Syllabus: CSCI 499 Cryptography -- Fundamentals of Secure Communication & Computation

Shang-Hua Teng

Scope of Course:

This course features a rigorous introduction to modern Cryptography – a field that conducts mathematical & algorithmic studies of concepts, methods, and tools for protecting information in computer and communication systems. The course will focus on:

- **information-theoretic and computational views of security, privacy, and knowledge**
- **fundamental cryptographic primitives** (public-key encryption, digital signatures, pseudo-random number generation, and key agreement, etc)
- **basic protocols to guarantee confidentiality and authenticity of data and computation** (secret sharing, homomorphic encryption, interactive and zero-knowledge proofs, and multi-party secure computation, digital money, etc)
- **computational complexity requirements** in cryptography and practical implementation of cryptographic algorithms/protocols

We will also cover the relevant number theory and complexity theory.

Prerequisites: CSCI 270 (originally CSCI 303) or permission of the instructor.

Target Audience and Objectives:

This course constitutes an advanced undergraduate course covering the most important concepts, techniques, algorithms, and applications of modern Cryptography. It is targeted primarily at undergraduate students in Computer Science and related fields, who have strong theoretical and mathematical interests in data security and privacy.

A key goal of the course is to assist students with the necessary mathematical rigor regarding computer security and data privacy through the lens of computational complexity, as well as to provide students examples that interface theory and practice in the field of computation and communication.

Readings:
- Handouts by the instructor: research papers (by various authors) and lecture notes (from various universities):

- Additional recommended books (not required):
  1. The Foundations of Cryptography (vol I and II), by Oded Goldreich
     http://www.wisdom.weizmann.ac.il/~oded/foc.html
  2. Lecture Notes on Cryptography by Shafi Goldwasser and Mihir Bellare
     http://cseweb.ucsd.edu/~mihir/papers/gb.pdf
  4. Applied Cryptography by Bruce Schneier

**Syllabus (15 weeks):**

Lecture 1: Introduction to the theory of provable security
   Perfect Information Security vs Computational Security
   P vs NP
   Symmetric ciphers vs Public-Key Encryption
   Indistinguishability and unpredicatability
Lecture 2: Shamir’s Secret Sharing Scheme: An Example of Perfect Security
Lecture 3: Secret Sharing II: A general Scheme
Lecture 4: Symmetric ciphers I (possible guest lecture from Prof. Knight)
Lecture 5: Symmetric ciphers II (possible guest lecture from Prof. Knight)
Lecture 6: Message Authentication Codes (MAC)
Lecture 7: Pseudorandom generators and its use in symmetric ciphers
Lecture 8: Blum-Micali Construction
Lecture 9: Indistinguishability and unpredicatability
   Number Theoretic Basic I: Chinese Remainder Theorem
Lecture 10: Composability theorem and analysis of pseudorandom generators
Lecture 11: Blum-Blum-Shub Pseudorandom generator
Lecture 12: Public-key encryption
Lecture 13: RSA, Rabin, and computational security
   Number Theoretic Basic II
Lecture 14: Probabilistic Encryption
Lecture 15: Key Agreement: Diffie-Helman
Lecture 16: One Way and trapdoor functions, hardcore bits
Lecture 17: Signature Schemes
Lecture 18: Hashing Functions
Lecture 19: Intereactive and Zero Knowledge Proofs
Lecture 20: Zero Knowledge Proofs II
Lecture 21: Applications of Zero Knowledge Proofs
Lecture 22: Multiparty Computation I
Lecture 23: Multiparty Computation II
Lecture 24: Quick Introduction of Homomorphic Encryption
Lecture 25: Digital Money
Lecture 26: Other Cryptographic Primitives
Lecture 27-30 Student Presentations

Final

Grading Basis:
20% Quizzes
40% Projects and Presentations
40% Final Exam

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 the instructor as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m.-5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776.

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/.