CS 4823/5823 CRYPTOGRAPHY
SPRING 2021

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

Class time and location: Zoom and Rawls Engr Practice Facility (REPF 0200) 11:00 AM - 11:50 AM (MWF).

Office hours: MW 2:30-4

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: For 4823 students: Attendance (10%), assignments (30%), one midterm exam (20%) and final (40%). For 5823 students: Attendance (10%), assignments(25%), one midterm exam (15%), one programming project (10%) and final (40%). One homework of your choice can be turned in after its due time, for which you can earn up to 90% of credit. 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 As outlined by the University of Oklahoma[1]s Chief COVID Officer, until further notice, employees, students, and visitors of the OU community will be mandated to wear masks (1.) when they are inside University facilities and vehicles and (2.) when they are outdoors on campus and social distancing of at least six feet is not possible. For the well-being of the entire university community it is important that everyone demonstrate the appropriate health and safety behaviors outlined in the University Mandatory Masking Policy (`https://www.ou.edu/coronavirus/masking-policy`). As this mandate includes all campus classrooms, please make sure you are wearing your mask while in class. If you do not have a mask or forgot yours, see the professor for available masks. If you have an exemption from the Mandatory Masking Policy, please see the professor to make accommodations before class begins. If and where possible, please make your professor aware of your exemption and/or accommodation prior to arriving in class.

If a student is unable or unwilling to wear a mask and has not made an accommodation request through the ADRC, they will be instructed to exit the classroom.

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.

Title IX Resources and Reporting Requirement For any concerns regarding gender-based discrimination, sexual harassment, sexual assault, dating/domestic violence, or stalking, the University offers a variety of resources. To learn more or to report an incident, please contact the Sexual Misconduct Office at 405/325-2215 (8 to 5, M-F) or smo@ou.edu. Incidents can also be reported confidentially to OU Advocates at 405/615-0013 (phones are answered 24 hours a day, 7 days a week). Also, please be advised that a professor/GA/TA is required to report instances of sexual harassment, sexual assault, or discrimination to the Sexual Misconduct Office. Inquiries regarding non-discrimination policies may be directed to: Bobby J. Mason, University Equal Opportunity Officer and Title IX Coordinator at 405/325-3546 or bjm@ou.edu. For more information, visit `http://www.ou.edu/eoo.html`.

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 your professor or the Disability Resource Center at 405/325-3852 as soon as possible. Also, see `http://www.ou.edu/eoo/faqs/pregnancy-faqs.html` for answers to commonly asked questions.

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.