Portland State UNIVERSITY

Fall 2025 CS 485/585

Intro to Cryptography

Instructor:	Fang Song
Course Meeting Schedule:	M/W 13:30 – 15:10 @ FAB 10
Email:	fsong@pdx.edu Start email subject line with "f25-4585"
Course webpage:	https://fangsong.info/teaching/f25_4585_icrypto/
Office hours:	W 09:45 – 10:45 @ FAB 120-25 and by appointment

Course Description

This course will explore the key concepts in modern cryptography, including *private-key* cryptography such as perfect secrecy, block ciphers, cryptographic hash functions and message authentication; as well as *public-key* cryptography such as public-key encryption and digital signatures. We will take a *conceptual* and *theoretical* approach: the focus is on the *ideas* rather than *implementations*, and on how to define and reason about security of cryptographic constructions in a mathematically sound manner.

Course Objectives

Upon the successful completion of this class, students will be able to:

1. understand the fundamental principles of modern cryptography: formal definitions, constructions, and proofs of security.
2. describe private-key primitives such as private-key encryption, pseudorandom generator, block ciphers and message authentication.
3. explain security definitions of private-key primitives, and prove security of representative constructions using reductions.
4. describe public-key primitives such as key exchange, pubic-key encryption, and digital signatures.
5. explain security definitions of public-key primitives, and analyze security of basic constructions such as the RSA and ElGmal schemes.
6. evaluate the effectiveness and identify potential flaws in newly designed cryptosystems.
7. integrate the above and develop a cryptographic way of thinking.

Course Prerequisites

CS 350 or equivalent. You must be comfortable with reading and writing mathematical proofs.

Readings

The following book is required. Other recommended readings can be found on the course webpage.

- [**KL**] Introduction to Modern Cryptography (3rd edition) by Jonathan Katz and Yehuda Lindell. Chapman and Hall/CRC, Dec. 2020. PSU Library Link.

Grading Policies

- Homework: 50%. Biweekly.
- Quizzes: 15%. Biweekly.
- Project: 30%.

- Participation: 5%.

Homework Policy

- You have a quota of 5 days in total for late submissions of homework or quizzes without penalty. You can use them at your will. Once the quota run out, no late submissions will be accepted.
- Collaboration on homework problems is highly encouraged, but you must write up solutions entirely on your own and clearly list who you discussed with for each problem. (See AI policy below.)
- All assignments must be submitted in PDF format. It is recommended to type-set your solutions using LaTeX.
- For each assignment, a random subset of problems will be graded.
- Quizzes must be completed on your own without any external references.

Course Topics and Tentative Schedule

Check course webpage for details and updates

Week	Topic	Suggested Reading
Week	**Topic**	**Suggested Reading**
1	Intro, history, perfect secrecy.	KL 1
2 – 4	Private-key cryptography: pseudorandom generators, block ciphers, message authentication, hash functions.	KL 2 – 8
5 – 8	Public-key cryptography: Diffie-Hellman key exchange, RSA, ElGamal public-key encryption, digital signatures.	KL 9 – 14
9 – 10	Selected topics	Online articles

Flexibility Statement

The instructor reserves the right to modify course content and/or substitute assignments and learning activities in response to institutional, weather, or class situations.

PSU Policies & Resources

Academic Integrity

Academic integrity is a vital part of the educational experience at PSU. Please see the PSU Student Code of Conduct for the university's policy on academic dishonesty. A confirmed violation of that Code in this course may result in failure of the course.

AI Policy

In this course, AI tools, such as ChatGPT, are permitted. However, to uphold scholarly standards, students are required to cite any AI-generated material that contributes to their work, including in-text citations, quotations, and references. If you have consulted AI tools on homework problems, you must describe how you interacted with them. You may NOT directly search for and use solutions via

AI or elsewhere online. You may be asked to explain your solutions to the course staff. The generation of content through AI without appropriate attribution constitutes academic misconduct.

Student Support Resources

- How to Find Help at PSU
- Access and Inclusion for Students with Disabilities
- Understanding Sexual Misconduct
- Title IX Reporting
- Religious Accommodations

Recording Technology Notice

We will use technology for virtual meetings and recordings in part of this course. Our use of such technology is governed by FERPA, the Acceptable Use Policy and PSU's Student Code of Conduct. A record of all meetings and recordings is kept and stored by PSU, in accordance with the Acceptable Use Policy and FERPA. I will not share recordings of your class activities outside of course participants, which include your fellow students, TAs/GAs/Mentors, and any guest faculty or community-based learning partners that we may engage with. **You may not share recordings outside this course. Doing so may result in disciplinary action.**

Turnitin

Students agree that all required papers may be subject to submission review for textual similarity for the purpose of detection of unoriginal writing, including plagiarism. All submitted papers will be included as source documents in the Turnitin.com reference database solely for the purpose of detecting unoriginal writing, including plagiarism of such papers. Use of the Turnitin.com service is subject to the Turnitin Acceptable Use.

In Case of Emergency

- **Call 9-1-1 for Emergencies**: Immediate threat to life and safety For issues such as a medical emergency, urgent violent incident, fire, etc., you can also call 503-725-5911
- **Call 503-725-4407** for Non-Emergencies: Campus Public Safety Office (CPSO) – Non-Emergency. For non-emergency issues such as vandalism, disturbance, suspicious person, theft, suspicious packages, access control, etc.