Computer Science 388H - Fall 2011
Cryptography

Instructor: Brent Waters
Office: ACES 3.438
E-mail: bwaters@cs.utexas.edu
Office Hour: Monday Immediately after class

TA: Yannis Rouselakis
Email: johnysrouss@gmail.com
Office Hours: Wednesdays 3-4, Friday 11-12:30
Location: Painter 5.33, desk 1

Class: Monday, Wednesday 11-12:30 in RLM 5.120

Course Objective We will study the foundations and practice of Cryptography. Topics include: formal notions of security, encryption, signatures, complexity assumptions, and zero knowledge.

Textbook The textbook for this course is "Introduction to Modern Cryptography" by Katz and Lindell. 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 (40%) There will be 4-5 problem sets assigned. Problem sets will emphasize both class learned in class as well as problem solving skills. You may collaborate with up to 2 other students. You must list collaborators and **you must write up solutions on your own.** Students are not allowed to consult with past exams or homework solutions from previous versions of the class.

Exams (50 %) Two in class exams will be given.

Participation (5 %) Class attendance and participation.

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

Course Schedule The course will roughly follow the schedule below.

Introduction and Background

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

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

Lecture 3: Number Theory II

Public Key Cryptography and Signatures

Lecture 4: Collision Resistant Hash Functions, DL Construction *KL 4.6 , 7.4*

Lecture 5: Digital Signatures, GMR Definition, One-Time Signatures *KL Ch. 12*

Lecture 6: Standard Signatures from One-Time *KL Ch. 12*

Lecture 7: "Textbook RSA" and Full-Domain Hash RSA *KL Ch. 12*

Lecture 8: Schnorr Signatures

Public Key Encryption

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

Lecture 10: ElGamal Encryption and the DDH Assumption *KL 10.5*

Lecture 11: RSA Encryption *KL 11.1*

Foundations and Symmetric Key Primitives

Lecture 12: Pseudorandom Generators: Definitions, Construction *KL 3.3, 6.4*

Lecture 13: Pseudorandom Functions, GGM Construction *KL 6.5*

Lecture 14: Symmetric Key Encryption, Construction from PRFs *KL Ch. 3*

Lecture 15: MACs, Constructions from PRFs *KL Ch. 4*

Lecture 16: Chosen Ciphertext Secure Encryption — Putting it together *KL 4.8*

Lecture 17: Pseudo Random Permutations and Practical Block Ciphers

Lecture 18: Cipher Modes

Advanced Topics

Lecture 19: Impagilazzo's Worlds

Lecture 20: Zero Knowledge I

Lecture 21: Zero Knowledge II

Lecture 22: Bilinear Maps and Identity-Based 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. Cheating is not allowed and will result in failure of the class.

3. *Tentative* Exam Dates are: Wednesday October 10th and Monday November 15th. These are the best current estimates and are subject to change. Students must be in attendance for the exams and should understand that they may become rescheduled.

   The first exam will roughly be in the material up through public key signatures, but may include some on public key encryption. The second exam will be on material up to the Advanced Topics.

4. We will not have class on Wednesday Nov. 21.

5. 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.