Applied Cryptography

Yingjiu (Joe) Li

September 13, 2025

Department of Computer Science, University of Oregon

1 Course Identity, Teaching Staff, and Logistics

- Course title: **CS 333: Applied Cryptography**
- CRN: 16379
- Prerequisites: CS 212.
- Recommended: CS 102
- Instructor: Joe Li (yingjiul@uoregon.edu)
- Course Materials:
  - **Textbook:** Katz and Lindell, "Introduction to Modern Cryptography 2e", ISBN 9781466570269.
  - **Slides:** Class slides will be provided.

2 Course Description

This course provides a systematic study of cryptography and its application. It covers cryptographic algorithms, including symmetric-key cryptography, public-key cryptography, cryptanalysis, cryptographic hash functions, and their usage toward message authentication codes, digital signatures, key management and distribution, and user authentication protocols. This course further covers structures, algorithms, methods, and systems that apply cryptographic methods, including how real-world needs and applications drive the design of cryptosystems and how real-life breaches with common cryptosystems may occur.

3 Expected Learning Outcomes

This course covers the basic concepts and practices of applied cryptography. The primary topics are familiarity with symmetric key cryptography, public key cryptography, message authentication codes and hash functions.

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

- Understand the basic purposes and principles of cryptography, classic cipher, and perfect cipher.
- Understand the basic concepts of symmetric-key cryptography, including the definitions of security, stream cipher, block cipher, DES, 3DES, AES, and block cipher modes; know how to use Cryptool and Openssl to perform symmetric-key cryptographic operations.
- Understand the basic concepts of public-key cryptography, including number theory basics, public key encryption and decryption, digital signature, and PKI operations. Know how to use Cryptool

and Openssl to perform public-key cryptographic operations.

- Understand how cryptography is used in message authentication codes, digital signatures, and key management and distribution.
- Become familiar with how different cryptographic methods are used in various real-world applications; and
- Explain how some cryptosystem breaches occur.

4 Scheduling

- Class time: WF 4:00-5:20pm
- Class location: Chiles 128
- Office hours: T 3:30-4:30pm at DES 256
- Midterm: class time in week 6
- Final: Thursday, December 11, 2025, 2:45pm-4:15pm

5 Course Schedule and Assignments

Week	Topic	Assessment	Textbook
1	Introduction and classical ciphers: The basic purposes and principles of cryptography, applying cryptography for real needs, the pros, cons, and risks in using cryptography, classical cipher, and perfect cipher		Ch1, Ch2 (p3-38)
2	Symmetric cryptosysttem: definitions of security, stream cipher, and block cipher		Ch3 (p43-106)
3	Symmetric cyrptosystem: DES, 3DES, AES, and block cipher modes	Exercise 1 (10%)	Ch6.1-Ch6.2 (p194-230)
4	Asymmetric cryptosystem: number theory		Ch8.1–Ch8.3 (p287-331)
5	Public key encryption	Exercise 2 (10%)	Ch11 (p375-438)
6	Midterm Exam	Midterm (30%)	
7	MAC		Ch4.1-4.4 (p107-130)
8	Hash		Ch5 (p153-192), Ch6.3 (p231-235)
9	Digital signature	Exercise 3 (10%)	Ch12.1-12.5 (p439-460)

10	PKI		Ch12.7-Ch12.8 (p473-480)
11	Final Week	Final exam (30%) class and lab attendance (10% = 1%*10 weeks)	

Assignments:

- Exercise 1: A symmetric key encryption exercise is given for students to perform file encryption using standard block ciphers such as AES and compare their security strength and runtime performances.
- Exercise 2: A public key encryption exercise is given for students to perform file encryption using standard public key algorithms such as RSA and compare their security strength and runtime performances.
- Exercise 3: A digital signature exercise is given for students to generate and verify digital signatures on data files and compare their security strength and runtime performances.

6 Grading Policy

Exercises 30% Class participation 10% Midterm 30% Final 30%

Grading Rubric:

A Excellent. Solid grasp of concepts, approaches, and/or programming skills introduced or used in this course. Very well prepared to apply this knowledge to future studies or employment.

B Very good. Generally good grasp of concepts, approaches, and/or programming skills introduced or used in this course. Prepared to apply this knowledge to future studies or employment.

C Pass. Basic grasp of concepts, approaches, and/or programming skills introduced or used in this course. Minimally prepared to apply this knowledge to future studies or employment.

D No Pass (Earns UO credit). Demonstrated grasp of concepts, approaches, and/or programming skills introduced or used in this course is not yet sufficient to apply this knowledge to future studies or employment.

F No Pass (No credit). Little or no demonstrated grasp of concepts, approaches, and/or programming skills introduced or used in this course, and/or failure to carry out much of the required work.

A+ Distinction. A+ grades will be given only in cases where the student has excelled in all course topics and overall performance is distinctly better than that required for an A grade.

Grading Scheme:

A+	100 %	to 97.0%
A	< 97.0 %	to 94.0%
A-	< 94.0 %	to 90.0%
B+	< 90.0 %	to 87.0%
B	< 87.0 %	to 84.0%
B-	< 84.0 %	to 80.0%
C+	< 80.0 %	to 77.0%
C	< 77.0 %	to 74.0%
C-	< 74.0 %	to 70.0%
D+	< 70.0 %	to 67.0%

D	< 67.0 %	to 64.0%
D-	< 64.0 %	to 61.0%
F	< 61.0 %	to 0.0%

The instructor reserves the right for some small changes of grading. Any variation will be made for the benefit of students. Contact the instructor if there is still a disagreement.

For class participation, the following grading rubric is used:

- Far below standards: Comments vague if given at all; frequently demonstrates a lack of interest
- Satisfactory: Sometimes participates constructively in group work and class discussions, sometimes goes on auto-pilot
- Good: Participates constructively in group work and class discussion throughout the term
- Excellent: Plays an active, dynamic role in discussions and group work throughout the term

7 Estimated Student Workload

The workload of this course is expected to be as follows.

- **Class participation**. Students should actively participate in the class (usage of any device is forbidden unless used for the class), including raising questions and being involved in discussions.
- **Course review**. Students should carefully review the class materials after the class. Five hours a week on average is expected.
- **Homework**. There will be 3 exercise assignments throughout the term. Each assignment will need 3-5 hours on average.

8 Communication Outside of Class

- Fully use the office hours of the instructor and the teaching GE of this class.
- Canvas and Zoom: We will use canvas to post course materials, post and collect assignments, and support discussions. We will use Zoom for the remote delivery of this course if it is arranged so.
- Feel free to email the instructor and the GE.

9 Academic Dishonesty

For this course, all work must be done individually. You are encouraged to generally discuss problems with other students, but you may never use some other student's solution or code in any way. The use of sources (ideas, quotations, paraphrases) must be properly acknowledged and documented.

The student conduct code allows an instructor to impose an appropriate sanction for a student found guilty of academic dishonesty, up to and including an *N* or an *F*.

For more information on academic honesty, please talk to the instructor or see the Student Conduct Code at http://arcweb.sos.state.or.us/rules/OARS_500/OAR_571/571_021.html.

10 Universal Learning Environment

The University of Oregon is working to create inclusive learning environments. Please notify me if there are aspects of instruction or design of this course that result in barriers to your participation.

(Students with a UO disability notification letter should please meet with me at their earliest convenience during the first two weeks of the term. You may also wish to contact Accessible Education Center in 164 Oregon Hall at 346-1155. For information about Support and Services for Students with Disabilities, see the Accessible Education Center Web page (http://aec.uoregon.edu/).)