Math 360, Mathematics of Information Security, MWF 11:00, Room E203

Lecturer: Alexander Hulpke, Weber 104

Office Hours: See `http://www.math.colostate.edu/~hulpke/officetimes.html`
Tentatively: T11,MF2

Email: `hulpke@math.colostate.edu`

WWW: `http://www.math.colostate.edu/~hulpke/lectures/m360`

This class covers (as it says on the tin) the mathematics that underlies moidern methods for information security. While we will look at encryption schemes and their weaknesses this class is focussed neither on cryptoanalysis (breaking encryptions), nor on practical aspects of implementing solid encryption schemes. (And if you expected the textbook to be written by Dan Brown, you are definitively in the wrong class ...)

Textbook: Hoffstein, Pipher, Silverman: *An Introduction to Mathematical Cryptography*, Springer. A downloadable PDF version is available freely through CSU (your computer must be on the campus network) at `http://link.springer.com/book/10.1007/978-0-387-77993-5/page/1`. If you trust your notes you will take in class, you can do without a textbook.

(Relevant to the topic, but not to the class:) If you are interested in cryptoanalysis and in the history of the subject you might find

- F. Bauer, *Decrypted Secrets*, Springer,
`http://link.springer.com/book/10.1007/978-3-540-48121-8/page/1` (same rules as above), and:
- C. Bauer, *Secret History: The Story of Cryptology*, Chapman and Hall/CRC

interesting. If you are interested in practical aspects or descriptions of existing cryptosystems

- Katz, Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, Chapman and Hall/CRC,
- Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, and
- Ferguson, Schneier, Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley
- Stinson, *Cryptography: Theory And Practice*, Chapman and Hall/CRC

are good sources.

Public Service Announcement

The encryption schemes discussed in this course (and in many books) are in themselves just proofs of concept. To make a cryptosystem safe in practice it is often necessary to implement further mechanisms (such as padding) to protect against repeated patterns in messages.

Exams

There will be two midterms: October 4 and November 8 at the usual class time, as well as a final on Dec 20, at 7:30am (Sorry! That time is not my choice), all in the regular class room.

Grades

will be based on homework (40%), midterms (20% each) and final (20%). (This implies in particular, that it will be extremely hard to get a good grade if homework is not submitted regularly!) Grades will be given on a linear scale with about 50% corresponding to D and 90% to A.

I expect to see you regularly in class and to regularly hand in solutions to the homework problems.
For privacy reasons the university does not permit open posting of grade information. Because of this, grades (in particular for the final and overall grades) will be posted regularly in RamCT. (RamCT will only be used for posting grades. Discussion or email tools in RamCT will not be used.)

Homework

Homework will be handed out every Monday in the lecture, and is due at the start of the lecture of the Wednesday of the following week. Late homework will be accepted only if the delay is due to reasons beyond your control. I will consider 20% of the homework as bonus, that is full homework points will be obtainable with 80% of the homework. (But homework points cannot make up for exam points.) Homework sheets will also list some problems from the book as "practice" problems (which cannot be handed in, but may be exam relevant). These problems are typically routine calculations, which I will assume you are able to do.
Because of time restrictions, only to some of the problems can be worked in class, but I'm happy to go through any problems during office hours.

Academic Integrity

This course will adhere to the CSU Academic Integrity Policy as found in the General Catalog - section 1.6, pages 7-9 and the Student Conduct Code. At a minimum, violations will result in a grading penalty in this course and a report to the Office of Conflict Resolution and Student Conduct Services.

Computer use

Some problems will involve calculations that would be tedious to do by hand (or even with a simple pocket calculator). For these we will be using the computer algebra system GAP. (You are welcome to use other software if you want to, but I will not provide help with these.)
This program is installed on the PCs in the Mathematics lab. If you want to install it on your home PC (Linux/Windows/Mac) you can either download the program from the link on the course webpage. (You won't be examined about the use of this program.)
More about this program later.

In general you are welcome to use a computer/calculator for part of homework problems if doing so does not render the problem trivial. (E.g. if the problem is to calculate $17 \bmod 9$ you may not simply use the calculator to get the result. On the other hand, if the problem is to solve $5x \bmod 9 = 2$ you may do an auxillary calculation $17 \bmod 9$ with the calculator, and so on.)

I wish you success with this course and all the best for the coming semester.