CS 4600 Cryptography and IS

Instructor Info

Mingyan Xiao

Assistant Professor, Computer Science
Office: Building 8, Room # 8-45
Email: mxiao@cpp.edu

Lecture Info

Time: 1:00 PM–2:15 PM MoWe
Location: Bldg 8 Rm 345

Office Hrs

Time: 2:30 PM–4:00 PM and 5:30 PM-6:00 PM MoWe. Also, by appointment (email)

Course Description

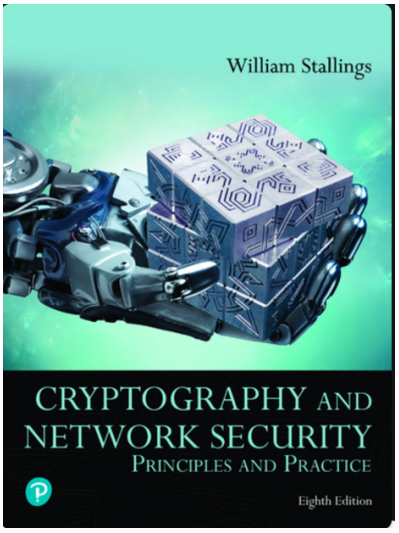
Information security fundamentals, symmetric and asymmetric encryption, digital signatures, certificates, applications of cryptography

Prerequisites

Pre-requisite(s): CS 2400 with a grade of C or better, or consent of instructor. A strong proficiency in systems and networking principles, C/C++/Java programming is also highly desirable.

Course Materials

Textbook: William Stallings. Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson, 2020. The following is how the cover of the book looks like.



Grading Policy

You will have a total numerical grade for this course, which will be converted to a letter grade that appears on your transcript. Following is a tentative structure how the total grade might be calculated. See the Section "Conversion to Letter Grades" for how to convert the numerical grade to the letter grade.

- Mid-term Group Presentation (30%):

There will be a mid-term group presentation of a specific cryptographic scheme (topic). There are 11 cryptographic schemes (topics). Each group will be responsible for one topic and has at most 5 students. Details will be provided two weeks before the first presentation date.

- Final Group Project (30%):

There will be a final group project. Each group has at most 2 students. In this project, each group will design and (partially) implement a cryptographic system with the desired properties and then make a short presentation regarding your work. Details will be provided at least two weeks before the presentation date. The presentation date is May 12.

- Quizzes, In-class exercise, Class participation (15%):

There will be 3 quizzes (in-class, take-home) throughout the course. The goal of these quizzes is to review and re-emphasize the materials covered in the class. Students are required to participate in class discussion and in-class exercises. This will be closely monitored by the course instructor and an essential component to successfully complete the class.

- Homework Assignments (25%):

There will be 3 homework assignments that will include theoretical and practical questions about computer security skills. These assignments are to be completed individually unless otherwise noted. Assignment submission and related details will be announced in the class. You will usually have at least two weeks to finish the homework.

- Bonus credit (up to 5%):

Community activity: Students can receive these bonus credits for presentation (paper or poster) in a cybersecurity related event such as a conference or club meeting, participation in an online capture-the-flag competition such as National Cyber League. Please discuss with the instructor prior to such activities for bonus credit and reporting details.

Late Submission Policy: Late submission beyond the deadline will not be accepted. In cases of emergencies (such as a medical emergency) or justifiable reasons, contact the instructor if you are unable to make the deadline. Submissions of assignments will be handled through Canvas and the submission site will close automatically at the deadline. (Some students will have extended deadline as they request accommodations through DRC)

Missing Quizzes/Exams Policy: Rescheduling will not be accepted. In cases of emergencies (such as a medical emergency) or justifiable reasons, contact the instructor if you cannot make it. Make-up quizzes/exams/presentation are allowed only with the instructor's permission.

Letter Grade Policy (Subject to change)

A: 95% -100% A-: 90%-94%, B+: 87%-89%, B: 84%-86%, B-: 80%-83%, C+: 77%-79%, C: 74%-76%, C-: 70%-73%, D: 60%-69%, F: < 60%

Tentative schedule

Date	Day	Topic
01/22	We	Lecture1-2: Introduction to Cryptography and IS
01/27	Mo	
01/29	We	Lecture 3-4: Introduction to Cryptography and IS
02/03	Mo	
02/05	We	Lecture 5-6: Encryption and Classical Ciphers
02/10	Mo	
02/12	We	Lecture 7-8: Symmetric Encryption (DES, AES)
02/17	Mo	
02/19	We	Lecture 9-10: Asymmetric Encryption (Diffie & Hellman Key Exchange, RSA)
02/24	Mo	
02/26	We	Lecture 11-12: Security in Asymmetric Encryption
03/03	Mo	
03/05	We	Lecture 13-14: Hash Function, MAC and Digital Signature
03/10	Mo	
03/12	We	Midterm Group Presentation
03/17	Mo	
03/19	We	Midterm Group Presentation
03/24	Mo	
03/26	We	Lecture 13-14: Hash Function, MAC and Digital Signature
04/07	Mo	
04/09	We	
04/14	Mo	Lecture 15-16: Key Management and Certificates
04/16	We	
04/21	Mo	
04/23	We	
04/28	Mo	Lecture 17-18: Authentication
04/30	We	
05/05	Mo	Final Group Project
05/07	We	
05/12	Mo	Final Group Project Presentation

Code of Academic Honesty

Honor code is in effect for this course. Unless specified otherwise, all the work in the course is individual work, to be done by the student alone. All violations will be reported and may result in a failing grade for the assignment and/or course.

It can be very helpful to communicate with each other (and with the instructor) about the assigned work. However, each student is responsible for understanding each assignment, then

completing and handing in their own assignment. Any group activities will be clearly identified as such.

Campus Resources:

Students with Disabilities.
Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Disability Resource Center (https://www.cpp.edu/~drc). The Disability Resource Center is located in Building 9 Room #103, telephone 909-869-3333 or drc@cpp.edu.

Learning Resource Center (LRC) (https://www.cpp.edu/~lrc/index.shtml). The LRC provides academic tips, workshops, tutoring services, and other student support.

Counseling and Psychological Services (CAPS). If you are a student seeking support, services, or resources from CAPS, please contact them at 909-869-3220, or by email at caps@cpp.edu. Also, you can always talk to me, but I may not be able to maintain confidentiality for students, as instructors are mandatory to report to the University.