**Instructor:** Alexandra (Sasha) Boldyreva

## COURSE DESCRIPTION AND GOALS

A graduate-level introduction to modern cryptography, which focuses on the classical goals of cryptography, such as data privacy, authenticity, and integrity.

### PREREQUISITES

No previous knowledge of cryptography is necessary. This course is about applying theory to practical problems, but it is still a theory course. The main requirement is basic "mathematical maturity." You have to be able to read and write mathematical definitions, statements and proofs.

It is expected that you were successful in your undergraduate discrete math class, and took basic algorithms and computability/complexity theory classes. In particular, you have to know how to measure the running time of an algorithm and how to do proofs by contradiction and contraposition. You also have to know very basic probability theory.

If you cannot recall what terms like permutation, sample space, random variable, conditional probability, big-O notation mean, you should consider taking the course in a later semester and refresh your knowledge of the above topics in the meanwhile. I recommend you review an undergraduate textbook on discrete math.

All necessary elements of number theory will be presented during the course.

### COURSE LEARNING OUTCOMES

You will learn various cryptographic schemes and how they are used in practice. For example, you will learn what AES, CBC, RSA, DSA, TLS stand for and how they "work." But the main objectives are more fundamental. The goals are to build an understanding of what "secure" is and how to evaluate and measure security. You will also learn how to compare the security of various cryptographic schemes, and how to select parameters to achieve required security guarantees.

### COURSE MATERIALS

The lecture slides and the video lectures are the main source of information. Some of the slides are designed by Mihir Bellare. As supplemental material, I highly recommend you to use

the lecture notes by Mihir Bellare and Phil Rogaway (BR lecture notes). We will use it as the (slightly outdated) textbook for the course. I will refer to it as "the BR lecture notes". Reading the lecture notes is highly recommended. I will not assign reading specifically; just read the chapters corresponding to the video lectures. You can also use the lecture slides created by Mihir Bellare.

If you prefer to have more materials, you may also consult the book by Dan Boneh and Victor Shoup, the book by Nigel Smart and "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell.

## COURSE DELIVERY

The course will be delivered in a "flipped classroom" fashion. Each week we will meet in class on Tuesday to discuss the material you learned the week before. To learn the material, you will be watching recorded lecture videos (which are carefully prepared and are much better than my average live lectures). The lectures can be found under the Modules tab. I will also ask you to submit a question about the material each week. This will help me with the discussions. On Tuesdays you will also take a very short quiz about the material learned the week before.

On Thursdays I, or sometimes a TA, will go over the solutions for the Tuesday quiz, and the prior homework. We will also some exercises. I will also leave time for questions and concerns.

## COMMUNICATION

The course will be managed via the course Canvas page. All course info and materials can be accessed from Canvas. You will submit homeworks and take quizzes via Canvas. Exams are in class.

## ED DISCUSSIONS

Ed Discussions will be the forum for the course, accessible through Canvas. We are careful about checking messages on the discussion board and making sure that your questions are answered in a timely fashion. Most importantly, by asking questions on Ed Discussions, you can benefit from the collective knowledge of your classmates and instructors. For this reason, we encourage you to ask questions publicly to the class, rather than privately to the instructors, as that maximizes your chances to get a prompt reply and, most importantly, allows your classmates to see questions, answers, and discussions that can benefit them.

It is just as important that you also check forum postings regularly, as important information and announcements will be made there. **Please read the BR lecture notes and prior forum posts related to your question *before* posting the question.**

Do not post any solutions or hints to solutions for ongoing assignments on the forum. The TAs sometimes may give hints, but the students should not.

We do our best to respond to forum messages daily, or at most within a couple of days (depending on volume and other factors). Replies on weekends or during breaks may be slower. If you don't get an answer to a post within 48 hours, feel free to post a follow-up, but please avoid doing so a few hours after posting. Please also avoid reposting the same message twice to get more attention; you should add a follow-up to your existing post instead.

## COURSE REQUIREMENTS AND GRADING POLICY

Students in this course are required to watch all course video materials, attend the discussions and complete the homeworks, quizzes and exams. They are also expected to complete the course evaluation at the end. The grading policy is as follows.

- Short quizzes/knowledge tests (11 out of 12- lowest score dropped): 15% total
- Homeworks (4 out of 5- lowest score dropped): 20% total
- Coding Homeworks (2): 3% total
- Midterm exam: 30%
- Final exam: 30%
- Submitting questions: 2%

Grades will be assigned as:

- A: 80+%
- B: 60+ - 80%
- C: 40+ - 60%
- D: 20+ - 40%
- F: 0-20%

However, sometimes I will curve in your favor. The grade in this class will be based solely on demonstrated performance. No grade will ever be changed because the student needs a better grade to stay in the program, to keep a fellowship, to get a job, or any other reason.

Assignments must be submitted via Canvas by the indicated due date and time. Exams are in class. No late homework is accepted, but the lowest homework score will be dropped.

Your submissions will typically be graded within 2 weeks. If you feel that you were mis-graded on anything, first look at the solutions. If you still feel you were mis-graded, submit a regrade request through Gradescope. If you are still not happy after your re-grade request is addressed, please talk to the instructor. Please keep in mind that, if the re-grading reveals issues that the TA had initially missed, this may result in a lower grade.

**I expect that every student leaves the course review at the end.** This is very important.

## HOMEWORKS

In doing homeworks, you are forbidden from referring to any resources other than course materials (videos, slides, lecture notes and solutions to previous homeworks), unless stated otherwise. In particular, you are not allowed to use the Internet or AI to find solutions, unless stated otherwise. Violators will be reported. You can search the Internet to study the concepts, of course.

We release homeworks after you are scheduled to learn the corresponding content. Please do not ask us to post assignments in advance. Start working on the assignments as soon as possible.

You can discuss homeworks with **up to two more people**, but you must **write the solutions entirely by yourself**. You must indicate the names of your collaborators on your solutions.

Remember, you are graded on what you write, not on what you think you "meant." Please read the article on Mathematical Writing.

## QUIZZES

Quizzes typically cover the prior week's material, but they can touch on earlier material as well. They are "closed book". The lowest quiz score will be dropped. No late submissions will be accepted.

## EXAMS

For the exams you are forbidden from referring to any resources other than course materials (videos, slides, lecture notes, your notes, and solutions to previous homeworks).

## ATTENDANCE and/or PARTICIPATION

This will be an active classroom, where you will be expected to attend and participate.

## EXTRA CREDIT OPPORTUNITIES AND MAKE-UP WORK

There are no extra credit opportunities for this class. There will be no make-up assignments, so if you need a particular grade plan to perform accordingly on the homeworks, tests and the exams.

If extreme and unforeseen circumstances are preventing you from completing an assignment on time, please contact the office of the Dean of Students and provide them with all the necessary details and documentation (see http://studentlife.gatech.edu/content/contact-us). Contact us and confirm that you have provided the required documentation to the office of the Dean of Students. The Dean's office is equipped to verify these exceptions better than us, and provides a level of uniformity across courses on how emergencies are handled. The office of the Dean of Students will check your documentation and follow-up with me. At that point the instructor will be able to take the appropriate action and follow up with you.

## PLAGIARISM & ACADEMIC INTEGRITY

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/rules/18/.

**Do not copy any content (solutions or parts thereof) from other students in current or previous semesters or solutions found on the Web or generated by AI. Do not post publicly or share any content (assignments, hints, solutions or parts thereof) with others, during or after you take the course.**

Any student suspected of cheating or plagiarizing on a test, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations. Those can be quite severe.

## ACCOMMODATIONS FOR STUDENTS WITH DISABILITIES

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)-894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also email me as soon as possible in order to set up a time to discuss your learning needs.

## STUDENT-FACULTY EXPECTATIONS AGREEMENT

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. See http://www.catalog.gatech.edu/rules/22/ for an articulation of some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

## SUBJECT TO CHANGE STATEMENT

The syllabus and course schedule may be subject to change. Changes will be communicated via Ed Discussions and/or the Canvas announcement tool. It is the responsibility of students to check email messages and course announcements to stay current in their online courses.