CS 6260: Applied Cryptography
Course Information and Syllabus

1 Basic Information

Instructor:	Prof. Chris Peikert, cpeikert@cc.gatech.edu, Klaus 3146
TA:	Eric Crockett, ecrockett3@gatech.edu, Klaus 2124
Class meetings:	T,Th 9:35-10:55am, Klaus 1456
Office hours:	(Chris) TBA, or by appointment
	(Eric) TBA, or by appointment
Optional textbook:	*Introduction to Modern Cryptography*, by Jonathan Katz and Yehuda Lindell
Course website:	https://t-square.gatech.edu/portal/site/XLS0814164958201208.201208
Piazza site:	https://piazza.com/gatech/fall2012/cs6260

2 Course Description

This is a 3-credit graduate-level introduction to modern cryptography. We focus on the classical goals of cryptography, including data privacy (confidentiality), authenticity, and integrity. Specific topics of study include pseudorandom functions and permutations, block ciphers, symmetric encryption schemes, cryptographic hash functions, message authentication codes (MACs), public-key (asymmetric) encryption, public key infrastructure (PKI), digital signatures, secret sharing schemes, and threshold cryptography.

In this course you will learn a variety of cryptographic tools and how they are used in practice, but the main objectives are more fundamental. Our primary goal is to build an understanding of what it *means* for different cryptographic objects to be "secure," how to evaluate and measure such security, and how to determine which tools are appropriate for different application scenarios. In particular, we understand the meaning of security by way of precise mathematical *models* and *definitions* for various kinds of primitives.

Cryptography is only one part of the much broader area of computer security. There are many topics that are beyond the scope of cryptography and will not be covered in this course, such as viruses, worms, buffer overflow and denial of service attacks, access control, intrusion detection, etc. (The course *Introduction to Information Security* (CS 4253/8803) covers many of these topics.) We do not consider implementation issues in depth, though there may be opportunities to implement some schemes. The course *Theoretical Foundations of Cryptography* (CS 7560) course studies complementary, more theoretical and often more advanced topics of cryptography.

Prerequisites. No previous knowledge of cryptography is necessary. This course is about applying cryptography to solve real-world problems, but it is still in large part a theory-oriented course. The main requirement is "**mathematical maturity**:" you will need to be able to read and write precise mathematical definitions, statements, and proofs. You should have done well in an undergraduate discrete math class, and taken introductory algorithms and computability/complexity theory classes. In particular, you will have to know how to analyze the running time of an algorithm, and it will also be helpful to understand the notion of a *reduction* from one problem to another. You will also need to know some basic probability theory. All necessary elements of number theory will be presented in class. No programming will be required, though there may be optional programming assignments. If you have doubts about whether you have the right background, please talk to or email the instructor.

Piazza. This term we will be using Piazza for class discussion. The system is designed to get you help fast and efficiently from classmates, the TA, and myself. Rather than emailing questions to the teaching staff, I encourage you to post your questions on the Piazza site, and answer others' questions. (However, please do not ask for or provide direct answers to the homework questions.) You can reach Piazza from the course T-Square site, or directly at the address above.

3 Assignments and Grading

Homework. Homeworks are designed to reinforce your understanding of the material from class and readings. There will be 6–7 homeworks, which are due roughly every two weeks at the start of class, via T-Square. Late homeworks will not be accepted without getting an extension from the instructor or TA in advance. Solutions must be **typed**, preferably in LaTeX; well-organized; and clearly understandable.

Collaboration with other students taking the class is both allowed and encouraged! However, as part of the course's academic honesty policy you must abide by the following rules:

- **Try the problems by yourself first.**
- **Write up your solutions from scratch, in your own words.**
- **List all your collaborators**—i.e., anyone with whom you discussed a problem—at the top of your homework. (When in doubt, include! There is no penalty for collaborating.)
- **Do not consult any external sources** (e.g., Internet web sites, students who've already taken the class, or their notes) other than the ones already mentioned.

Exams. There will be 3 in-class exams, but no final exam. During each exam, you may use **one 8.5-by-11" (double-sided) study sheet, prepared by you in advance**. You may not use any electronic devices or other resources during the exams. The in-class exams are *tentatively* scheduled for:

- 11 September (Tuesday)
- 4 October (Thursday)
- 6 November (Tuesday)

(Any changes to this schedule will be announced well in advance.)

Final project. For the final project, as part of a small group you will study in depth a particular topic of your choosing. There is wide latitude in the type and scope of the project. Some possible types of projects include:

- A detailed evaluation/audit of an existing cryptographic system or standard (e.g., a software library, a password manager, an industry standard);
- An analysis of the security and cryptographic requirements of some real-world application, and a design meeting those requirements;
- A survey of a few research papers on a particular cryptographic topic;
- A significant implementation of some cryptographic scheme or attack.

Final grades. My approach toward grading is a hybrid of a fixed scale (i.e., $X\%$ for an A, $Y\%$ for a B, etc.) and a "curve" (i.e., $X\%$ of students get an A, $Y\%$ get a B, etc.). I start with an approximate idea of what percentage is an appropriate cut-off for each letter grade, and adjust it to fit the particular circumstances of the class.

Final scores will be determined as follows:

- 35% Homeworks and participation (e.g., asking and answering good questions, pointing out errors in class materials, etc.)
- 50% In-class exams
- 15% Final project

Grades will be posted on the course web site as they become available.

Academic Honesty. I recognize and fully support the Georgia Tech Academic Honor Code as defined for the GT community. A copy of the Honor Code can be found at the Georgia Tech web site. All students are expected to maintain high standards of academic integrity. Unless stated otherwise above, all work is to be done individually.

Violations of the academic honesty policy may lead to a zero score on the assignment in question for the first violation, and a penalty up to and including a failing grade for the course for a second violation. All violations will be reported to the Office of Student Integrity.