CS 4823/5823 CRYPTOGRAPHY
SPRING 2025

Instructor: Qi Cheng (qcheng@ou.edu, DEH 254)

Class time and location: Location: Sarkeys Energy Ctr (SEC M0207) 10:30 AM - 11:45 AM (TR)

Office hours: TW 3-4:30 Zoom and/or in-person.

Topics: In this course, we cover the following topics:

- Basics of computational number theory, including Extended Euclidean algorithm, Fermat Little Theorem, repeated squaring algorithm, Chinese Remainder Theorem and finite fields. (6 weeks)
- Symmetric/Asymmetric encryption, and digital signature, including AES and RSA. (5 weeks)
- The lattice-based cryptography (4 weeks).

Students who enroll in CS5823 are required to complete a project on lattice-based cryptosystems. We take an algorithmic approach when introducing abstract mathematical objects. We will use computer algebra systems, e.g. SAGE (http://www.sagemath.org) extensively in the class and in the homeworks.

Required book: Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography, Second Edition, Springer-Verlag.

References: Johannes A. Buchmann, Introduction to Cryptography, Springer-Verlag, Second Edition.

A. Menezes, P.C. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC press. (On-line version and errata are at http://www.cacr.math.uwaterloo.ca/hac/)

Grading: Attendance (10%), assignments(25%), one midterm exam (20%), one programming project (15%) and final (30%). The CS4823 students will be excused from the project. One homework of your choice can be turned in after its due time without penalty. No other late homework will be accepted. Attendance will be taken at 10 class meetings, selected by the instructor. Your attendence score is determined by

Number of sign-in	score
9-10	10
$2 \leq n \leq 8$	n
0-1	Your course grade is F or AW

University Policies

Masking Policy for In-Person Classes Masking is welcome on the OU Norman campus. People may choose to mask at any time or for any purpose.

Academic Integrity Student's Guide to Academic Integrity can be found at `http://integrity.ou.edu/students_guide.html`

Religious Observance It is the policy of the University to excuse the absences of students that result from religious observances and to reschedule examinations and additional required classwork that may fall on religious holidays, without penalty.

Reasonable Accommodation Policy Students requiring academic accommodation should contact the Disability Resource Center for assistance at (405) 325-3852 or TDD: (405) 325-4173. For more information please see the Disability Resource Center website `http://www.ou.edu/drc/home.html`. Any student in this course who has a disability that may prevent him or her from fully demonstrating his or her abilities should contact me personally as soon as possible so we can discuss accommodations necessary to ensure full participation and facilitate your educational opportunities.

Adjustments for Pregnancy/Childbirth Related Issues Should you need modifications or adjustments to your course requirements because of documented pregnancy-related or childbirth-related issues, please contact me as soon as possible to discuss. Generally, modifications will be made where medically necessary and similar in scope to accommodations based on temporary disability. Please see `www.ou.edu/content/eoo/faqs/pregnancy-faqs.html` for commonly asked questions.

Title IX Resources For any concerns regarding gender-based discrimination, sexual harassment, sexual misconduct, stalking, or intimate partner violence, the University offers a variety of resources, including advocates on-call 24.7, counseling services, mutual no contact orders, scheduling adjustments and disciplinary sanctions against the perpetrator. Please contact the Institutional Equity Office 405-325-3546 (8-5, M-F) or OU Advocates 405-615-0013 (24.7) to learn more or to report an incident.

Final Exam Preparation Period Pre-finals week will be defined as the seven calendar days before the first day of finals. Faculty may cover new course material throughout this week. For specific provisions of the policy please refer to OU's Final Exam Preparation Period policy (`https://apps.hr.ou.edu/FacultyHandbook#4.10`).

Emergency Protocol During an emergency, there are official university procedures that will maximize your safety.

Severe Weather: If you receive an OU Alert to seek refuge or hear a tornado siren that signals severe weather 1. LOOK for severe weather refuge location maps located inside most OU buildings near the entrances 2. SEEK refuge inside a building. Do not leave one building to seek shelter in another building that you deem safer. If outside, get into the nearest building. 3. GO to the building's severe weather refuge location. If you do not know where that is, go to the lowest level possible and seek refuge in an innermost room. Avoid outside doors and windows. 4. GET IN, GET DOWN, COVER UP. 5. WAIT for official notice to resume normal activities.

Armed Subject/Campus Intruder: If you receive an OU Alert to shelter-in-place due to an active shooter or armed intruder situation or you hear what you perceive to be gunshots: 1. GET OUT: If you believe you can get out of the area WITHOUT encountering the armed individual, move quickly towards the nearest building exit, move away from the building, and call

911. 2. HIDE OUT: If you cannot flee, move to an area that can be locked or barricaded, turn off lights, silence devices, spread out, and formulate a plan of attack if the shooter enters the room. 3. TAKE OUT: As a last resort fight to defend yourself. For more information, visit http://www.ou.edu/emergencypreparedness.html

Fire Alarm/General Emergency: If you receive an OU Alert that there is danger inside or near the building, or the fire alarm inside the building activates: 1. LEAVE the building. Do not use the elevators. 2. KNOW at least two building exits 3. ASSIST those that may need help 4. PROCEED to the emergency assembly area 5 ONCE safely outside, NOTIFY first responders of anyone that may still be inside building due to mobility issues. 6. WAIT for official notice before attempting to re-enter the building.