CSCI 556 Introduction to Cryptography
Fall 2015

Lecture: 3:30-5:20 pm, MW, RTH 105

Instructor: Prof. Ming-Deh Huang
Office: Sal 314, Office Hours: MW 1:30-2:30pm (or by appointment)
Email: mdhuang[at]usc[dot]edu, Tel: (213) 740-4783

Course Information:

- **Text:**
    - Introduction to Modern Cryptography, Second Edition, Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC.
- **Supplemental Text:**
    - Handbook of Applied Cryptography, A. Menezes, and P.C. van Oorschot and S. Vanstone (On-line version and errata is at http://www.cacr.math.uwaterloo.ca/hac/)
- **Course Outline:** This is an introductory course to modern cryptography. The topics to be covered include: private-key cryptography, cryptographic hash functions, public-key cryptography including the RSA cryptosystems, Discrete-logarithm based cryptosystems, and Digital signature. If time permits, we will give a brief introduction to elliptic curve cryptography. The following Chapters will be covered: 1-5, 8-12..
- **Required Background:** We refer to the paragraph on **Required background** in the Preface of the textbook. We refer to Appendix A and Appendix B of the textbook for a review on asymptotic notation, basic probability theory, modular arithmetic and very basic group theory.

Class Structure:

- **Homework:** There will be about 5 assignments. You are not required to turn in your assignments. Instead there will be two quizzes based on the assignments which will determine your homework grade.
- **Exams:** There will be an in-class midterm exam and a final exam.

	Date
Quiz 1	Wednesday, Sept. 16
Midterm	Monday, Oct. 19

Quiz 2	Monday, Nov. 16
Final Exam	Monday, Dec 14, 2-4pm

- University rules prohibit any student from taking the final exam early. Please make your plans for the winter vacation accordingly.
- **Grade Policy:**

Homeworks	30%
Midterm	30%
Final Exam	40%

- Student Conduct Code of the University will be strictly enforced. Please review these policies.
- Please review University grading policies
- Please visit course homepage and check Announcement regularly.

Statement for Students with Disabilities
Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to TA) as early in the semester as possible. DSP is located in GFS 120 and is open 8:30 a.m.-5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776.
The email: ability@usc.edu

Statement on Academic Integrity
USC seeks to maintain an optimal learning environment. General principles of academic honesty include the concept of respect for the intellectual property of others, the expectation that individual work will be submitted unless otherwise allowed by an instructor, and the obligations both to protect one's own academic work from misuse by others as well as to avoid using another's work as one's own. All students are expected to understand and abide by these principles. Scampus, the Student Guidebook, contains the Student Conduct Code in Section 11.00, while the recommended sanctions are located in Appendix A: http://www.usc.edu/dept/publications/SCAMPUS/gov/. Students will be referred to the Office of Student Judicial Affairs and Community Standards for further review, should there be any suspicion of academic dishonesty. The Review process can be found at: http://www.usc.edu/student-affairs/SJACS/.