Computer Science 388H - Fall 2009
Cryptography

Instructor: Brent Waters
Office: ACES 2.438
E-mail: bwaters@cs.utexas.edu
Office Phone: 512-232-7464

Class: MW 11-12:30 in Jester A218A
Office Hours: by appointment

Course Objective This course reviews the foundations of Cryptography. Topics include: formal notions of security, encryption, signatures, complexity assumptions, zero knowledge, and multiparty computation.

Textbook The Textbooks for this course are "Introduction to Modern Cryptography" by Katz and Lindell and "Foundations of Cryptography Volume I" by Oded Goldreich. Not all material covered in class will be included in the textbooks.

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 3-5 problem sets assigned. Problem sets will emphasize both class learned in class as well as problem solving skills.

Midterm (40 %) A midterm will be given approximately 2/3 through the course.

Participation (10 %)

Course Schedule The course will roughly follow the schedule below.

Introduction

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

Number Theory

Lecture 2: Number Theory I *KL 7.1-7.3*

Lecture 3: Number Theory II

Lecture 4: Number Theory III

Public Key Cryptography

Lecture 5: Collision Resistant Hash Functions, DL Construction *KL 4.6 , 7.4*

Lecture 6: Digital Signatures, GMR Definition, One-Time Signatures *KL Ch. 12*

Lecture 7: Tree-Based Constructions *KL Ch. 12*

Lecture 8: "Textbook RSA", Full-Domain Hash RSA and the Random Oracle Model *KL Ch. 12*

Lecture 9: Definitions and Equivalences (GM) in Public Key Encryption *KL 10.1,10.2*

Lecture 10: RSA Encryption *KL 11.1*

Lecture 11: ElGamal Encryption and the DDH Assumption *KL 10.5*

Foundational Underpinnings

Lecture 12: One Way Functions and Permutations *KL 6.1-6.2*

Lecture 13: Hard Core Predicates, Goldreich-Levin Theorem *KL 6.3*

Building on Foundations

Lecture 14: Pseudom Generators: Definitions, Construction *KL 3.3, 6.4*

Lecture 15: Pseudorandom Functions, GGM Construction *KL 6.5*

Symmetric Key Cryptography (from Foundations)

Lecture 16: Symmetric Key Encryption, Construction from PRFs *KL Ch. 3*

Lecture 17: MACs, Constructions from PRFs *KL Ch. 4*

Lecture 18: Chosen Ciphertext Secure Encryption — Putting it together *KL 4.8*

Lecture 19: Midterm Review

Class Midterm

Zero Knowledge and Applications

Lecture 20: Bit Commitment — Construction from PRGs

Lecture 21: Zero Knowledge I

Lecture 22: Zero Knowledge II

New Topics

Lecture 23: Lossy Trapdoor Functions

Lecture 24: A Broader Look and Wrapup