 Mathematical Sciences Building
Office Hours: Remote office hours will be available via Google Hangouts and/or Skype by appointment.

Online Classroom (D2L) site: https://oc.okstate.edu (then log in and find our course)
Prerequisite: MATH 3013; MATH 3613 or CS 3653
Textbook: An Introduction to Mathematical Cryptography, by Hoffstein, Pipher, and Silverman.

About this course: The basic problem of cryptography concerns how two people can identify each other and communicate privately in the presence of eavesdroppers or middlemen. Early uses of rudimentary cryptography date back at least as far as Caesar, but the subject did not reach its modern form until the invention of public key cryptography in the 1970s. We will study some of the common modern cryptosystems in use today and the problems on which they are based, such as the integer factorization problem, the discrete logarithm problem, and some elliptic curve analogues. It has been known since Shor's seminal 1994 paper that several of these systems will become obsolete with the growth of quantum computing, spurring an interest in so-called "post-quantum" cryptography. We will discuss the implications of quantum computing and review one class of post-quantum cryptosystems, specifically, lattice based systems.

As part of this emphasis on these computational applications, we will also make use of the open-source computational software package Sage, which is a set of mathematical libraries built over the Python language. *No programming knowledge is assumed*. Sage is available for free download from www.sagemath.org or can be run remotely on the server www.sagenb.org. Sage is best installed locally if you have a Mac (choose the “Notebook interface” download) or if you run Linux, however, in Windows it must be run in a virtual machine. This is easy but can be a little demanding on your hardware, and it might be easier to to use the online server in this case. If you choose to use the website, beware that the website does has occasional connectivity issues and plan accordingly for your homework. If you would like help setting up Sage, please feel free to come talk to me!

Homework: There will be weekly homework in this course. You should expect the homework to take a significant amount of time each week. Some of the questions assigned might be rather difficult, and I expect each of you to e-mail me, come to my office hours, and talk with each other in order to complete the homework. You are allowed to collaborate on homework so long as you do not copy each other's work (i.e., you can discuss the ideas, but you must write your own solutions without looking at other students' write-ups). Repeated direct copying of other students' work may result in an an F!, so be sure to write up your own solutions.

Students are encouraged to use LaTeX to typeset their homework. **A 5% bonus will be given on each typeset homework.** Templates will be provided to ease learning of LaTeX, and you can easily find answers to many basic LaTeX questions on the web. For more information on typesetting software, visit the LaTeX project at http://www.latex-project.org. You will need to download and install first a “distribution” and then download a typesetting front-end which will use that distribution. Common choices for a front-end include Texmaker (cross-platform), Kile (Linux – my personal favorite), and LyX (Mac and Linux, Windows under cygwin). LyX in particular is a WYSIWYG editor so it might be easier for first time users.

For the 503 section, homework may either by e-mailed to me, or uploaded onto D2L in the appropriate drop boxes. You must be able to scan your homework, or upload a LaTeX'd PDF.

Exams: There will be two midterm exams. The first will be an hour-long in class; the second may be again in class or may be a take-home exam depending on the material covered at that point in the semester. (Perhaps I will take a vote to see what students would prefer.)

For the 503 section, exams will be administered by a local testing center which we will agree upon. It is your responsibility to make arrangements for the testing center in time for the exam day, and to help me get in touch with them to supply them with a copy of the exam.

Grading: The grading for this course will be as follows:

Two midterm exams	15% each (x 2 = 30%)
Final exam	20%
Homework, quizzes, any other misc. classwork	50%

Graduate credit: You may take this course for graduate credit. You will be required to do assignments on the graduate level during the course of the semester, which will typically be 2-week long assignments, in addition to the undergraduate assignments.

Undergraduates may also hand in solutions to the graduate for 20% extra credit, thus, if an undergraduate scores 50/100 on a graduate assignment, that will count as +10 on the homework score.

Lectures: Lecture videos will be available online for the 503 section. Please e-mail me with any questions or problems you have accessing the videos, and be sure to watch them regularly to keep up with the course.

Policy on missed work: Students will be offered reasonable accommodation in the event of a missed major assessment activity for a valid and documented reason. You will be required to notify me and provide me documentation of this reason as soon as is possible.

Syllabus Attachment: Please read the OSU syllabus attachment on the web, linked at http://academicaffairs.okstate.edu/current-students. This has a lot of important information, including instructions about disability accommodations. Please contact me privately during the first week of the course if you need accommodations as the result of a disability.