CS 346 Cryptography (Spring 2020)

Logistics:
TTh 2:00-3:30, GDC 4.302
Unique Number: 50540
Course web page: `http://www.cs.utexas.edu/~diz/346`

Professor: David Zuckerman
Email: *diz@cs.utexas.edu*
Phone: 512-471-9729
Office: GDC 4.508
Office Hours: TTh 3:30-4:30

TA: Ridwan Syed
Email: *ridwan@cs.utexas.edu*
Office Hours: MW 3:30-4:30, TA desk 4, GDC 1st floor

Textbook: Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*

Course Overview: This undergraduate course is an introduction to cryptography, covering the mathematical techniques behind computer security. It includes methods to communicate secretly and authenticate data in the presence of adversarial attacks. We will show how to do seemingly impossible tasks, such as how two parties can communicate secretly even if they didn't agree on a secret key beforehand. To do this properly, we'll need to give precise definitions and computational assumptions, so that we can rigorously prove security. This course will be very mathematical, relying on probability and number theory and mathematical proof. A list of topics and approximate times follows.

Prerequisites: CS 331 or 331H. Naturally, you also need the prerequisites and corequisites for CS 331, including Discrete Math (CS 311 or 311H), Probability (SDS 321 or M 362K), and Linear Algebra (SDS 329C, Math 340L, or Math 341). Probability is essential, so make sure you know it well. Number theory is helpful but not required.

Grading:
70% In-Class Exams
30% Homework

Exams: There will be three in-class exams. Exam 1 will be held in class on Thursday, February 20. Exam 2 will be held in class on Thursday, April 2. Exam 3 will be held in class on Thursday, May 7. No make-up exams will be given, so plan accordingly. You may bring a single, 8.5x11 inch, handwritten sheet of paper (you may use both sides). No calculators are allowed (they won't be necessary).

Laptops/Phones: The use of laptops and mobile devices is generally prohibited; however, I will allow a tablets if you sit in the first row and only use them for class-related purposes. Other exceptions may be made in unusual circumstances. All phones must be silenced.

Class Schedule:

Date	Topic
Jan 21	Introduction
Jan 23	Perfect Secrecy
Jan 28	Security Definitions
Jan 30	Pseudorandom Generators and Stream Ciphers
Feb 4	Pseudorandom Functions and CPA Security
Feb 6	Pseudorandom Permutations and AES
Feb 11	Computational Number Theory 1
Feb 13	Computational Number Theory 2
Feb 18	Review
Feb 20	Exam 1
Feb 25	One-Way Functions
Feb 27	OWFs, PRGs, and PRFs
Mar 3	Message Authentication Codes
Mar 5	Extending Input Length for MACs
Mar 10	Chosen Ciphertext Security
Mar 12	Collision Resistant Hashing
Mar 24	Constructing CRHFs
Mar 26	Public-Key Revolution and Key Exchange
Mar 31	Review
Apr 2	Exam 2
Apr 7	El Gamal Encryption
Apr 9	RSA Encryption
Apr 14	Homomorphic Encryption
Apr 16	Digital Signatures
Apr 21	Secret Sharing
Apr 23	Secure Multiparty Computation
Apr 28	Interactive Proofs
Apr 30	Zero Knowledge
May 5	Class Summary, Review
May 7	Exam 3

Homework: There will be 8-10 homework assignments.

Collaboration policy: While you should first think about the problems on your own, you are encouraged to discuss the problems with your classmates. Please limit your collaborations on any particular homework to at most three other students. Discussion of homework problems may include brainstorming and verbally walking through possible solutions, but should not include one person telling the others how to solve the problem. In addition, each person must write up their solutions independently, and these write-ups should not be checked against each other or passed around or emailed. You must acknowledge any collaboration by writing your collaborators' names on the front page of the assignment. You don't lose points by having collaborators.

Citation policy: Try to solve the problems without reading any published literature or websites, besides the class text and links off of the class web page. If, however, you do use a solution or part of a solution that you found in the literature or on the web, you must cite it. Furthermore, you must write up the solution in your own words. You will get at most half credit for solutions found in the literature or on the web.

Late policy: No late homeworks will be accepted.

Students with Disabilites: Any student with a documented disability (physical or cognitive) who requires academic accommodations should contact the Services for Students with Disabilities area of the Office of the Dean of Students at 471-6259 (voice) or 471-4641 (TTY for users who are deaf or hard of hearing) as soon as possible to request an official letter outlining authorized accommodations.

Last updated January 21, 2020.