Computer Science CS 388H, Fall 2015
Graduate Cryptography

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

TA: Venkata Koppula
Email: kvenkata@cs.utexas.edu
Office Hours: Wednesday 2:00-3:30
Location: GDC 1.302, Desk 1

Class: Monday, Wednesday 11:00-12:30 in GDC 2.210

Course Overview The objective of this course is to give a graduate level introduction 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**. While no prior knowledge of cryptography is required, comfort with CS theory 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 four 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%** Two 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 university's 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 and History of Encryption *KL Ch. 1,2*

Lecture 2: Perfect Secrecy Requirements and the One Time Pad

Encryption

Lecture 3: Encryption Security Definitions and Reductions *KL Ch 3*

Lecture 4: Pseudo Random Functions and Encryption

Lecture 5: Hybrid Proofs and Many Message Encryption

Lecture 6: GGM Pseudo Random Function Construction

Lecture 7: Practical Design of Block Ciphers, DES and AES

Lecture 8: Modes of Operation

Hash Functions and Authentication

Lecture 9: Collision Resistant Hash Functions: Uses, Definitions and Constructions *KL 4.6*

Lecture 10: Message Authentication Codes: Uses and Security Definitions *KL 4.1-4.5*

Lecture 11: MACs for Longer Messages

Lecture 12: Putting it together − Chosen Ciphertext Security

Number Theory

Lecture 13: Number Theory I *KL 7.1-7.3*

Lecture 14: Number Theory II

Public Key Cryptography

Lecture 15: Using Number Theory: Collision Resistant Hash Functions

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

Lecture 17: Digital Signatures and RSA construction *KL 12*

Lecture 18: Encryption from Learning with Error