CS 5158/6058 Data Security and Privacy, Spring 2018
Course Syllabus

Instructor: Dr. Boyang Wang

Course Information

Instructor:	Boyang Wang, Assistant Professor
Email:	boyang.wang@uc.edu
Office:	ERC 532
Office Phone:	(513)-556-4785

Lecture Time:	TuTh 12:30pm – 1:50pm
Lecture Location:	Baldwin 645
Office Hours:	Tu 2:30pm – 4:30 pm (or by appointment)

Course Description

(3 Credits) An introduction to data security and privacy, including fundamentals of applied cryptography, techniques and algorithms to protect data security and privacy in networks, cloud computing, location-based services, databases, information retrieval and digital currency.

Prerequisites (By Topics)

Probability, Programming (C/C++, Python, or Java)

Course Goals and Expected Learning Objectives

Students will gain an understanding of fundamental techniques to protect data security and privacy, and learn how to design and analyze the security and privacy of systems in practice. They will also implement data security and privacy techniques in course projects.

This course will prepare students to use methods and algorithms to build systems that protect data security and privacy in different applications. By the end of this course, each student shall be able to

- Choose appropriate methods from existing data security and privacy techniques to solve a given problem
- Understand and analyze the security and privacy of a given system.
- Design and implement data security and privacy algorithms in practice.

Textbooks

Recommanded:

- Introduction to Modern Cryptography (2nd Edition), Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC, 2014.

Additional References:

- The Joy of Cryptography (*available online*), Mike Rosulek, Oregon State University, 2017.
- Lecture Notes on Cryptography (*available online*), By Shafi Goldwasser and Mihir Bellare
- Additional papers and references will be provided for advanced topics.

Course Topics

- One-time Pad and Pseudo Random Functions
- Symmetric-Key Encryption and Public-Key Encryption
- Message Authentication Codes, Hash Function and Signatures
- Diffie-Hellman Key Exchange, Secret Sharing
- Homomorphic Encryption
- Differential Privacy
- Searchable Encryption
- Order-Preserving Encryption
- Private Information Retrieval
- Multi-Party Computation, Garbled Circuits
- Crypto Currency

Course Assignments and Exams

There will be 3 individual programming assignments, 1 group programming assignment, 5 homework assignments, 1 final project (including a presentation and a final paper). Details of each assignment will be posted later. There will be no midterm or final exams.

- You will need to finish 3 individual programming assignments, all the homework assignments by yourself.
- You will need to form a group of 2 or 3 to finish the group programming assignment and the final project.

Grades will be assigned based on the performance on homeworks, programming assignments, and the final project. The weight assigned to each component for **both CS5158 and CS6058** are listed as below

Component	**Percentage**
Individual Programming Assignments	30%
Group Programming Assignment	20%
Homeworks	30%
Final Project	20%

CS5158 and CS6058 will have (slightly) different requirements in each assignment and the final project. Course grades will be assigned based on your final numerical grades as follows:

A	90 – 100
B	80 – 89
C	70 – 79
D	60 – 69
F	0 – 59

Late Submission Policy. You are expected to submit assignments on the due dates. Late submissions will lose 10% of the total grade of each assignment for each day they are late. Submissions after 2 days will not be accepted, unless arrangements are made with the instructor in advance or with proof of medical or other emergency.