# Computer Science CS 346
## Cryptography

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

TA: Rishab Goyal
Email: goyal@utexas.edu
Office Hours: Tuesday 12:30-2:00
Location: GDC 1.302, Desk TBA

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

TA: Andrew Poelstra
Email: apoelstra@math.utexas.edu
Office Hours: Thursday 11:00-12:30
Location: GDC 1.302, Desk TBA

Class: Monday, Wednesday 11:00-12:30 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 foucs 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

*Authentication*

Lecture 7: Message Authentication Codes: Uses and Security Definitions *KL 4.1-4.5*

Lecture 8: MACs from Pseudo Random Functions

Lecture 9: Putting it together − Chosen Ciphertext Security

*Hash Functions*

Lecture 10: Collision Resistant Hash Functions: Uses and Definitions; Birthday Attacks *KL 4.6*

Lecture 11: Merkle-Damgard and Practical Hash Functions

*Number Theory*

Lecture 12: Number Theory I *KL 7.1-7.3*

Lecture 13: Number Theory II

*Public Key Cryptography*

Lecture 14: Using Number Theory: Collision Resistant Hash Functions

Lecture 15: The Public Key Revolution and Diffie-Hellman Key Exchange

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

Lecture 17: RSA Encryption *KL 11.1*

Lecture 18: Digital Signatures, GMR Definition, One-Time Signatures *KL 12*

Lecture 19: Textbook RSA, Full-Domain Hash RSA and the Random Oracle Model *KL 12*

*Special Topics*

Lecture 20: Traitor Tracing

Lecture 21: Client Puzzles

Lecture 22: Functional 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. Allowed absences are for religious observance and medical emergencies (with a doctors note). If you need to reschedule an exam for either reason, please notify the instructor as soon as possible.