CSCE 4050 Applications of Cryptography (Spring 2026)

Instructor: Kirill Morozov, Department of Computer Science and Engineering
Office: F283, Email: Kirill.Morozov@unt.edu, Tel.: 940-565-2268

Class Day/Time/Venue: Thursdays, 5:30-8:20pm, NTDP B185

Course description: This course aims at introducing fundamentals of cryptography and their applications. The knowledge gained from this course will enable students to apply cryptographic algorithms as building blocks for designing secure solutions.

Learning objectives:

- Understand core cryptographic principles and security goals.
- Analyze and apply symmetric and public-key cryptographic primitives.
- Analyze and apply mechanisms for data integrity and authentication.
- Reason about and apply real-world cryptographic systems and protocols.

Office hours: The office hours are offered by both the instructor and the teaching assistants (TA) to address students' questions and concerns and to provide additional guidance on the course assignments. Additional office hours, in person and virtually, may be offered upon request.

Recommended literature:

- N. Ferguson, B. Schneier, and T. Kohno: "Cryptography Engineering: Design Principles and Practical Applications", Wiley, 2010.

[Supplementary reading]:

- D. Boneh and V. Shoup: "A Graduate Course in Applied Cryptography". Available online at: http://toc.cryptobook.us/
- M. Rosulek: "The Joy of Cryptography", Sample chapters available online at: https://joyofcryptography.com/
- D.R. Stinson, M. Paterson: "Cryptography: Theory and Practice", 4th Edition, CRC Press, 2018.
- J. Katz and Y. Lindell: "Introduction to Modern Cryptography" (2nd Edition), Chapman & Hall/CRC, 2015.

Technology Requirements: This course has digital components. To fully participate in this class, students will need internet access to reference content on the Canvas Learning Management System, Oracle VirtualBox software, and the programming language environment of the student's choice (Python is recommended). If circumstances change, the students will be informed of other technical needs to access course content. Information on how to be successful in a digital learning environment can be found at Learn Anywhere (https://online.unt.edu/learn).

Course schedule:

Lecture 1 (Jan 15): Course overview, historical ciphers, mathematical background

Lecture 2 (Jan 22): One-time pad

Lecture 3 (Jan 29): Pseudorandom generators and stream ciphers

Lecture 4 (Feb 5): Block ciphers

Lecture 5 (Feb 12): Cryptographic hash functions

Lecture 6 (Feb 19): Message authentication codes

Lecture 7 (Feb 26): Authenticated encryption

---------- (Mar 5): **Midterm Exam** (1st half)
Project Overview (2nd half)
---------- (Mar 12): **Spring Break (no class)**
Lecture 8 (Mar 19): Public-key encryption
Lecture 10 (Mar 26): Digital signatures
Lecture 11 (Apr 2): Public-key infrastructure and other applications
Lecture 12 (Apr 9): Authenticated key exchange and TLS
Lecture 13 (Apr 16): Identification and secure login. Kerberos
Lecture 14 (Apr 23): Post-quantum cryptography. Homomorphic encryption
Lecture 15 (Apr 30): Advanced cryptographic functionalities. Course review
---------- (May 2): **Final Exam**

Note: The course schedule is subject to change if the classes are impacted by the campus closing. The students will be notified of the latter by Eagle Alert according to the Campus Closures Policy (https://policy.unt.edu/policy/15-006).

Assignments: The course includes 8 homework assignments, 2 labs, one project, the midterm exam, and the final exam. The number of assignments may be changed at the instructor's discretion. Additional makeup assignments may be offered throughout the semester at the instructor's discretion.

Late submission policy: Assignments may be submitted up to 3 days late, with a penalty of 15% for each day. No credit will be given after 3 days. This policy may be changed at the instructor's discretion.

Grading Policies:

Grading Scale:
A = 90-100
B = 80-89
C = 70-79
D = 60-69
F = 0-59

Course Grade Composition:
Homeworks: 30%
Labs: 10%
Programming project: 15%
Mid-term exam: 20%
Final exam: 25%

Attendance and Participation: Attendance is not mandatory, and it does not contribute to the course grade. Attendance will only be taken during the first few classes to verify enrollment. Students are generally expected to attend every class unless an absence is excused. Research shows that students who attend class are more likely to be successful.

Academic Integrity: Cheating in exams/assignments, plagiarism in exams/assignments, collusion, and falsification of academic records constitute academic dishonesty. Sabotage means acting to prevent others from completing their work or willfully disrupting the academic work of others.
Students are responsible for being familiar with UNT's Student Academic Integrity Policy: https://policy.unt.edu/policy/06-003. Cheating/collusion/plagiarism in assignments/exams will result in

zero credit for them, a possible "F" grade for the course, and possible disciplinary action. Sabotage will result in removal from the classroom and possible disciplinary action.

Honor Code: "I commit myself to honor, integrity, and responsibility as a student representing the University of North Texas community. I understand and pledge to uphold academic integrity as set forth by UNT Student Academic Integrity Policy, 06.003 (https://policy.unt.edu/policy/06-003). I affirm that the work I submit will always be my own, and the support I provide and receive will always be honorable."

Policy on GenAI Use: In this course, the students are encouraged to use Generative AI (GenAI) tools such as ChatGPT, Gemini, Copilot, and others to support their learning and develop skills for a GenAI-oriented workforce. This use will help them stay technically proficient and ethically grounded. However, GenAI should complement, not replace, our course materials. The instructor may use GenAI to enhance materials, streamline assignments, draft syllabi, and perform other tasks. The instructor will always disclose the use of GenAI, and the same is expected from the students. In line with the UNT Honor Code, all work you submit must be your own. Using GenAI tools without proper attribution or submitting GenAI-generated output verbatim violates academic integrity and will be addressed in accordance with course policy.

ADA Accommodations: UNT makes reasonable accommodations for students with disabilities. To request accommodations, you must first register with the Office of Disability Access (ODA) by completing an application for services and providing documentation to verify your eligibility each semester. Once your eligibility is confirmed, you may request your letter of accommodation. ODA will then email your faculty a letter of reasonable accommodation, initiating a private discussion about your specific needs in the course. You can request accommodations at any time, but it is important to provide ODA notice to your faculty as early as possible in the semester to avoid delays in implementation. Keep in mind that you must obtain a new letter of accommodation for each semester and meet with each faculty member before accommodations can be implemented in each class. You are strongly encouraged to meet with faculty regarding your accommodations during office hours or by appointment. Faculty have the authority to ask you to discuss your letter during their designated office hours to protect your privacy. For more information and to access resources that can support your needs, refer to the ODA website (https://studentaffairs.unt.edu/office-disability-access).

Academic Success Resources: UNT offers a range of mental health and wellness services to help maintain balance and well-being. Utilizing these resources is a proactive way to support your academic and personal success. To explore campus resources designed to support you, check out mental health services (https://clear.unt.edu/student-support-services-policies), visit unt.edu/success, and explore unt.edu/wellness. To get all your enrollment and student financial-related questions answered, go to scrappysays.unt.edu.