[1]

Course Name: Cryptography
Course Number: CS 427 **Credits:** 4 **Instructor name:** Maher Elshakankiri
Instructor email: Maher.Elshakankiri@oregonstate.edu

Course Description

Introduction to the theory and practice of modern cryptography. Fundamental primitives including pseudorandom generators, block ciphers, hash functions. Symmetric-key cryptography for privacy and authenticity. Public-key cryptography based on number theoretic problems.

Prerequisites: CS 261 with C or better or MTH 355 with C or better

Friendly Description

There are two main goals for this course:

1. You will learn the fundamental concepts of provable security. What does it mean for something to be [in]secure? How can we formalize what it means to be secure? How can we mathematically prove things about security? How can security definitions tell us whether we are using a component in a safe way?
2. You will understand the most fundamental cryptographic building blocks, especially regarding the different security guarantees that they do[not] provide. We will focus on the building blocks that comprise 95% of the cryptography used in the real-world today.

Communication

If you have a question whose answer may benefit other students (e.g., clarifications of homework problems), please consider asking in the designated Q&A Discussion. Weekly office hours will also be held on Teams (schedule to be announced). For any other questions, email is the preferred method (Maher.Elshakankiri@eecs.oregonstate.edu).

Course Credits

Students will be expected to spend about 12 hours a week (15 hours in summer term) on the course for a total of 120 hours of instruction, activities, and assignments for 4 credits.

Technical Assistance

If you experience any errors or problems while in your online course, contact 24-7 Canvas Support through the Help link within Canvas. If you experience computer difficulties, need help downloading a browser or plug-in, or need assistance logging into a course, contact the

[1] a

IS Service Desk for assistance. You can call (541) 737-8787 or visit the IS Service Desk online.

Learning Resources

Textbook: *The Joy of Cryptography*: http://joyofcryptography.com

Note to prospective students: Please check with the OSU Beaver Store for up-to-date information for the term you enroll (OSU Beaver Store Website or 800-595-0357). If you purchase course materials from other sources, be very careful to obtain the correct ISBN.

Measurable Student Learning Outcomes

After successful completion of this course, students will be able to:

- Demonstrate understanding of provable security concepts
- Judge the security of cryptographic constructions by giving a security proof or attack
- Choose appropriate cryptographic primitives for different applications, and justify their choice.
- Identify inappropriate uses of cryptography and suggest appropriate alternatives.

Evaluation of Student Performance

The above Student Learning Outcomes will be measured through the following:

- Canvas Discussions – 10%
- Self-test Quizzes - 10%
- Problem Sets - 40%
- Exams - 40% (20% each)
- **Total - 100%**

Letter Grade

Grade	Percent Range
A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66

D-	60-62
F	Less than 60

Course Content

Module	Topic	Reading Assignments	Learning Activities
1	Unconditional Security • One-time pad • Secret sharing • Provable security fundamentals	Textbook: Chapters 1-2 Textbook: Chapters 2-3	Reading discussions Self-test quizzes Written homework Practice problems
2	Symmetric-Key Primitives • Pseudorandom generators • Pseudorandom functions • Block ciphers	Textbook: Chapters 4-5 Textbook: Chapters 5-6	Reading discussions Self-test quizzes Written homework Practice problems
3	Symmetric-Key Encryption • Security against chosen plaintext attacks • Block cipher modes • Security against chosen ciphertext attacks	Textbook: Chapters 7-8 Textbook: Chapters 8-9	Reading discussions Self-test quizzes Written homework Practice problems Midterm exam
4	Symmetric-Key Authentication • Message authentication codes • Hash functions • Authenticated encryption	Textbook: Chapters 10-11 Textbook: Chapters 11-12	Reading discussions Self-test quizzes Written homework Practice problems
5	Public-Key Cryptography	Textbook: Chapters 13-14	Reading discussions Self-test quizzes Written homework

	• Key agreement • Public-key encryption • Digital signatures	Textbook: Chapters 14-15	Practice problems Final exam
	Finals		

Course Policies

Discussion Participation

Students are expected to participate in all graded discussions. While there is great flexibility in online courses, this is not a self-paced course. You will need to participate in discussions according to their given deadlines.

Late Work Policy

Late work is not accepted, except by prior arrangement, or in case of emergency.

Incompletes

Incomplete (I) grades will be granted only in exceptional circumstances and at the discretion of the instructor. If you are having any difficulty that might prevent you completing the coursework, please don't wait until the end of the term; let me know right away.

Statement Regarding Religious Accommodation

Oregon State University is required to provide reasonable accommodations for employee and student sincerely held religious beliefs. It is incumbent on the student making the request to make the faculty member aware of the request as soon as possible prior to the need for the accommodation. See the Religious Accommodation Process for Students.

Guidelines for a Productive and Effective Online Classroom

Students are expected to conduct themselves in the course (e.g., on discussion boards, email) in compliance with the university's regulations regarding civility. Civility is an essential ingredient for academic discourse. All communications for this course should be conducted constructively, civilly, and respectfully. Differences in beliefs, opinions, and approaches are to be expected. In all you say and do for this course, be professional. Please bring any communications you believe to be in violation of this class policy to the attention of your instructor.

Active interaction with peers and your instructor is essential to success in this online course, paying particular attention to the following:

- Unless indicated otherwise, please complete the readings and view other instructional materials for each week before participating in the discussion board.
- Read your posts carefully before submitting them.
- Be respectful of others and their opinions, valuing diversity in backgrounds, abilities, and experiences.

- Challenging the ideas held by others is an integral aspect of critical thinking and the academic process. Please word your responses carefully, and recognize that others are expected to challenge your ideas. A positive atmosphere of healthy debate is encouraged.

Expectations for Student Conduct

Student conduct is governed by the university's policies, as explained in the Student Conduct Code. Students are expected to conduct themselves in the course (e.g., on discussion boards, email postings) in compliance with the university's regulations regarding civility.

Academic Integrity

Students are expected to comply with all regulations pertaining to academic honesty. For further information, visit Student Conduct and Community Standards, or contact the office of Student Conduct and Mediation at 541-737-3656.

OAR 576-015-0020 (2) Academic or Scholarly Dishonesty:

a) Academic or Scholarly Dishonesty is defined as an act of deception in which a Student seeks to claim credit for the work or effort of another person, or uses unauthorized materials or fabricated information in any academic work or research, either through the Student's own efforts or the efforts of another.
b) It includes:
   i) CHEATING - use or attempted use of unauthorized materials, information or study aids, or an act of deceit by which a Student attempts to misrepresent mastery of academic effort or information. This includes but is not limited to unauthorized copying or collaboration on a test or assignment, using prohibited materials and texts, any misuse of an electronic device, or using any deceptive means to gain academic credit.
   ii) FABRICATION - falsification or invention of any information including but not limited to falsifying research, inventing or exaggerating data, or listing incorrect or fictitious references.
   iii) ASSISTING - helping another commit an act of academic dishonesty. This includes but is not limited to paying or bribing someone to acquire a test or assignment, changing someone's grades or academic records, taking a test/doing an assignment for someone else by any means, including misuse of an electronic device. It is a violation of Oregon state law to create and offer to sell part or all of an educational assignment to another person (ORS 165.114).
   iv) TAMPERING - altering or interfering with evaluation instruments or documents. v) PLAGIARISM - representing the words or ideas of another person or presenting someone else's words, ideas, artistry or data as one's own, or using one's own previously submitted work. Plagiarism includes but is not limited to copying another person's work (including unpublished material) without appropriate referencing, presenting someone else's opinions and theories as one's own, or working jointly on a project and then submitting it as one's own.

c) Academic Dishonesty cases are handled initially by the academic units, following the process outlined in the University's Academic Dishonesty Report Form, and will also be referred to SCCS for action under these rules.

Establishing a Positive Community:
It is important you feel safe and welcome in this course. If somebody is making discriminatory comments against you, sexually harassing you, or excluding you in other ways, contact the instructor, your academic advisor, and/or report what happened at https://studentlife.oregonstate.edu/studentconduct/reporting so we can connect you with resources.

TurnItIn
Your instructor may ask you to submit one or more of your writings to Turnitin, a plagiarism prevention service. Your assignment content will be checked for potential plagiarism against Internet sources, academic journal articles, and the papers of other OSU students, for common or borrowed content. Turnitin generates a report that highlights any potentially unoriginal text in your paper. The report may be submitted directly to your instructor or your instructor may elect to have you submit initial drafts through Turnitin, and you will receive the report allowing you the opportunity to make adjustments and ensure that all source material has been properly cited. Papers you submit through Turnitin for this or any class will be added to the OSU Turnitin database and may be checked against other OSU paper submissions. You will retain all rights to your written work. For further information, visit Academic Integrity for Students: Turnitin – What is it?

Statement Regarding Students with Disabilities
Accommodations for students with disabilities are determined and approved by Disability Access Services (DAS). If you, as a student, believe you are eligible for accommodations but have not obtained approval, please contact DAS immediately at 541-737-4098 or at http://ds.oregonstate.edu. DAS notifies students and faculty members of approved academic accommodations and coordinates implementation of those accommodations. While not required, students and faculty members are encouraged to discuss details of the implementation of individual accommodations.

Accessibility of Course Materials
All materials used in this course are accessible. If you require accommodations please contact Disability Access Services (DAS).

Additionally, Canvas, the learning management system through which this course is offered, provides a vendor statement certifying how the platform is accessible to students with disabilities.

Tutoring and Writing Assistance
Tutoring and academic support through the College of Engineering is available through the following link https://engineering.oregonstate.edu/current-students/academic-support

The Oregon State Online Writing Suite is also available for students enrolled in Ecampus courses.

Ecampus Reach Out for Success

University students encounter setbacks from time to time. If you encounter difficulties and need assistance, it's important to reach out. Consider discussing the situation with an instructor or academic advisor. Learn about resources that assist with wellness and academic success.

Ecampus students are always encouraged to discuss issues that impact your academic success with the Ecampus Success Team. Email ecampus.success@oregonstate.edu to identify strategies and resources that can support you in your educational goals.

If you feel comfortable sharing how a hardship may impact your performance in this course, please reach out to me as your instructor.

- **For mental health:**
  Learn about counseling and psychological resources for Ecampus students. If you are in immediate crisis, please contact the Crisis Text Line by texting OREGON to 741-741 or call the National Suicide Prevention Lifeline at 1-800-273-TALK (8255).
- **For financial hardship:**
  Any student whose academic performance is impacted due to financial stress or the inability to afford groceries, housing, and other necessities for any reason is urged to contact the Director of Care for support (studentassistance@oregonstate.edu or 541-737-8748).

Academic Calendar

All students are subject to the registration and refund deadlines as stated in the Academic Calendar: https://registrar.oregonstate.edu/osu-academic-calendar.

Student Bill of Rights

OSU has twelve established student rights. They include due process in all university disciplinary processes, an equal opportunity to learn, and grading in accordance with the course syllabus: https://asosu.oregonstate.edu/advocacy/rights.

Student Learning Experience Survey

During Fall, Winter, and Spring term the online Student Learning Experience surveys open to students the Wednesday of week 9 and close the Sunday before Finals Week. Students will receive notification, instructions, and the link through their ONID email. They may also log into the survey via MyOregonState or directly at https://beav.es/Student-Learning-Survey. Survey results are extremely important and are used to help improve courses and the learning experience of future students. Responses are anonymous (unless a student chooses to "sign" their comments, agreeing to relinquish anonymity of written comments) and are not available to instructors until after grades have been posted. The results of scaled questions and signed comments go to both the instructor and their unit head/supervisor. Anonymous (unsigned) comments go to the instructor only.