CS 4823/5823 CRYPTOGRAPHY
SPRING 2026

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

Class time and location: TR 12 - 1:15 pm Sarkeys Energy Ctr M0207

Office hours: T Th 2-3:30

Prerequisite: CS 3823 and CS 4413.

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

- Week 1: Introduction and Bit complexity of large number arithmetic
- Week 2: Extended Euclidean Algorithm
- Week 3: Modular arithmetic
- Week 4: Fermat Little Theorem and Repeated squaring algorithm
- Week 5: Chinese Remainder Theorem
- Week 6: Polynomials over Finite Fields
- Week 7: Review and Midterm
- Week 8: Symmetric Cipher
- Week 9: Advanced Encryption Standard
- Week 10: Asymmetric cipher and Merkle-Hellman
- Week 11: Lattices
- Week 12: The NTRU cryptosystem and the graduate project
- Week 13: The RSA cryptosystem
- Week 14: Hash and signature
- Week 15: Review and Final

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

AI policy You are allowed to use AI LLM as an study aid. Please be warned that while the current popular AI models can be helpful sometimes, they often give misleading information. You should not copy text from LLM and paste into your homework, even with some modification. You can not access AI models during online quizzes and exams.

Academic Integrity and Plagiarism

The overall goal of this course is your learning. In order to demonstrate that you have reached this goal, the work you turn in needs to be your own. This includes putting written work into your own words and citing your sources, as appropriate to avoid plagiarism. If you work in a group, seek assistance from a tutor, use a resource on campus, and/or use online resources (including AI software), the work you turn in must be your own, demonstrating your own understanding of the material that you have gained through the learning process. If you have questions about academic integrity or plagiarism, please ask: my aim is to foster an environment where you can learn and grow, while also maintaining academic honesty and a clear representation of your learning and ideas. Penalties for serious offenses include a zero on the assignment and egregious offenses can even result in expulsion from the university, so it is important to understand expectations. Plagiarism as defined by the OU Integrity Office includes:

- Copying words and presenting them as your own writing.
- Copying words, even if you give the source, unless you also indicate that the copied words are a direct quotation
- Copying words and then changing them a little, even if you give the source.
- Even if you express it in your own words, it is plagiarism to use someone else's idea as your own.

Visit the OU Integrity Office for more information on what constitutes plagiarism.

University Policies

Mental Health Support Services

Support is available for any student experiencing mental health issues that are impacting their academic success. Students can either been seen at the University Counseling Center (UCC) located on the second floor of Goddard Health Center or receive 24/7/365 crisis support from a licensed mental health provider through TimelyCare. To schedule an appointment or receive more information about mental health resources at OU please call the UCC at 405-325-2911 or visit

University Counseling Center. The UCC is located at 620 Elm Ave., Room 201, Norman, OK 73019.

Title IX Resources and Reporting Requirement

The University of Oklahoma faculty are committed to creating a safe learning environment for all members of our community, free from gender and sex-based discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking, in accordance with Title IX. There are resources available to those impacted, including: speaking with someone confidentially about your options, medical attention, counseling, reporting, academic support, and safety plans. If you have (or someone you know has) experienced any form of sex or gender-based discrimination or violence and wish to speak with someone confidentially, please contact OU Advocates (available 24/7 at 405-615-0013) or University Counseling Center (M-F 8 a.m. to 5 p.m. at 405-325-2911).

Because the University of Oklahoma is committed to the safety of you and other students, and because of our Title IX obligations, I, as well as other faculty, Graduate Assistants, and Teaching Assistants, are mandatory reporters. This means that we are obligated to report gender-based violence that has been disclosed to us to the Institutional Equity Office. This means that we are obligated to report gender-based violence that has been disclosed to us to the Institutional Equity Office. This includes disclosures that occur in: class discussion, writing assignments, discussion boards, emails and during Student/Office Hours. You may also choose to report directly to the Institutional Equity Office. After a report is filed, the Title IX Coordinator will reach out to provide resources, support, and information and the reported information will remain private. For more information regarding the University's Title IX Grievance procedures, reporting, or support measures, please visit Institutional Equity Office at 405-325-3546.

Adjustments for Pregnancy and Related Issues

Should you need modifications or adjustments to your course requirements because of pregnancy or a pregnancy-related condition, please request modifications via the Institutional Equity Office website or call the Institutional Equity Office at 405/325-3546 as soon as possible. Also, see the Institutional Equity Office FAQ on Pregnant and Parenting Students' Rights for answers to commonly asked questions.

Reasonable Accommodation Policy

The University of Oklahoma (OU) is committed to the goal of achieving equal educational opportunity and full educational participation for students with disabilities. If you have already established reasonable accommodations with the Accessibility and Disability Resource Center (ADRC), please submit your semester accommodation request through the ADRC as soon as possible and contact me privately, so that we have adequate time to arrange your approved academic accommodations.

If you have not yet established services through ADRC, but have a documented disability and require accommodations, please complete ADRC's pre-registration form to begin the registration process. ADRC facilitates the interactive process that establishes reasonable accommodations for students at OU. For more information on ADRC registration procedures, please review their Register with the ADRC web page. You may also contact them at (405)325-3852 or adrc@ou.edu, or visit www.ou.edu/adrc for more information.

Note: disabilities may include, but are not limited to, mental health, chronic health, physical, vision, hearing, learning and attention disabilities, pregnancy-related. ADRC can also support students experiencing temporary medical conditions.

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. [See Faculty Handbook 3.15.2]

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.

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.

Additional Weather Safety Information is available through the Department of Campus Safety.

The University of Oklahoma Active Threat Guidance

The University of Oklahoma embraces a Run, Hide, Fight strategy for active threats on campus. This strategy is well known, widely accepted, and proven to save lives. To receive emergency campus alerts, be sure to update your contact information and preferences in the account settings section at one.ou.edu.

RUN: Running away from the threat is usually the best option. If it is safe to run, run as far away from the threat as possible. Call 911 when you are in a safe location and let them know from which OU campus you're calling from and location of active threat.

HIDE: If running is not practical, the next best option is to hide. Lock and barricade all doors; turn of all lights; turn down your phone's volume; search for improvised weapons; hide behind solid objects and walls; and hide yourself completely and stay quiet. Remain in place until law enforcement arrives. Be patient and remain hidden.

FIGHT: If you are unable to run or hide, the last best option is to fight. Have one or more improvised weapons with you and be prepared to attack. Attack them when they are least expecting it and hit them where it hurts most: the face (specifically eyes, nose, and ears), the throat, the diaphragm (solar plexus), and the groin.

Please save OUPD's contact information in your phone.

NORMAN campus: For non-emergencies call (405) 325-1717. For emergencies call (405) 325-1911 or dial 911.

TULSA campus: For non-emergencies call (918) 660-3900. For emergencies call (918) 660-3333 or dial 911.

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.

Video: OU Fire Safety on Campus