CSCI 556 Introduction to Cryptography
Fall 2021

Lecture: 10-11:50 am, MW

Instructor: Prof. Ming-Deh Huang

Email: mdhuang[at]usc[dot]edu

Office Hours: TBD

Course Information:

- **Text:** *Introduction to Modern Cryptography*, Second Edition, Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC.
- **Additional text:** *Bitcoin and cryotocurrency technologies*, Arvind Narayanan, Joseph Bonneau, Edward Felten,,Andrew Miller, Steven Goldfeder (draft version available at https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf
- **Course Outline:** This is an introductory course to modern cryptography. The topics to be covered include: private-key cryptography, pseudorandom generators and functions, cryptographic hash functions, zero-knowledge proof, public-key cryptography including the RSA cryptosystems, Discrete-logarithm based cryptosystems, and Digital signature. Selected topics from Chapters 1-12 will be covered. Additional topics may include elliptic curve cryptography, cryptocurrencies, quantum cryptography.
- **Objectives:** The objective is to study the theory and applications of modern cryptography, and its relations to complexity theory and number theory..
- **Required Background:** Please read *Required background* in the Preface of the textbook. Read *Appendix A* and *Appendix B* of the textbook for a review on asymptotic notation, basic probability theory, and basic algorithmic number theory (especially modular arithmetic and basic group theory).

Grade Policy:

Homeworks	40%
Midterm paper	30%

Final paper	30%

- 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/.