Math 8570-001
Cryptography
Spring 2023

Class Time/Location: T/Th, 11:00am-12:15pm, Martin M-204
Instructor: Dr. Ryann Cartor
Office: Martin O-018
Email: rcartor@clemson.edu
Phone Number: 864-656-5239
Office Hours: Wednesdays 1-2pm, or by appointment.

Course information

Textbook: Dough R. Stinson and Maura B. Peterson, Cryptography: Theory and Practice, Fourth Edition, Chapman and Hall/CRC Press.

Other resources:

- Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen, Post-Quantum Cryptography, Springer (Also can be viewed here)
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press.

Prerequisites: Linear Algebra (MATH 3110), basic probability (MATH 4000 or 6000) and some familiarity with the basic concepts of groups, rings and fields (MATH 4120 or 8510).

Learning Outcomes: At the end of the course, you will be able to: understand and perform encryption and decryption of messages using different cryptosystems, perform cryptanalysis of well-known cryptosystems, securely exchange keys over a public channel and constructing pseudo-random generators.

Topical Outline: Topics of the course will be chosen from the following pool:

- Classical cryptography.
- Shannon's Theory, entropy, perfect secrecy, and the One-Time Pad.
- Advanced Encryption Standard (AES),
- The RSA Cryptosystem and Factoring Integers.
- Block ciphers and stream ciphers.
- Hash functions and message authentication.
- Public-key Cryptography
- Identification schemes and entity authentication.
- Discrete Logarithm Problem and Diffie-Hellman Key Exchange
- Signature schemes.
- Post-Quantum Cryptography.
- Key distribution and key agreement schemes.
- Public-key infrastructure (PKI).
- Secret sharing schemes.

Absent Professor Policy: Class is cancelled if the instructor is more than 15 minutes late.

Attendance: Attendance at every class is expected whenever safe and possible. Students are expected to attend class in person when healthy and are expected to avoid in-person contact when sick. If you have an unavoidable conflict with an exam or other in-class assessment, please contact me *before* the class. In the case of a sudden emergency or illness, contact me as soon as possible. You are responsible for obtaining the content discussed in class.

Class modality: This is an in-person class. In the event that we need to switch to virtual meetings, the class would continue through synchronous Zoom meetings. I will communicate with you via email, Zoom, and Canvas for this class.

Covid Related Policies: Students are expected to follow University and CDC guidelines related to masking, quarantining, etc. Current policies can be found at the following links:

- https://www.cdc.gov/coronavirus/2019-ncov/communication/guidance.html
- https://www.clemson.edu/covid-19/index.html

GRADING

The final grade will be calculated as follows:

Homework	70%
Presentation	10%
Final Portfolio	20%

In the computation of the grade, numbers will be rounded to an integer using the floor operator, e.g. floor(79.77)=79. The grade will follow the scheme:

A: ≥90% B: 80-89% C: 70-79% D:60-69% F: 0-59%

Note, +/- may be used to reflect exemplary effort/performance.

Homework: You will have 1-2 homework assignments assigned each week. Late homework will not be accepted. Your 2 lowest scores will be dropped.

Presentation: Students will read and give a presentation on a current (published within the last 5 years) cryptography research paper. Presentations should last 10 minutes, and students should expect to answer questions after the presentation for about 5 minutes. More information on this assignment will be given closer to the due date. The presentations are tentatively scheduled for Thursday April 6, Thursday April 13, Thursday April 20, Tuesday April 25, Thursday April 27, Wednesday May 3rd, 3-5:30pm.

Final Portfolio: Students will submit a portfolio containing student work and reflections. This portfolio will allow students to demonstrate their understanding of the course topics. More details will be provided closer to the assignment due date (Wednesday, May 3rd). No late assignments will be accepted.

Standard Academic Policies

Academic Integrity. As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a "high seminary of learning." Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form.

All infractions of academic dishonesty by undergraduates must be reported to Undergraduate Studies for resolution through that office. In cases of plagiarism instructors may use the Plagiarism Resolution Form.

See the Undergraduate Academic Integrity Policy website for additional information and the current catalogue for the policy. For graduate students, see the current Graduate School Handbook for all policies and procedures.

Accessibility. Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should let the instructor know and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible.

You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen, if at all possible, but there could be a significant wait due to scheduled appointments. Students who have accommodations are strongly encouraged to request, obtain and send these to their instructors through the AIM portal (https://www.clemson.edu/academics/studentaccess/register.html) as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester.

You can access further information at the Student Accessibility website (https://www.clemson.edu/academics/studentaccess/index.html), or at the university's Accessibility Portal (https://www.clemson.edu/accessibility/access/accommodations-services.html).

The Clemson University Title IX Statement Regarding Non-Discrimination. The Clemson University Title IX statement: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This Title IX policy is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX

Clemson University aspires to create a diverse community that welcomes people of different races, cultures, ages, genders, sexual orientation, religions, socioeconomic levels, political perspectives, abilities, opinions, values and experiences.

Emergency Preparation. Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees should be familiar with guidelines from the Clemson University Police Department. Visit here for information about safety.

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

1. Ensure you are signed up for emergency alerts
2. Download the Rave Guardian app to your phone (https://www.clemson.edu/cusafety/cupd/rave-guardian/)
3. Learn what you can do to prepare yourself in the event of an active threat (http://www.clemson.edu/cusafety/EmergencyManagement/)

Tentative Schedule

- Thursday, January 12: First class
- January 31-February 7: Asynchronous virtual classes
- February 24-25: Clemson's Math For All Conference
- Thursday, March 16: Virtual class (on Zoom)
- Friday, March 17: Last day to withdraw
- March 20-March 24: Spring Break!! (No class)
- Thursday, April 27: Last class
- Wednesday, May 3, 3-5:30pm: Final portfolio due, final day of presentations (on Zoom)

Note: This syllabus is subject to change based on the needs of the class.