Math Foundations of Cryptography 4950/6950 (Spring 2023)

Instructor: Dr. Ming Ming Tan
Email: mtan@augusta.edu

Course Description:

In this course, students will learn about basic number theory and abstract algebra necessary to understand the definitional details of modern number-theoretic encryption schemes. All of the mathematical developments in this course are directly motivated by cryptographic applications.

Learning Outcomes: After taking this course, you will

- Learn the fundamental concepts of number theory and abstract algebra needed for modern number-theoretic encryption schemes.
- Learn to derive properties/theorems needed for modern number-theoretic encryption schemes.
- Gain exposure to the modern number-theoretic encryption schemes and their underlying assumptions.
- Learn to formulate and understand the security properties given by the encryption schemes.

Meeting Venue/Time

M W	1430-1545	Hull McKnight GA Cyber Center 2201

Prerequisites

- CSCI 3400 - Data Structures with a grade of C or better

- CSCI 3030 - Mathematical Structures for Computer Science with a grade C or better
- MATH 3280 - Linear Algebra with a grade C or better

Textbook

- Cryptography: An Introduction (3rd Edition) by Nigel Smart.

Suggested Reference Books

- Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell
- An Introduction to Mathematical Cryptography by Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

Class

Class will be conducted in face-to-face mode. Whether a given class is provided face-to-face in a traditional classroom environment, or online via WebEx or TEAMs, you are expected to attend. I expect you to be in class. I recognize the need to miss classes due to unforeseen circumstances. Missing class will miss content. You will need to make an effort to keep current on the material.

Note The course delivery methodology may change at some point during the semester based on future CDC Georgia Department of Health guidelines. We may be forced to go temporarily or completely online to satisfy future health safety requirements. In the event this occurs, procedures outlined in the syllabus will be adjusted as necessary to accommodate the modified class environment.

Course Information and material

course webpage: https://mmtan.github.io/mathcrypto/
The course information posted on the course webpage will have the latest information and grading scheme. It will contain any updates or modifications. The posted schedule and grading scheme will have precedence and priority if there are any questions.
All the course material (such as homeworks) will be posted on the course webpage.

Sharing of Instructor-generated Materials

The policy prohibits students from posting instructor-generated materials on external sites. The selling, sharing, publishing, presenting, or distributing of instructor-prepared course lecture notes, videos, audio recordings, or any other

instructor-produced materials from any course for any commercial purpose is strictly prohibited unless explicit written permission is granted in advance by the course instructor. This includes posting any materials on websites such as Chegg, Course Hero, Discord, OneClass, Stuvia, StuDocu and other similar sites. Unauthorized sale or commercial distribution of such material is a violation of the instructor's intellectual property and the privacy rights of students attending the class and is prohibited.

Grading

Points are allotted for the following activities.

	Point distribution
Homework	50
Midterm (1hr)	25
Final. (1hr)	25

Course Grade Scale

Total Points Earned	Final Grade
90-100	A
80-89	B
70-79	C
60-69	D
Below 60	F

Tentative Semester Schedule by week/topic

> *The tentative schedule is subjected to changes throughout the semester. Depending on the progress of the course, we might have to adjust the number of topics.*

Week 1 (Jan 9)	Syllabus review and introduction to classical shift ciphers
Week 2 (Jan 16) (No class on Jan 16) Jan 18	Attacks on classical shift ciphers via frequency statistics
Week 3 (Aug 29)	Abstract group definition and basic properties
Week 4 (Jan 23)	GCDs and Isomorphism of groups
Week 5 (Jan 30)	Review of discrete probability theory
Week 6 (Feb 6)	The one time pad cryptosystems and various equivalent definitions of perfect secrecy
Week 7 (Feb 13)	Multiplicative group and Euler totient function
Week 8 (Feb 20)	Efficient algorithms for Euclidean gcd, modular exponentiation and finding inverse in Z/n*
Week 9 (Feb 27)	Midterm Exam
Week 10 (Mar 6)	Randomized primality testing
Week 11 (Mar 13)	RSA cryptosystem
Week 12 (Mar 20)	Prime number theorems and proving the security of RSA cryptosystem
Week 13 (Mar 27)	Quadratic residues and its applications in Rabin encryption scheme
Week 14 (Apr 3) (No class on Apr 3 and Apr 5)	Discrete log problem and its applications in digital signature schemes
Week 15 (Apr 10)	Finite fields
Week 16 (Apr 17)	Spring Break/Fall Pause
Week 17 (Apr 24)	Legendre interpolation and its applications in secure secret sharing
Week 18 (May 1) (No class on May 3)	Revision

Last Day of withdrawal: TBA
Final Exam : THURS MAY 11 2-4 PM

Homework and Exams

As listed above in the grading section, there will be homework. You can discuss the homework with your classmates. Depending on the size of the class, you might be asked to form a group of 1-3 students. You should turn in only one write-up for your entire group.
The homework will consist questions that require solving problems by writing concrete mathematics proof and writing small programming programs.
Questions in homework may be discussed during the tutorial sessions.
Exams are written exams. Students will be asked to solve problems similar to homework problems. The exams will be an open book exam. Printed materials, textbooks, and handwritten notes are allowed. Calculators are allowed . Phones, laptops, tablets , and other electronic devices are not allowed.

Missed Exams

No make-up exams will be allowed. In case of a documented excuse, the weight of the missed exam be placed onto the final's weight.

Academic Accommodations

Augusta University will make reasonable academic accommodations for students with documented disabilities. Students should contact Testing and Disability Services (Galloway Hall; 706.737.1469; www.augusta.edu/tds/) as soon as possible for more information and/or to initiate the process for accessing academic accommodations.
"Augusta University believes academically qualified individuals with disabilities should have equal opportunity and access to a quality education. We are actively involved in fostering an environment that encourages full participation by students with disabilities in every segment of the University.
The Office of Disability Services was established to help ensure an accessible and positive college experience for students with disabilities. Our Office [Testing and Disability Services] provides a variety of services and accommodations to meet the needs of disability related concerns in accordance with the Rehabilitation Act of 1973 as amended, the Americans with Disabilities Act of 1990, and Board of Regents' policies" https://www.augusta.edu/tds/disabilityservices.php

Distracting Behavior

Distracting behavior such as uninvited casual talk among students, use of cell phones, snoring, or inappropriate behavior toward fellow students or faculty will not be tolerated. Faculty have the right and the responsibility to maintain a classroom free of such distractions. Students who persist in such behavior may be asked to leave the class and may be counted absent for the session. Persistent disruptive behavior may result in forced withdrawal from the course.

Academic Honesty

In an academic community, honesty and integrity must prevail if the work done and the honors awarded are to receive their respect. The erosion of honesty is the academic community's ultimate loss. The responsibility for the practice and preservation of honesty must be equally assumed by all of its members. Any type of dishonesty in securing those credentials therefore invites serious sanctions, up to and including, a "WF" or "F" in the course, and expulsion from the institution. Please reference the http://catalog.augusta.edu/content.php?catoid=27&navoid=3332&hl=honesty&returnto=search#Academic_Honesty for further details and specific definitions of cheating and plagiarism.

"Augusta University ("AU") recognizes that academic honesty is essential to its academic function. The [AU academic honesty policy] following regulations protect the equity and validity of the University's grades and degrees, and help students develop ethical standards and attitudes appropriate to academic and professional life. Violations of academic honesty include, but are not limited to, cheating of all kinds, plagiarism, research misconduct, collusion, and false statements made to avoid negative academic consequences." - *from the AU Academic Honesty policy which can be found in the AU Policy Library at* https://www.augusta.edu/compliance/policyinfo/policies.php

Academic standards and procedures can also be found in the AU Student Manual (section 5 – 2018/19 Manual) - which can be found on the AU Student life website at https://www.augusta.edu/student-affairs/

In an academic community, honesty and integrity must prevail if the work done and the honors awarded are to receive their respect. The erosion of honesty is the academic community's ultimate loss. The responsibility for the practice and preservation of honesty must be equally assumed by all of its members. Any type of dishonesty in securing those credentials therefore invites serious sanctions, up to

and including, a “WF” or “F” in the course, and expulsion from the institution. Please reference the http://catalog.augusta.edu/content.php?catoid=27&navoid=3332&hl=honesty&returnto=search#Academic_Honesty for further details and specific definitions of cheating and plagiarism.

Unethical behavior of students in any form is not acceptable and will not be tolerated in the School for Computer and Cyber Sciences. Academic dishonesty – to include cheating on exams, plagiarism of the work of others, unapproved collaboration on graded work, and the like - will be dealt with immediately and with clear consequences. Depending on the nature and severity of the problem, a student who is guilty of any such violation may be: 1) withdrawn from the course with a grade of WF (counted as an F in the GPA); 2) given a grade of zero on the assignment; 3) given a grade of F in the course; or 4) otherwise penalized, at the discretion of the faculty member. Two occurrences of a WF grade for academic dishonesty can result in a student’s being expelled from the University, per current University policy as described in the University Catalog. - HCB Professional Behavior Guidelines

Library Resources

Augusta University has a designation as a Center of Academic Excellence in Cyber Defense Education. Please be aware that students and faculty have no-additional-fee access to subscription-based on-line CD journals, books, and other publications. The Library’s Cyber Resource Center is at http://guides.augusta.edu/friendly.php?s=cyber.

Campus Carry Law

House Bill 280, commonly known as the “campus carry” legislation, is effective as of July 1, 2017. Below is a link to the guidelines developed by the Office of Legal Affairs for the implementation of House Bill 280 that must be followed on all University System campuses. http://www.usg.edu/hb280