Computer Science CS 346
Cryptography

Class Time and Location
Monday, Wednesday 9:30-11 in UTC 3.132

People

Instructor: Brent Waters
Office: GDC 6.810
E-mail: bwaters@cs.utexas.edu
Office Hours: Monday, Wednesday 11-11:45 (Immediately after class)
Please alert instructor at end of class if attending office hours

TA: Rachit Garg
Email: rachg96@cs.utexas.edu
Office Hours: Monday 4-5, Thursday 12-1
Location: GDC 1.302

TA: George Lu
Email: gclu@cs.utexas.edu
Office Hours: Tuesday 3-4, Friday 1-2
Location: GDC 1.302

Course Overview The objective of this course is to familiarize the students with cryptography and its applications. Topics will include encryption, authentication , public key cryptography, number theory. This class will focus on understanding the **theoretical** underpinnings of cryptography. Key components of this course are understanding how to precisely formulate security definitions and how to rigorously prove theorems. This course is designed to be a **challenging theory course**. A good background and comfort in classes such as CS331 is important. A large component will be problems sets. These sets are meant to develop problem solving skills.

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 - 50%** There will be 5 problem sets assigned. The lowest score is dropped. 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 Exam - 15% March 23, Wed.** One in class exams will be given during the course. It is important that students are in class for the exams at the scheduled time.
- **Final Exam - 25%**
- **Class participation - 5%** Students will be graded on class attendance and discussion.
- **Research Investigation - 5 %** Students will prepare a short report on a current topic.

Face-to-Face Classes This course is designated as a "face-to-face" class. The material will be taught on site and no remote options or lecture recordings will be made. Students should plan on attending lectures in person to understand the material. *An exception to this exists for the first three lectures on Jan. 19,24,26 per university directive. Starting Jan. 31 all material will be taught in person.*

Exam Absences 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.

Seeking Assistance For questions about course material students are encouraged to first attend office hour (either TA or instructors). There are a total of six office hour times per week allocated between TAs and the instructors. Otherwise, for general questions students are encouraged to first try posting to the online class discussion board. For questions that cannot be handled in this manner (e.g. a private question about homework), the students should email the TAs by contact information above.

Course Schedule The following is a tentative schedule for the course. 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

Collision Resistant Hashing and Authentication

Lecture 7: Collision Resistant Hash Functions and Merkle-Damgard *KL 4.6*

Lecture 8: Message Authentication Codes *KL 4.1-4.5*

Lecture 9: MACs for longer Messages

Lecture 10: Putting it together − Chosen Ciphertext Security

Number Theory

Lecture 11: Groups and Number Theory *KL 7.1-7.3*

Lecture 12: Modular Arithmetic

Public Key Cryptography

Lecture 13: Using Number Theory: Collision Resistant Hash Functions

Lecture 14: The Public Key Revolution *KL 10.5*

Lecture 15: Digital Signatures and RSA *KL 11.1,12*

Lecture 16: Bit Commitments

Lecture 17: Public Key CCA from Encryption with Randomness Recovery

Lecture 18: Learning with Errors and Postquantum Cryptography