MA 481/581 – Cryptography

Spring 2021; Section 101

Instructor. Dr. Armin Straub

Email. `straub@southalabama.edu`

Email is the best way to get in touch with me. I strive to reply as soon as possible and definitely within 24 hours; if you don't hear back within 24 hours, please check the email address and contact me again (most likely, something went wrong).

Course website. `http://crypto.straub.link`

Office. MSPB 313

Office phone. (251) 460-7262 (please use e-mail whenever possible)

Office hours. MWF 9-11am, or by appointment

Held virtually using Zoom; please make an appointment by email at least 2 hours in advance.

Class schedule. MWF, 1:25-2:15pm, in MSPB 235 (however, see COVID adjustments)

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) (optional)

Course format. Web-enhanced

Pre-requisite. C or better in MA 311 (Intro to Number Theory)
or: C or better in both MA 126 (Calculus II) and MA 267 (Discrete Math)

Grading

Exams. There will be two midterm exams and a comprehensive final exam, which will be delivered online. Our **tentative** exam schedule is:

- Midterm Exam 1: Monday, March 1
- Midterm Exam 2: Wednesday, April 7
- Final Exam: Wednesday, May 5 — 1:00pm-3:00pm

Homework. Regular homework is assigned and needs to be submitted online. You have an unlimited number of attempts (a 15% penalty applies if homework is submitted after the posted due date, unless an extension has been granted due to special circumstances). 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. Homework scores are available on our course website. Exam grades will be posted to USAonline: `https://usaonline.southalabama.edu`

Dropping. The final drop date is Friday, April 2. 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, as well as recordings covering key points.

COVID adjustments. In-person class meetings are restricted by university regulations. In our case, at most 12 students are allowed to attend each time.

- A schedule of upcoming class is posted on our course website. Some of the in-person class meetings will be replaced with online lectures (either held synchronously via Zoom or via prerecorded lectures).
- Attendance of in-person classes is not required.
- In order to attend an in-person meeting, you must sign up for a cohort by sending me an email. You may attend in-person meetings only on those days designated to your cohort, as reflected by the schedule. Cohort membership is first come, first served; if your cohort of choice is full, you will be able to sign up for another cohort.
- If you are signed up for a cohort and fail to attend without informing me in advance, you will be removed from the cohort. After three days, you may sign up again (but, if full, you might not be able to get back into the previous cohort).
- Lecture recordings will be posted which you can view at your own time. These replace the classes you cannot attend. The in-person meetings will be used mainly to keep sight of the big picture and to address any questions you have.
- You are expected to have viewed all relevant lecture recordings before attending an in-person class.
- In addition to during the in-person meetings, you will be able to ask questions during office hours which will be held virtually.
- Unless specified otherwise, exams will be held online during the scheduled class times.

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.

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!

...please ask anytime if you have questions.