Math 587

Syllabus

▶ TABLE OF CONTENTS

Course Information

Course Name and Number

Introduction to Cryptography – CSCE 557/Math 587

Term

Fall 2024

Meeting Time and Location

Mondays, Wednesdays, and Fridays 9:40-10:30 AM in LeConte College Room 422

Instructor Information

- Instructor Name and Preferred Title: Prof. Matthew (Matt) Ballard
- Preferred pronouns: He/Him/His
- Office : LeConte College Room 341
- E-mail: ballard@math.sc.edu

Office Hours

Mondays 12-3 or by appointment

Academic Bulletin Description

Design of secret codes for secure communication, including encryption and integrity verification: ciphers, cryptographic hashing, and public key cryptosystems such as RSA. Mathematical principles underlying encryption. Code-breaking techniques. Cryptographic protocols.

Full Course Description

Since the advent of human communication, people have wanted to communicate privately. And others have wanted to listen in on those ostensibly private communication. Our modern situation where a large portion of our interactions occur online presents a special need for such security and an attractive target.

In this course, we cover the basics of cryptography starting from ciphers used in ancient times up to modern encryption and signature protocols. We focus on the mathematical foundations of both cryptography and cryptanalysis.

Prerequisites

C or better in CSCE 145 or MATH 241, and at least one of CSCE 355, MATH 300, or MATH 374.

Learning Outcomes

After successful completion of course, you will:

- Apply and attack polyalphabetic ciphers
- Explain the conceptual framework for different methods of encryption
- Obtain fluency in the underlying mathematics for common cryptosystems like Elgamal and RSA
- Be introduced to more advanced methods of cryptography like elliptic curve cryptography

Course Materials

The main resources for materials are the course website, the Microsoft Team for the course, and the Github organization.

The main text for this course is

- J. Hoffstein, J. Pipher, J. Silverman. An introduction to mathematical cryptography. A free electronic copy is available through USC libraries.

Some other texts that you might find useful/interesting:

- W. Stallings. Cryptography and network security. A previous choice for text.
- S. Singh. The code book. A popular history of cryptography and cryptanalysis through the ages.
- B. Schneier. Applied cryptography.

We will be using the Lean programming language and theorem prover as an integral part of this course. You will be introduced to Lean as the course progresses. No prior experience with Lean (or programming) is expected.

Some useful resources for becoming familiar with Lean:

- D. Thrane Christiansen. Functional programming in Lean. A good introduction to using Lean to write executable code.
- J. Avigad, L. de Moura, S. Kong and S. Ullrich, with contributions from the Lean Community Theorem Proving in Lean. The standard reference for learning how to use Lean as a theorem prover.
- The Lean Manual.

All course materials comply with copyright/fair use policies.

Course Requirements

Course Format

To wholly and successfully engage with the course, you will need to be need to attend class, attempt lots of problems, and engage both with me and your fellow classmates. All course materials are will be made available online so regular Internet access is essential for successful completion of the course.

It is expected that much of this material will be unfamiliar to you. (If not, more power to you.) The course is structured to guide every student to mastery in terms of conceptual understanding and computational fidelity by the end of the semester.

Class time will be spent working in small groups and presenting solutions to problems. It is expected you will have consumed the relevant material ahead of each course. It is not expected you will be comfortable with the material. Class time is for learning through doing and working through your misunderstandings.

Weekly short quizzes will help to diagnose any problems.

At the end of the class, a project will be due in place of a final exam.

Course Communication

I will be communicating with you regarding grades and assignments. If you need to get in touch with me, the best method is via Microsoft Team chat or email. Generally, I will reply within 24 hours and will provide feedback on assignments within one week.

You may also post questions pertaining to the course in the Questions channel in the course team. These questions will be answered within 24 hours. I encourage all students to take a stab at answering any question.

If you are having trouble with this course or its material, you should contact me via Microsoft Team chat or email to discuss the issues.

Announcements will be posted to this course whenever necessary. If there is any other information I think is important, I will send it to your preferred university email address. It is your responsibility to ensure that your email account works properly in order to receive email.

If you are unsure of your preferred email, check your account at myaccount.sc.edu. For more information on setting your preferred university email, please see the Knowledge Base Article How To Change Your Primary University Email Address.

Technology

To participate in learning activities and complete assignments, you will need:

- Access to a working computer that has a current operating system with updates installed with a modern web browser installed;
- Reliable Internet access and a USC email account;
- If you plan to submit handwritten assignments, a scanning device such as a smartphone with the Microsoft Office Lens app. Latex submissions are encouraged but not required.
- The main hub for this course communication is the Microsoft Teams team COTEAM-BALLARMR-MATH-587-001-FALL-2024 run through USC's Microsoft Teams account. To access the team for the first time on your desktop/laptop, you can use the join link including in your welcome email.

As part of the class, you will gain some familiarity with the version control system git, the git repository hosting platform Github, and the programming language Lean. No previous familiarity will be assumed.

Minimal Technical Skills Needed

Minimal technical skills are needed in this course. All work in this course must be completed and submitted online. Therefore, you must have consistent and reliable access to a computer and the Internet. The minimal technical skills you have include the ability to:

- Organize and save electronic files;
- Check and use the Microsoft Teams site daily;
- Download and upload documents;
- Locate and enter information with a browser.

Technical Support

If you have problems with your computer, technology, IT-related questions, support, including Microsoft Teams, please contact the Division of Information Technology (DoIT) Service Desk at (803) 777-1800 or submit an online request through the Self-Service Portal or visit the Carolina Tech Zone. The Service Desk is open Monday – Friday from 8:00 AM – 6:00 PM (Eastern Daylight Time). The Thomas Cooper Library at USC has computers for you to use in case you encounter computer issues/problems.

Course Assignments and Grading

Homework

Homework will need to be completed in groups of 5-6 that will be randomly assigned each week. The assignments will be available in and must be returned through Github Classroom. All homework assignments are due by 11:59 pm (Eastern Time) on the day indicated on the course schedule. Homework will be graded for correctness. You will be allowed up to two revisions on each homework assignment.

Quizzes

Each week will end with a short quiz. The goal of the quiz is to diagnose any gaps in the understanding and make sure we all stay on the same page. Quizzes are graded for correctness. You will be allowed up to two revisions on each quiz.

Presentations

All students are expected to regularly present solutions to in-class work group problems. Your target should be to present one solution every two weeks. Presentations are graded simply for completion. If you attempt it, it counts.

Project

A list of project topics will be released on October 3. These can be done in groups of 1-5 of your own choosing. Projects are due by December 7 at 11:30 am (EST).

Evaluation and Grading Scale

All grades will be posted on Teams. You are strongly encouraged to check you scores in Teams regularly. A final letter grade will be assigned based on the weighting below.

Assignment Weights

Component	Percent of total
Homework	25%
Quizzes	25%
Presentations	25%
Project	25%

Grading Scale

Final total intervals	Letter Grade
[90,100]	A
[85,90)	B+
[80,85)	B
[75,80)	C+
[70,75)	C

Final total intervals	Letter Grade
[65,70)	D+
[60,65)	D
[0,60)	F

Assignment Submission

All written assignments are required to be submitted through Github. If you choose to upload a scan, then

- the handwriting must be clear and legible – otherwise you will receive no credit
- you will need to use the Office 365 Lens app to scan and upload you work to your university OneDrive account before attaching to the assignment. No HEIC extensions are allowed.

Revisions

All homework turned in on-time is eligible for revision at full credit. All quizzes taken on-time are eligible for revision at full credit. Each assignment can undergo at most two revisions. Revisions must be resubmitted within one week of receiving a marked assignment or revision.

Academic Success

Accessibility

The Student Disability Resource Center (SDRC) empowers students to manage challenges and limitations imposed by disabilities. Students with disabilities are encouraged to contact me to discuss the logistics of any accommodations needed to fulfill course requirements (within the first week of the semester). In order to receive reasonable accommodations from me, you must be registered with the Student Disability Resource Center (1705 College Street Close-Hipp, Suite 102 Columbia, SC 29208, 803-777-6142). Any student with a documented disability should contact the SDRC to make arrangements for appropriate accommodations.

Student Success Center

In partnership with USC faculty, the Student Success Center (SSC) offers a number of programs to assist you in better understanding your course material and to aid you on your path to success. SSC programs are facilitated by professional staff, graduate students, and trained undergraduate peer leaders who have previously excelled in their courses. Resources available to you in this and other courses may include:

Peer Tutoring: You can make a one-on-one appointment with a Peer Tutor. Drop-in Tutoring and Online Tutoring may also be available for this course. Visit their website for a full schedule of times, locations, and courses.

Peer Writing: Improve your college-level writing skills by bringing writing assignments from any of your classes to a Peer Writing Tutor. Similar to Tutoring, you can visit the website to make an appointment, and to view the full schedule of available drop-in hours and locations.

Success Consultations: In Success Consultations, SSC staff assist you in developing study skills, setting goals, and connecting to a variety of campus resources. Throughout the semester, I may communicate with the SSC via Success Connect, an online referral system, regarding your progress in the course. If contacted by the SSC, please schedule a Success Consultation. Success Connect referrals are not punitive and any information shared by me is confidential and subject to FERPA regulations.

SSC services are offered to all USC undergraduates at no additional cost. You are invited to call the Student Success Hotline at (803) 777-1000, visit SSC website, or stop by the SSC in the Thomas Cooper Library on the Mezzanine Level to check schedules and make appointments.

Writing Center

This course has many writing assignments. The University Writing Center is an important resource you should use! It's open to help any USC student needing assistance with a writing project at any stage of development. The main Writing Center is in Byrnes 703.

University Library Resources

University Libraries has access to books, articles, subject specific resources, citation help, and more. If you are not sure where to start, please Ask a Librarian! Assistance is available at sc.edu/libraries/ask.

Remember that if you use anything that is not your own writing or media (quotes from books, articles, interviews, websites, movies – everything) you must cite the source in MLA (or other appropriate and approved) format.

Teams and Technology

Teams and Technology. As a student in this course, you have access to support from the Division of Information Technology (DoIT) for Teams and computer issues. The service desk can be reached at 803-777-1800.

Counseling Services

The University offers counseling and crisis services as well as outreach services and self-help.

Course Policies and Procedures

Attendance Policy

Unexcused Absences

In traditional lecture-based, in-person courses, students are allowed to miss 5% of the total class meeting time, regardless of the reason.

In general, this "5% rule" means that students won't be penalized for missing two sessions of a 50-minute MWF course or one session of a 75-minute TR course. Online, lab, clinical, practicum and certain other courses may allow fewer absences.

Example Reasons for Unexcused Absences

- Illness without a doctor's note
- Routine doctor's appointments
- Friend or family events such as weddings and vacations
- Car trouble
- Work obligations

Excused Absences

In certain cases, students who miss class will be given excused absences. Students won't be penalized for these absences, and they'll be offered the opportunity to make up missed work or complete an alternate assignment. Instructors may require make-up work to be completed within one week of returning to class.

Example Reasons for Excused Absences

- Military duty or jury duty
- Observance of a religious practice, holiday or holy day
- Illness or injury too severe or contagious to attend class, with appropriate documentation
- Death or severe illness of immediate family member, with appropriate documentation

Request an Excused Absence

Follow these steps to help us process your request as quickly as possible.

- Check whether your absence may be excused.
- Review the appropriate attendance policy — undergraduate or graduate — and the guidelines below to determine whether your absence may be excused and what type of documentation is required.
- Submit your complete request as soon as reasonably possible. Submit your complete request — including appropriate documentation — as soon as possible, but no later than 30 days following the absence, or by the last day of class for the semester, whichever is sooner. -For absences that are known at the beginning of the semester (such as religious holidays or authorized university activities), students should submit their requests no later than the second week of class.
- Requests for excused absences that occur during final exams should be submitted within 72 hours of the scheduled exam time.
- Be aware of possible exceptions.
- Instructors may refuse to give an excused absence or make-up work that would result in a fundamental alteration of the essential academic requirements of the course. In some of these cases, you may want to consider dropping a course. Undergraduate students can review information on the hardship withdrawal webpage. Graduate students should review their academic bulletin.

Academic Integrity

You are expected to practice the highest possible standards of academic integrity. Any deviation from this expectation will result in a minimum academic penalty of your failing the assignment, and will result in additional disciplinary measures. This includes improper citation of sources, using another student's work, and any other form of academic misrepresentation.

The first tenet of the Carolinian Creed is, "I will practice personal and academic integrity."

Below are some websites for you to visit to learn more about University policies:

- Carolinian Creed
- Academic Responsibility
- Office of Student Conduct and Academic Integrity
- Information Security Policy and Standards

Plagiarism

Using the words or ideas of another as if they were one's own is a serious form of academic dishonesty. If another person's complete sentence, syntax, key words, or the specific or unique ideas and information are used, one must give that person credit through proper citation. You should in particular cite any resources, person, text, or otherwise, you used to assist in preparation of your work. Copying proofs or problem solutions is strictly forbidden.

Use of Artificial Intelligence (AI) Tools and Citation

In this course, the use of Artificial Intelligence (AI) tools, such as ChatGPT, is governed by the University of South Carolina's academic integrity policies. Students are required to seek explicit permission from the instructor before using AI tools to complete assignments or any academic work. Unauthorized use of AI, especially without proper citation, may constitute a violation of the Honor Code, including offenses such as unauthorized aid, plagiarism, or falsification.

If AI is permitted for use, students must clearly distinguish between their original work and content generated by AI, ensuring that all AI contributions are properly cited. Failure to adhere to these guidelines may result in academic penalties. It is the student's responsibility to clarify any doubts about AI usage with the instructor in advance, as ignorance of these rules is not an acceptable defense.

Group Work

Group work should be performed in safe manner. Remote work will certainly form a larger component of a career going forward. You are encouraged to take advantage of Microsoft Teams video and chat abilities to aid in collaboration.

Class Conduct

Professionalism will be expected at all times, but most especially with your interactions online and in person. Because the university classroom is a place designed for the free exchange of ideas, we must

show respect for one another in all circumstances. We will show respect for one another by exhibiting patience and courtesy in our exchanges. Appropriate language and restraint from verbal attacks upon those whose perspectives differ from your own is a minimum requirement. Courtesy and kindness is the norm for those who participate in the class.

Mistakes, in particular during the running phase, are expected and natural. Mistakes are how learning happens. All students should recognize and respect the bravery of a student presenting a proof or solution. If you ever feel uncomfortable beyond the intellectual challenge of the course, please contact me.

Teams is a way for you to share your ideas and learning with your colleagues in this class. We do this as colleagues in learning, and the online space is meant to be a safe and respectful environment for us to conduct these discussions.

Some general netiquette rules:

- Treat one another with respect. It will be expected that we will not attack one another personally for holding different opinions.
- Do not use all CAPITAL LETTERS in emails or discussion board postings. This is considered “shouting” and is seen as impolite or aggressive.
- Begin emails with a proper salutation (Examples: Dr. Name; Ms. Name; Hello Professor Name; Good afternoon Mr. Name). Starting an email without a salutation or a simple “Hey” is not appropriate.
- When sending an email, please include a detailed subject line. Additionally, make sure you reference the course number (Ex. ENGL 287) in the message and sign the mail with your name.
- Use proper grammar, spelling, punctuation, and capitalization. Text messaging language is not acceptable.
- Use good taste when communicating. Profanity should be avoided.
- Re-Read, think, and edit your message before you click “Send/Submit/Post.”
- Please remember when posting to be respectful and courteous to your colleagues, and limit your communication to topics of this course and the assignments.

Late Work/Make-up Policy

All assignments due by the deadline as posted on the course schedule. Late work is not accepted and not eligible for revision.

Please plan accordingly, and complete these assignments in advance of their deadlines to ensure any unanticipated circumstances do not result in a missed assignment. User error does not qualify you for any kind of makeup or retake opportunity.

Completing and submitting the assignments by the due date is the sole responsibility of you. If you fail to submit the assignment or test by the due date, then your score for that assignment will be recorded as "zero."

You will be allowed to access the assignments an unlimited number of times until the due date/time. If you are concerned about missing a deadline, post your assignment the day before the deadline.

Be Careful: The clock on your computer may be different than the clock in Teams. If the clock is different by one second, you will be locked out of the assignment. Plan accordingly.

Incomplete Grades

The grade of Incomplete will be granted only in accordance with university policy.

Tolerance

The university is committed to a campus environment that is inclusive, safe, and respectful for all persons, and one that fully embraces the Carolinian Creed: "I will discourage bigotry, while striving to learn from differences in people, ideas and opinions." Likewise, the Student Code of Conduct stresses, "The University of South Carolina strives to maintain an educational community that fosters the development of students who are ethical, civil and responsible persons."

To that end, all course activities will be conducted in an atmosphere of friendly participation and interaction among colleagues, recognizing and appreciating the unique experiences, background, and point of view each student brings. You are expected at all times to apply the highest academic standards to this course and to treat others with dignity and respect.

Title IX and Gendered Identity

This course affirms equality and respect for all gendered identities and expressions. Please don't hesitate to correct me regarding your preferred gender pronoun and/or name if different from what is indicated on the official class roster. Likewise, I am committed to nurturing an environment free from discrimination and harassment. Consistent with Title IX policy, please be aware that I as a

responsible employee am obligated to report information that you provide to me about a situation involving sexual harassment or assault.

Expectations of the Instructor

I am expected to facilitate learning, answer questions appropriately, be fair and objective in grading, provide timely and useful feedback on assignments and treat you as I would like to be treated.

Copyright/Fair Use Statement

I will cite and/or reference any materials that I use in this course that I do not create.

Anything that appears on this website is copyright © 2024 Matthew Ballard and is distributed by an MIT license.

Course materials that do not appear on this website are copyright © 2024 Matthew Ballard and all rights are reserved. In particular, you may not distribute any of these course materials in any fashion.

Tentative Schedule

This is the (ambitious) plan for the semester. But it is only a plan. The successful progression of each student is the most important guide to through the material. As such, you should expect revisions as we go.

Week 1

- **Wed 08/21**: Introducing the course and ourselves
- **Fri 08/23**: Substitution and transposition ciphers

Week 2

- **Mon 08/26**: Frequency analysis
- **Wed 08/28**: Evolution of cryptography
- **Fri 08/30**: Division algorithm

Week 3

- **Mon 09/02 (Labor Day - No Classes)**

- **Wed 09/04**: Euclidean algorithm
- **Fri 09/06**: Modular arithmetic

Week 4

- **Mon 09/09**: Prime factorization and finite fields
- **Wed 09/11**: Powers and primitive roots in finite fields
- **Fri 09/13**: The discrete logarithm problem

Week 5

- **Mon 09/16**: Order notation
- **Wed 09/18**: Symmetric and asymmetric ciphers
- **Fri 09/20**: Diffie-Hellman key exchange

Week 6

- **Mon 09/23**: Elgamal public key cryptosystem
- **Wed 09/25**: Shanks Babystep-Giantstep algorithm
- **Fri 09/27**: Chinese remainder theorem

Week 7

- **Mon 09/30**: Pohlig-Hellman algorithm
- **Wed 10/02**: Roots modulo a product of two primes
- **Fri 10/04**: RSA public key cryptosystem

Week 8

- **Mon 10/07**: Finding large primes
- **Wed 10/09**: Lots of primes (probably)
- **Fri 10/11**: Pollard's (p-1) factorization

Week 9

- **Mon 10/14**: Factorizations using differences of squares
- **Wed 10/16 (Fall Break - No Classes)**

- **Fri 10/18 (Fall Break - No Classes)**

Week 10

- **Mon 10/21**: Smooth numbers and the quadratic sieve
- **Wed 10/23**: The number field sieve
- **Fri 10/25**: The index calculus method

Week 11

- **Mon 10/28**: Quadratic residues
- **Wed 10/30**: Adding points on elliptic curves
- **Fri 11/01**: Elliptic curves over finite fields

Week 12

- **Mon 11/04**: Discrete logarithms on elliptic curves
- **Wed 11/06**: Fast powering for and complexity of ECDLP
- **Fri 11/08**: Elliptic curve Diffie-Hellman

Week 13

- **Mon 11/11**: Elliptic curve ElGamal
- **Wed 11/13**: Elliptic curve digital signatures
- **Fri 11/15**: Lenstra's factorization algorithm

Week 14

- **Mon 11/18**: Elliptic curves in characteristic 2
- **Wed 11/20**: Torsion points and divisors
- **Fri 11/22**: A little history of public key cryptography

Week 15

- **Mon 11/25 (Thanksgiving Break - No Classes)**
- **Wed 11/27 (Thanksgiving Break - No Classes)**
- **Fri 11/29 (Thanksgiving Break - No Classes)**

Week 16

- **Mon 12/02**: The Weil pairing
- **Wed 12/04**: Computing the Weil pairing
- **Fri 12/06**: The Tate pairing

Final Project

- **Wed 12/11 (Final Project Due)**

About this webpage. Copyright © 2024 Matthew Ballard. Distributed with an MIT license.