Computer Science 346 - Spring 2013
Cryptography

Instructor: Brent Waters
Office: GDC 6.810 A
E-mail: `bwaters@cs.utexas.edu`
Office Hour: Monday 11:30-12:30 (Immediately after class)

TA: Yannis Rouselakis
Email: `yannis.rouselakis@utexas.edu`
Office Hours: Tuesdays 2-3
Location: GDC 6.702A

TA: Richard McPherson
Email: `rfm4u@virginia.edu`
Office Hours: Wednesday, 2-3 pm, Friday (swapping with Yannis), 2-3 pm
Location: GDC 6.728E

Class: Monday, Wednesday 10-11:30 in CBA 4.326

Course Objective   The objective of this course is to familiarize the students with cryptography and its applications. Topics will include historical cryptography, encryption, authentication , public key cryptography, number theory. There will be a focus will teach and build upon theoretical computer science techniques. A good background and comfort in classes such as CS336 is important.

Textbook   The required textbook for this course is "Introduction to Modern Cryptography" by Katz and Lindell. Students are responsible for all material covered in class, including material that is not in the textbook.

Grading   Grading will be roughly distributed as follows. As the course progresses the instructor may make modifications to the weight distributions.

Problem Sets (45%) There will be 5 problem sets assigned. Problem sets will emphasize both class learned in class as well as problem solving skills. Students must write up problem set solutions on their own, although some collaboration with up to two other students before the writeup is allowed for each assignment.

In class exams (45 %) Three in class exams will be given throughout the course. It is important that students are in class for the exams at the scheduled times.

Participation (5 %) Students will be graded on class attendance and discussion.

"Research Investigation" (5 %) Students will prepare a short report on a current topic.

Academic Honesty   Students are expected to follow the university's academic honesty policy.

Course Schedule   The course will roughly follow the schedule below. Note that a "lecture" in some cases will take up more than one class day.

Introduction

    Lecture 1: Class Overview, History of Encryption,   *KL Ch. 1,2*

    Lecture 2: Perfect Secrecy Requirements and the One Time Pad; Modern Cryptography

Encryption

    Lecture 3: Security Definitions and Many Message Security I   *KL Ch 3*

    Lecture 4: Pseudo Random Functions and Encryption

    Lecture 5: Practical Design of Block Ciphers — DES and AES

    Lecture 6: Modes of Operation: ECB, CBC, and Counter Modes

Authentication

    Lecture 7: Message Authentication Codes: Uses and Security Definitions   *KL 4.1-4.5*

    Lecture 8: MACs from Pseudo Random Functions

    Lecture 9: Putting it together — Chosen Ciphertext Security

Hash Functions

    Lecture 10: Collision Resistant Hash Functions: Uses and Definitions; Birthday Attacks   *KL 4.6*

    Lecture 11: Merkle-Damgård and Practical Hash Functions

Number Theory

    Lecture 12: Number Theory I   *KL 7.1-7.3*

    Lecture 13: Number Theory II

Public Key Cryptography

    Lecture 14: Using Number Theory: Collision Resistant Hash Functions

    Lecture 15: The Public Key Revolution and Diffie-Hellman Key Exchange

    Lecture 16: ElGamal Encryption and the DDH Assumption   *KL 10.5*

    Lecture 17: RSA Encryption   *KL 11.1*

Lecture 18: Digital Signatures, GMR Definition, One-Time Signatures   *KL Ch. 12*

Lecture 19: "Textbook RSA", Full-Domain Hash RSA and the Random Oracle Model   *KL Ch. 12*

Special Topics

Lecture 20: Traitor Tracing

Lecture 21: Client Puzzles

Lecture 22: Functional Encryption

Other Information

1. For questions, the students should first contact the TA. If a question remains unresolved the student should contact the instructor.

2. *Tentative* Exam Dates are: 1) February 27th, 2) April 10 3) April 29

   These are the best current estimates and are subject to change. Students must be in attendance for the exams.

3. Allowed absences are for religious observance and medical emergencies (with a doctor's note). If you need to reschedule an exam for either reason, please notify the instructor as soon as possible.