MA 481/581 – Cryptography

Spring 2019; Section 101

Instructor. Dr. Armin Straub
Email. `straub@southalabama.edu`
Course website. `http://crypto.straub.link`
Office. MSPB 313
Office phone. (251) 460-7262 (please use e-mail whenever possible)
Office hours. MWF 9-10am, 11am-noon, or by appointment
Class schedule. MWF, 1:25-2:15pm, in MSPB 235

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.

Our **tentative** exam schedule is:

- Midterm Exam 1: Wednesday, February 20
- Midterm Exam 2: Wednesday, April 3
- Final Exam: Wednesday, May 1 — 1:00pm-3:00pm

Homework. After most classes, homework will be posted to our course website. Homework is submitted online, and you have an unlimited number of attempts (a 15% penalty applies if homework is submitted after the posted due date). Only the best score is used for your grade. Most problems have a random component (which allows you to continue practicing throughout the semester without putting your scores at risk).

(The homework system is written by myself in the hope that you find it beneficial. Please help make it as useful as possible by letting me know about any issues!)

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, homework, your project (optional for undergraduate students), and the final exam.

- Midterm Exams: 40% in total (50% without project)
- Homework: 16% (20% without project)
- Project: 20%
- Final Exam: 24% (30% 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.

Bonuses. There will be a number of bonus challenges, especially during the beginning of the semester. You can also earn bonus points by finding mathematical typos in the lecture notes, or by reporting mistakes in the homework system. Each bonus point is worth 1% towards a midterm exam.

Make-up policy. There will be no make-ups for missed midterm exams. If an exam 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. Grades will be posted to USAonline. Please check your grades after each exam at `https://ecampus.southalabama.edu` and report any discrepancies within two weeks.

Dropping. The final drop date is Friday, March 29. 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. In particular, homework and sketches of each lecture will be posted there.

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 exam score is replaced with the final exam (if beneficial).
- 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.

Dates of interest.

- Monday, January 21: Martin Luther King Holiday
- Monday–Friday, March 18–22: Spring Break
- Friday, March 29: Last day to drop
- Friday, April 26: 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.