PROFESSOR: Alexandra (Sasha) Boldyreva
TAs: George Kudrayvtsev, Chaitanya Rahalkar, Aarushi Dwivedi, Harini Dandu

OFFICE HOURS via BlueJeans (Eastern time):

George: Monday, 3pm (Solutions will be discussed, if anything was due.)
Harini: Tuesday, 6:30pm
Sasha: Wednesday, 1pm
Chaitanya: Wednesday, 3pm
Aarushi: Thursday, 1pm

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 and have a basic understanding of modular addition.

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 additional elements of number theory will be presented during the course.

COURSE GOALS

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 the understanding of what "secure" is and how to evaluate and measure security. You will also learn how to compare the security of various 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 We will use it as the (slightly outdated) textbook for the course.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 draft by Dan Boneh and Victor Shoup, the book by Nigel Smart and "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell.

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 tests via Canvas.

ED DISCUSSIONS

Ed Discussions will be the forum for the course, accessible through Canvas. Staff may miss email messages or DMs, but 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 and complete the homeworks, quizzes and exams.

- 5 out of 6 Homeworks (lowest score dropped): 25% total
- Short quizzes aka knowledge tests (lowest score dropped): 20% total
- Midterm exam: 25%
- Final exam: 30%

All assignments, quizzes and exams will be curved using the Standardize function in Excel. It takes into account the average and standard deviation. Very roughly, the average corresponds to the middle of Bs, and the students whose overall score is 0.5 standard deviations higher than the average will receive an A. *Often*, this system is equivalent to **roughly** the following:

- A: 81-100%
- B: 61-80%
- C: 41-60%
- D: 21-40%
- F: 0-20%

However, these are **not** precise cut-offs. The exact grade assignments for your class are within discretion of the instructor. 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.

To avoid problems with due dates, you can configure Canvas so that all deadlines reflect your local timezone. To do so, you should go to Canvas > Settings > Edit Settings and Time Zone and select your local time zone. Assignments must be submitted via Canvas by the indicated due date and time. **No late homework is accepted, but the lowest homework score will be dropped.**

Solutions will be provided quickly after each assignment is due. You may not get the solutions for the final exam. Your solutions will typically be graded within 2-3 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. Please keep in mind that, if the re-grading reveals issues that the TA had initially missed, this may result in a *lower* grade.

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 to find solutions, unless stated otherwise.

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.

Sending assignments (homework, quizzes, exams etc.), whether early, on time, or late directly to the instructor or TAs is not permitted and will not be accepted.

QUIZZES

The quizzes have to be taken by the end of the week they are assigned. They 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).

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. 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.

COURSE SCHEDULE

Week	Lessons and Assignments / Deliverables Due
1 Aug 22-28	M1: *Course introduction. Symmetric encryption overview. The One Time Pad. Perfect and Shannon secrecy and their limitations. Security and optimality of the OTP.*
	Homework 1 released.
2 Aug 29-Sep 4	M2: *Blockcipher modes of operation. IND-CPA definition. How to prove insecurity. (L1-17)*
	Quiz 1.
Sep 4	**Homework 1 due.**
Sep 5	Labor Day
3 Sep 6-11	M2: *ECB insecurity (L18-end).* M3: *Blockciphers, PRF definition.*
	Quiz 2. Homework 2 released.
4 Sep 12-18	M4: *How to prove security by reduction. Proof of IND-CPA security of CTRC. IND-CCA definition and IND-CCA insecurity of encryption modes.*
	Quiz 3.
Sep 18	**Homework 2 due.**
5 Sep 19-25	M5: *MACs and their security.* M6: *Hash functions and their security. HMAC.*
	Quiz 4. Homework 3 released.
6 Sep 26-Oct 2	M7: *Authenticated encryption. INT-CTXT definition.*
	Quiz 5. Practice exam released.
Oct 2	**Homework 3 due.**
7 Oct 3-9	M8: *PRGs and stream ciphers.* M9: *Implementation issues.*
	Quiz 6. Homework 4 (Coding Assignment) released.
Oct 10	Practice exam discussed.
8 Oct 11-16	***Midterm Exam***
Oct 17-18	Fall Break
9 Oct 19-23	M10: *Intro to asymmetric encryption.* M11: *Basics of number theory (first half).*
	Quiz 7.

Oct 23	**Homework 4 due.**
10 Oct 24-30	M11: *Basics of number theory (second half)*.
	Quiz 8. Homework 5 released.
Oct 29	Withdrawal deadline.
11 Oct 31-Nov 6	M12: *DL, CDH, DDH.* M13: *ElGamal, Cramer Shoup encryption*.
	Quiz 9.
Nov 6	**Homework 5 due.**
12 Nov 7-13	M14: *RSA function and encryption.* M15: *Hybrid encryption.* M16: *Multi-user encryption*.
	Quiz 10. Homework 6 released.
13 Nov 14-20	M17: *Digital signatures. FDH-RSA. DL-based signatures. Signature variants. Signcryption.*
	Quiz 11.
14 Nov 21-25	Thanksgiving Break
Nov 27	**Homework 6 due.**
15 Nov 28-Dec 4	M18: *Secret Key sharing. Key exchange, TLS. PKI, theory-practice gap*.
	Quiz 12. Practice final exam released.
Dec 5	Practice final exam discussed.
Dec 8-11	***Final Exam***