Portland State UNIVERSITY

Winter 2023 CS 485/585

Intro to Cryptography

Instructor:	Fang Song
Course Meeting Schedule:	M/W 14:00 – 15:50 @ CH 382
Email:	fsong@pdx.edu Stat email subject line with "w23-4585-icrypto"
Course webpage:	https://fangsong.info/teaching/w23_4585_icrypto/
Office hours:	TBD

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 representative 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 need to 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

- 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 allocate them at your will. Once the quota runs out, no late submissions will be accepted.
- Quizzes must be completed **on your own**.
- 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. You may NOT search solutions online.
- All assignments must be submitted in PDF format. It is recommended to type-set your solutions using LaTeX, and you will get extra credit doing so.
- "**I'll take 15%"** option on homework problems. Your solutions should be as clear and concise as possible. Partial credit will only be given for answers that make significant progress towards correct solutions. If you realize you cannot solve a problem, you may write "I'll take 15%" instead and get 15% for this problem (or part of the problem). You will get 0 if your solution is completely wrong. "I'll take 15%" option does not apply to problems of bonus credits.
- For each assignment, a random subset of problems will be graded.

Course Topics and Tentative Schedule

Check course webpage for details and updates

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

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.

Recording Technology Notice

We will use technology for virtual meetings and recordings in 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.

Disability Access Statement

If you have, or think you may have, a disability that may affect your work in this class and feel you need accommodations, contact the Disability Resource Center to schedule an appointment and initiate a conversation about reasonable accommodations. The DRC is located in 116 Smith Memorial Student Union, 503-725-4150, drc@pdx.edu, https://www.pdx.edu/disability-resource-center/

Safe Campus Statement

Portland State University desires to create a safe campus for our students. As part of that mission, PSU requires all students to take the learning module entitled Creating a Safe Campus: Preventing Gender Discrimination, Sexual Harassment, Sexual Misconduct and Sexual Assault. If you or someone you know has been harassed or assaulted, you can find the appropriate resources on PSU's Enrollment Management & Student Affairs https://www.pdx.edu/enrollment-management .

Title IX Reporting

As an instructor, one of my responsibilities is to help create a safe learning environment for my students and for the campus as a whole. Please be aware that as a faculty member, I have the responsibility to report any instances of sexual harassment, sexual violence and/or other forms of prohibited discrimination. If you would rather share information about sexual harassment, sexual violence or discrimination to a confidential employee who does not have this reporting responsibility and can keep the information confidential, please use these campus resources:

- Confidential Advocates: 503-894-7982 or schedule online (for matters regarding sexual harassment and sexual and relationship violence)
- Center for Student Health and Counseling: 1880 SW 6th Avenue #200; 503-725-2800

Discrimination and Bias Incidents

The Office of Equity and Compliance (OEC) addresses complaints of discrimination, discriminatory Harassment, and sexual harassment against employees (faculty and staff). If you or someone you know believes they have been discriminated against, you may file a complaint. Someone from the OEC will contact you to discuss how to best address your complaint.

The Bias Review Team (BRT) gathers information on bias incidents that happen on and around campus, and gives resources and support to individuals who experience them. You can report a bias incident you experienced or learned about. A member of the BRT will contact you if you indicate you would like to be contacted.

Religious Accommodations

If you would like to obtain religious accommodations, such as flexibility in attending evening courses or extension on assignments, please contact your instructors. If you need additional assistance, please contact the Office of the Dean of Student Life (DOSL) by emailing askdos@pdx.edu.

Cultural Resource Centers

The Cultural Resource Centers (CRCs) create a student-centered inclusive environment that enriches the university experience. We honor diversity, explore social justice issues, celebrate cultural traditions, and foster student identities, success, and leadership. Our centers include the Multicultural Student Center, La Casa Latina Student Center, Native American Student & Community Center, Pan African Commons, Pacific Islander, Asian, Asian American Student Center and the Middle Eastern, North African, South Asian program. We provide student leadership, employment, and volunteer opportunities; student resources such as computer labs, event, lounge and study spaces; and extensive programming. All are welcome!

Classroom Requirements for All Students and Faculty Due to Covid-19

The University has established rules and policies to make the return to the classroom as safe as possible. It is required for everyone to follow all the Return to Campus rules and policies. To participate in this class, PSU requires students to comply with the following.

Vaccination

- Be vaccinated against COVID-19 and complete the COVID-19 vaccination attestation form. Those students with medical or nonmedical exemptions or who will not be on campus at all must complete the process described on "COVID-19 Vaccine Exemption Request Form" to establish those exemptions.

Health Check, Illness, Exposure or Positive Test for COVID-19

- If you are feeling sick or have been exposed to COVID-19, do not come to campus. Call SHAC to discuss your symptoms and situation (503.725.2800). They will advise you on testing, quarantine, and when you can return to campus.
- If you test positive for COVID-19, report your result to SHAC and do not come to campus. SHAC will advise you on quarantine, notification of close contacts and when you can return to campus.
- Please notify your instructor, should you need to miss a class period for any of these reasons so that we can discuss strategies to support your learning during this time.
- If I become ill or need to quarantine during the term, either I or the department chair will notify you via PSU email about my absence and how course instruction will continue.

Failure to Comply with Any of these Rules

As the instructor of this course, the University has given me the authority to require your compliance with these policies. If you do not comply with these requirements, I may ask you to leave the classroom or I may need to cancel the class session entirely.

In addition, failure to comply with these requirements may result in a referral to the Office of the Dean of Student Life to consider charges under PSU's Code of Conduct. A student found to have violated a university rule (or rules) through the due process of student conduct might face disciplinary and educational sanctions (or consequences). For a complete list of sanctions, see Section 14 of the Student Code of Conduct & Responsibility.

Guidance May Change

Please note that the University rules, policies, and guidance may change at any time at the direction of the CDC, State, or County requirements. Please review the University's main COVID-19 Response webpage and look for emails from the University on these topics.