MA 581 – Cryptography

Spring 2026; 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

Class schedule. MWF, 1:25-2:15pm, in MSPB 370

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 (Pearson, 3rd Ed., 2020)

The textbook is a nice additional resource but is not required for the course. You will have access to the online textbook automatically on Canvas through the JagPack Program (https://www.southalabama.edu/programs/jagpack/) unless you opted out.

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 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: Monday, February 23
- Midterm Exam 2: Monday, April 13
- Final Exam: Wednesday, May 6 — 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. Students enrolled in MA 581 need to complete a project. The idea is to gain additional insight into a topic of cryptographic relevance that you are particularly interested in and which is not covered in class. Some suggestions for projects will be posted on our course website. The outcome of the project should be a short paper (about 5 pages) in which you introduce the topic, and then describe how you explored the topic. Here, exploring can mean (but is not limited to) computations or visualizations you did in, say, Sage, working out representative examples, or combining different sources to get an overall picture. Each project should have either a computational part or have a more mathematical component.

Grades. Your grade will be based on the total sum of your scores on the midterm exams, homework, your project, and the final exam.

- Midterm Exams: 40% in total
- Homework: 16%
- Project: 20%
- Final Exam: 24%

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. 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 5. 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. If you are unable to attend a class because you don't feel well, or because of any other reason, please let me know by email so that the absence can count as excused. 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.

Never attending this class, or stopping attendance before the end of the term, may result in the assignment of an F* grade. A grade of F* could affect your financial aid eligibility. Attendance in this context refers to attendance or participation in an academically-related activity, such as attending the class, participating in online activities for the class, taking exams, or submitting assignments.

Cell phones and other electronic devices. The use of cell phones and other electronic devices, such as laptops, is generally not acceptable during lecture due to its potential for distraction, and is reserved for emergencies. If use of an electronic device is helpful to your learning (for instance, for note-taking) please speak with me beforehand.

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.