



**Oregon State University**  
**Ecampus**

**Course Name:** Cryptography

**Course Number:** CS 427

**Credits:** 4

**Instructor name:** Mike Rosulek

**Instructor email:** [rosulekm@eecs.oregonstate.edu](mailto:rosulekm@eecs.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

I have 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[n't] 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 on Canvas or the course Slack group. Weekly office hours will also be held on Zoom (schedule to be announced). For any other questions, email is the preferred method ([rosulekm@eecs.oregonstate.edu](mailto:rosulekm@eecs.oregonstate.edu)). Please allow response time of 24 hours for discussion forum questions and emails. Expect homeworks to be graded and returned within 5 days.

## Course Credits

Students will be expected to spend about 12 hours a week 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 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	94-100
A-	90-93
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-73
D+	65-70
D	55-64
F	0-54

## Course Content

Module	Wk	Topic	Reading Assignments	Learning Activities
1	1	Unconditional Security <ul style="list-style-type: none"> <li>• One-time pad</li> <li>• Secret sharing</li> <li>• Provable security fundamentals</li> </ul>	Textbook: Chapters 1-2	Reading discussions Self-test quizzes Written homeworks Practice problems
	2		Textbook: Chapters 2-3	
2	3	Symmetric-Key Primitives <ul style="list-style-type: none"> <li>• Pseudorandom generators</li> <li>• Pseudorandom functions</li> <li>• Block ciphers</li> </ul>	Textbook: Chapters 4-5	Reading discussions Self-test quizzes Written homeworks Practice problems
	4		Textbook: Chapters 5-6	
3	5	Symmetric-Key Encryption <ul style="list-style-type: none"> <li>• Security against chosen plaintext attacks</li> <li>• Block cipher modes</li> <li>• Security against chosen ciphertext attacks</li> </ul>	Textbook: Chapters 7-8	Reading discussions Self-test quizzes Written homeworks Practice problems Midterm exam
	6		Textbook: Chapters 8-9	
4	7	Symmetric-Key Authentication <ul style="list-style-type: none"> <li>• Message authentication codes</li> <li>• Hash functions</li> <li>• Authenticated encryption</li> </ul>	Textbook: Chapters 10-11	Reading discussions Self-test quizzes Written homeworks Practice problems
	8		Textbook: Chapters 11-12	
5	9	Public-Key Cryptography <ul style="list-style-type: none"> <li>• Key agreement</li> <li>• Public-key encryption</li> <li>• Digital signatures</li> </ul>	Textbook: Chapters 13-14	Reading discussions Self-test quizzes Written homeworks Practice problems Final exam
	10		Textbook: Chapters 14-15	
	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 (3 discussions every 2 weeks).

### **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.

## **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**

[NetTutor](#) is a leading provider of online tutoring and learner support services fully staffed by experienced, trained and monitored tutors. Students connect to live tutors from any computer that has Internet access. NetTutor provides a virtual whiteboard that allows tutors and students to work on problems in a real time environment. They also have an online writing suite where tutors critique and return essays within 24 to 48 hours. Access NetTutor from within your Canvas class by clicking on the Tools button in your course menu.

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](mailto:ecampus.success@oregonstate.edu) to identify strategies and resources that can support you in your educational goals.

### **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](mailto:studentassistance@oregonstate.edu) or 541-737-8748).

## **Student Evaluation of Courses**

During Fall, Winter, and Spring term The online Student Evaluation of Teaching system opens to students the Wednesday of week 8 and closes the Sunday before Finals Week. Students receive notification, instructions and the link through their ONID. They may also log into the system via Online Services. Course evaluation results are extremely important and used to help improve courses and the hybrid learning experience for future students. Responses are anonymous (unless a student chooses to "sign" their comments, agreeing to relinquish anonymity) and unavailable 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.