Computer Science CS 346
Cryptography

Instructor: Brent Waters
Office: GDC 6.810
E-mail: bwaters@cs.utexas.edu
Office Hour: Monday 10-11 (Immediately after class)

TA: Rishab Goyal
Email: goyal@utexas.edu
Office Hours: Thursday and Friday 12-1
Location: GDC 1.302, Desk TBA

Class: Monday, Wednesday 8:30-10:00 in GDC 1.304

Course Overview 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. 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 rigoursly 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 - 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.
- **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.

Academic Honesty Students are expected to follow the universitys academic honesty policy.

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*

Other Information

1. For questions, the students should first contact the TA. If a question remains unresolved the student should contact the instructor.
2. 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.