1 General Information

Cryptography, or "secret writing," is nearly as old as written communication itself. Yet only over the past few decades has it grown from a "black art" into a science with rigorous mathematical foundations and methodologies. These have taken cryptography far beyond its roots in simple secret codes, to a discipline with far-reaching influence on computing as a whole.

This class is a graduate-level, theory-oriented introduction to the foundations of modern cryptography. The emphasis is on essential *concepts*, precise *models and definitions*, and *proof techniques*. Topics include: one-way functions and related complexity assumptions, pseudorandomness and symmetric-key schemes, public-key and identity-based crypto, zero knowledge and commitment, and connections to diverse areas of computer science. As time permits, we may also touch upon exciting recent topic areas such as secure multiparty computation, private information retrieval, or lattice-based cryptography.

1.1 Materials

The main course web page is located on Piazza at `https://piazza.com/gatech/spring2013/cs7560/home`. For homework submission and grading, we will also be using the course T-Square site, at `https://t-square.gatech.edu/portal/site/28862.201302/`.

There is no required textbook for this class; lectures and notes are the main source of content. As supplements, students may wish to refer to the following excellent textbooks:

- *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell. An accessible book aimed at advanced undergraduate and beginning graduate students.
- *Foundations of Cryptography*, Vol. 1 and 2 by Oded Goldreich. A very comprehensive treatment of the theoretical foundations of cryptography; a great reference for those interested in understanding the material in greater depth.
- *A Course in Cryptography*, lecture notes by Rafael Pass and abhi shelat, freely available at `http://www.cs.cornell.edu/courses/CS4830/2010fa/lecnotes.pdf`.

In addition, the course web page contains links to many other excellent cryptography classes.

1.2 Prerequisites

There are no formal prerequisite classes. However, this course is mathematically rigorous, hence the main requirement is *mathematical maturity*. Specifically, students should be comfortable with reading and writing formal proofs, devising and analyzing algorithms and reductions between problems, and working with probability.

Highly recommended courses include CS 6505 (Algorithms, Computability and Complexity), CS 6520 (Computational Complexity Theory), and/or CS 6260 (Applied Cryptography). The instructor reserves the right to limit enrollment to students who have the necessary background.

2 Course Policies

2.1 Grading

Grades will be determined roughly as follows:

(50%) Homework assignments (4–5), due approximately every two weeks. Collaboration and external sources are allowed; see academic honesty policy for details.

(25%) Take-home exam (Mar 10–17). *Absolutely no collaboration or external sources are allowed!*

(25%) Research project/survey (due Apr 28) and general attendance/participation.

All submitted work will be graded on *correctness*, *clarity*, and *conciseness*, and must be typeset in LaTeX (templates will be made available). It is good practice to start any longer solution with an informal (but accurate) "proof summary" that describes the core idea — this will help the reader (and you!) understand your solution better.

There are no predetermined score thresholds for A/B/C/etc. Your primary focus should be on *learning the material*, not your grade.

2.2 Academic Honesty

Your solutions to the take-home exam must exclusively represent your own work — *absolutely no collaboration or consultation with external sources is permitted.* You may refer only to materials that you and your colleagues prepared prior to the release of the exam, and to any materials or clarifications provided by the instructor.

On homework assignments, collaboration and consultation with external sources is allowed and encouraged, subject to the following conditions:

- You must submit your own individually written solution, and you must list your collaborators/sources for each problem.
- You may not submit a problem solution that you cannot explain orally.

There is no hard-and-fast list of (dis)honest conduct. When in doubt, err on the side of caution, or ask the instructor. Dealing with academic dishonesty is unpleasant for everyone involved, so please follow these policies!

3 Syllabus and Schedule

The course will be broken loosely into units, each covering a number of topics within a certain broad theme. The approximate plan is as follows. Note that the pace and/or content may change as needed, or to reflect levels of interest.

- **Background and overview.** (1 lecture) Overview of course. Shannon / perfect secrecy.
- **Computational hardness.** (3 lectures) Computational model. One-way functions / permutations. Hardness amplification. Number theory and candidate hard functions.
- **Indistinguishability and pseudorandomness.** (6 lectures) Hard-core bits and pseudorandom generators / functions. Shared-key (symmetric) encryption. Public-key (asymmetric) encryption.
- **Authentication.** (4 lectures) Message authentication codes. Hash functions. Digital signatures.
- **Interaction and knowledge.** (4 lectures.) Interactive proofs. Commitment. Zero knowledge. Secure computation.

- **Advanced encryption.** (4 lectures.) Chosen-ciphertext security. Identity-based encryption.
- **Special topics.** (5 lectures.) Possible topics: Lattice-based cryptography. Multi-party computation. Advanced zero knowledge.

Special Dates

Note the following special dates:

- **Feb 26 and 28.** Guest lecture and/or class cancelled, TBD.
- **Mar 19 and 21.** No class (spring break).
- **Mar 7.** Take-home exam out.
- **Mar 14.** Take-home exam due by start of class.
- **Apr 25.** Research project/survey due.