MA 481/581 – Cryptography

Spring 2017; Section 101

Instructor. Dr. Armin Straub
Email. straub@southalabama.edu
Course website. http://crypto.straub.link
Office. ILB 313
Office phone. (251) 460-7262 (please use e-mail whenever possible)
Office hours. MW, 9:05-1:15pm, or by appointment
Class schedule. MWF, 1:25-2:15pm, in ILB 465

Overview. This course gives an introduction to classical and modern methods of message encryption and decryption (cryptography) as well as possible attacks to cryptosystems (cryptanalysis). Topics include classical (symmetric) cryptosystems (DES, AES), public-key (asymmetric) cryptosystems (Diffie-Hellman, RSA, ElGamal), modes of operation, one-way and trapdoor functions, Hash functions, cryptographic protocols.

Learning objectives. The goal of this course is to familiarize you with several techniques for message encryption and decryption as well as possible attacks to cryptosystems. In particular, it will be explained how mathematics can be used to protect data and make electronic systems secure. By presenting a variety of accessible topics, the course will not only give an overview of the nature of cryptology but hopefully will also show how important pure mathematics, especially number theory and algebra, is in our current world.

Textbook. *Introduction to Cryptography with Coding Theory*, by Wade Trappe and Lawrence C. Washington (Prentice Hall, 2nd Ed., 2006)

Course format. Web-enhanced

Pre-requisite. C or better in MA 311 (Intro to Number Theory)

Grading

Exams. There will be two in-class midterm exams and a comprehensive final exam. Notes, books, calculators or computers are not allowed during any of the exams or quizzes.
Our **tentative** exam schedule is:

- Midterm Exam 1: Wednesday, February 22
- Midterm Exam 2: Wednesday, April 5
- Final Exam: Wednesday, May 3 — 1:00pm-3:00pm

Quizzes. Short quizzes will be given most weeks. The main purpose is to make sure that no one gets lost, and it is a way for you to monitor your progress.

Project. Details about the project will be announced later in class and on our course website. Students taking cryptography in the undergraduate version MA 481 do not have work on a project, but may optionally do so.

Grades. Your grade will be based on the total sum of your scores on the midterm exams, quizzes, your project (optional for undergraduate students), and the final exam.

- Midterm Exams: 40% in total (47.1% without project)
- Quizzes: 20% (23.5% without project)
- Project: 15%
- Final Exam: 25% (29.4% without project)

The resulting numerical score is then translated to your semester grade as follows:
$[90, 100]$: A, $[80, 90)$: B, $[70, 80)$: C, $[60, 70)$: D, $[0, 60)$: F.

Make-up policy. There will be no make-ups for missed midterms or quizzes. Missed quiz scores are dropped if a valid excuse is presented. If a midterm is missed and appropriate documentation (e.g. a doctor's note) is presented in a timely manner, then the corresponding exam score will be replaced with the final exam score. Otherwise, the score for the missed exam will be recorded as zero.

Online grades. Your grades will be posted to USAonline. Please check your grades weekly at `https://ecampus.southalabama.edu` and report any discrepancies within two weeks.

Dropping. The final drop date is Friday, March 31. Please speak with me (and/or your advisor) before making a final decision to drop. Ideally, talk to me as soon as you are getting behind, so I can help you complete the course successfully.

Course organization

Online material. This syllabus as well as relevant information and material for this course can be found at our course website.

Attendance. Attendance of all lectures is mandatory and roll will be taken. You are responsible for finding out what you missed on days when you were unable to attend.
Let X be the number of times you miss class without excuse throughout the semester.

- If $X \leqslant 3$, then your lowest quiz score will be dropped.
- If $X > 6$, then your overall semester grade will be decreased by a full letter grade.

Students are expected to be on time in class. Frequent late arrivals of a student to the classroom will be considered a disruption and a penalty may be applied in this circumstance.

Cell phones and other electronic devices. The use of cell phones and other electronic devices, such as laptops, is not acceptable during lecture and is reserved for emergencies.

Tutoring lab. The department offers a tutoring lab in room ILB 235 to all students taking mathematics and statistics classes. There is no lab fee. Please check the bulletin board outside ILB 235 for details.

Dates of interest.

- Monday, January 16: Martin Luther King Holiday
- Monday–Friday, March 13–17: Spring Break
- Friday, March 31: Last day to drop
- Friday, April 28: Last day of classes

Changes. Not all classes progress at the same rate. Thus course requirements and policies might have to be modified as circumstances dictate. You will be given notice if the course policies need to be changed.

Additional Academic Course Policies. Information on Student Disability Services, Academic Disruption Policy and Class Demeanor, Student Academic Conduct Policy, Operational Disruptions, and other university policies are posted on USAonline.

Welcome to Cryptography!

...and please ask anytime if you have questions.