Course Information

Welcome to CS 302.

This course presents an in-depth study of cryptography and its applications to information and computer security. Privacy and security are central to our emerging "information society", and cryptography is a key technology for achieving them; it is also a fascinating field of study in its own right.

Cryptography lies at the center of this course, but we will be approaching the subject broadly. On the one end, we'll look at problems of computer and information security and see how cryptographic tools can be used to solve them. We'll also touch on some social issues surrounding the use of cryptography. At the other end, we'll explore the mathematical structures from which cryptographic primitives are built, and learn how to use some of these techniques in real-world scenarios.

This handout describes basic course information and policies. Most of the sections will be useful throughout the course. The main items to pay attention to **NOW** are:

- ◇ Make sure you are signed up properly on the Ashoka LMS.
- ◇ Join the Piazza forum for the class.
  `piazza.com/ashoka.edu.in/spring2019/cs302`
- ◇ Add this course on gradescope using the code 9WB58J to submit assignments.
- ◇ Please note, and carefully adhere to, the collaboration policy for homework.

1 Course Website

We will be using Gradescope to submit and grade assignments, and Piazza to post course material, answer questions, and for announcements, such as changes to office hours. The LMS website will also be used for some announcements.

2 Staff

The lecturer for this course is Debayan Gupta (`debayan.gupta@ashoka.edu.in`).

We also have two amazing teaching assistants:
Barun Parruck (`barun.parruck_ug19@ashoka.edu.in`)
Rachit Rawat (`rachit.rawat_ugta@ashoka.edu.in`)

3 Prerequisites

Some computer science background and basic programming skills are required. Ideally, you should have taken: Introduction to Computer Programming, Computer Networks, Discrete Mathematics, Probability and Statistics. I will not impose hard pre-reqs, but if you feel you don't have the background and still want to take the course, you should get in touch with me.

4 Lectures and Recitations

Lectures will be held in room **AC01-104 (LR)** from 10:10 A.M. to 11:40 P.M. on Tuesdays and Thursdays. You are responsible for material presented in lectures, including oral comments made by the lecturers. While we will post lecture notes that will be helpful in the event of an unavoidable absence, the notes are meant to augment lecture attendance, not replace it. They may be one-hour recitation sections held on specific topics from time to time. You are responsible for material presented in recitations.

5 Problem Sets

Problem sets will be assigned throughout the semester. We expect to have one problem set every two weeks at the beginning of the semester, progressing to one every week towards the end, as we move into more interesting and complex material. Overall, we

shall probably have around 7 problem sets. The due date will always be written on the problem set itself. Homework must be turned in by 10:00 P.M. on the due date.

- **Late submissions:** We will not usually allow late submissions unless there are major extenuating circumstances, such as a medical issue.

  The only way to submit late is to email your solution to a TA and cc the instructor. We will sometimes allow small (read: 30 min) delays, but we intend to keep an eye out for habitual offenders and may reject such submissions out of hand.

- **Discount Policy:** Your lowest homework score will be ignored.

- **Office Hours:** There will be no office hours on the day a problem set is due.

- **Submission Format:** Solutions to written parts of the problem set should be submitted online to gradescope in a single PDF file. **Your file must be in PDF format prepared in LaTeX using the template provided.** If the file does not clearly indicate which parts the solutions refer to, or has parts missing, it is assumed that the student did not attempt that part of the problem. Therefore, before submitting, make sure all of your work is included in the PDF file.

  Start each question on a new page and mark the top of the page with the following: (1) your name, (2) the question number, and (3) the names of any people you worked with on the problem (see Section 9), or "Collaborators: none" if you solved the problem entirely by yourself.

  The problem sets may include exercises that should be solved but not handed in. These questions will be clearly marked and are intended to help you master the course material. Material covered in exercises will be tested on exams.

- **Regrade Requests:** Any student who feels that a problem set was not graded properly may submit a regrade request through Gradescope within one week of the graded assignment being returned to the student. Please note the following before submitting a regrade request:

  1. You should carefully read the posted solutions for the problem in question.
  2. Indicate which rubric items you deserve (if applicable), where in your solution write-up you address them, and explain why you deserve extra points. Any regrades without justification will not be processed.
  3. The course staff reserves the right to regrade the entire assignment, and your grade may increase or decrease as a result of a regrade.
  4. **Important:** Lots of requests from the same person (hoping to somehow get extra points) and nonsensical requests will be dealt with harshly. This sort of thing wastes the time of the course staff and means that we can't help other students who might actually need it.

If you are still unsatisfied with your grade after the regrade, please email Debayan.

6 On the Importance of Clarity

You should be as clear and precise as possible in your write-up of solutions. Understandability of your answer is as desirable as correctness, because communication of technical material is an important skill.

A simple, direct analysis is worth more points than a convoluted one, both because it is simpler and less prone to error, and because it is easier to read and understand. Sloppy answers will receive fewer points, even if they are correct, so make sure that your solutions are concise and well thought-out.

Sometimes, you will be asked to "give an algorithm" to solve a certain problem. Your write-up should take the form of a short essay. A topic paragraph should summarize the problem you are solving and what your results are. The body of your essay should provide the following:

1. A description of the algorithm in English and, if helpful, pseudocode.
2. A proof (or indication) of the correctness of the algorithm.
3. An analysis of the asymptotic running time behavior of the algorithm.
4. Optionally, you may find it useful to include a worked example or diagram to show more precisely how your algorithm works.

Remember, your goal is to communicate. Graders will be instructed to take off points for convoluted and obtuse descriptions.

7 Exams

This course will have a midterm and a final exam:

Midterm: 1.5 hours, in class, mid-March

Final Exam: 3 hours during Final Exam Week (scheduled by the Registrar)

The midterm and the final exam will be closed book. However, **you will be allowed to bring and use one double-sided, letter-sized piece of paper with your own notes for the first quiz, and two for the final**. These should not be necessary but might be helpful.

Attendance at the exams is mandatory. Legitimate conflicts can be discussed with the teaching staff but must be due to extenuating circumstances and discussed in advance. If a student misses either exam due to an emergency, make-up exams may be offered at the discretion of the instructor.

Please note that scheduling an interview on the day of an exam is not a valid excuse for a make-up.

Regrade requests. Any student who feels that a quiz or final exam was not graded properly may submit a regrade request. The request must be made online by the announced deadline. The request should include a detailed explanation of why she or he believes that a regrade is warranted. Please make sure you read the solutions carefully before requesting a regrade.

8 Grading Policy

The final grade will be calculated as follows:

Midterm	30%
Homework	30%
Final exam	40%

9 Collaboration Policy

We encourage you to collaborate with your peers to deepen your understanding of the course material. However, you should approach collaboration *on problem sets only* with care, and follow the guidelines below. **Copying from online resources, books, or notes from previous versions of this or other classes is strictly forbidden — copying will be considered a serious offense and dealt with accordingly.**

1. **You should spend at least 30–45 minutes trying to solve each problem entirely by yourself.** If you find yourself unable to solve the problem, you can seek help, either by approaching the TAs, or by using Piazza, or by collaborating with your peers.

2. **Do not be a Spoiler.** If you already solved the problem, do not give away the answer to your friend. The best way you can help your friend is to give hints and allow her or him the pleasure of coming up with the answer her/himself. Our past experience has overwhelmingly shown that students who do not attempt the problem sets on their own generally perform poorly on the exams, and thus in the class overall.

3. **You must write up each problem solution entirely by yourself without assistance,** even if you collaborate with others to solve the problem. Doing otherwise will be considered plagiarism, an academic offense with serious repercussions. You are asked on problem sets to identify your collaborators. If you did not work with anyone, you should write "Collaborators: none."

   It is a serious violation of this policy to submit a problem solution that you cannot orally explain to a member of the course staff. Plagiarism and other dishonest behavior cannot be tolerated in any academic environment that prides itself on individual accomplishment.

If you have any questions about the collaboration policy, or if you feel that you may have violated the policy, please talk to one of the course staff. Although the course staff is obligated to deal with cheating appropriately, we are far more understanding and lenient if we find out from the transgressor himself or herself rather than from a third party or on our own.

Needless to say, **no collaboration whatsoever is permitted on quizzes or exams.**

10 Textbook

We will not use any textbook for this course. The internet is your friend.

11 Advice and resources for effective learning

Because of the conceptual nature of the material, just attending lectures and doing the homework are unlikely to be sufficient for learning all the concepts. **Setting aside time to do the reading and to study your notes from lecture and recitation is generally necessary to truly learn and internalize the material**, and to be able to apply it in new ways later in the course as well as for the rest of your life.

Homework is essential for learning the material. Rather than thinking of problem sets as just a requirement, recognize them as an excellent means for learning the material, and for building upon it. Spread out the time you have to work the problems. Many people learn best by reading the problems long before they are due, and working on them over the course of a whole week; they find that their minds make progress working the problems in the background or during downtime throughout the day. Few people do their best learning the night before an assignment is due. Work with others if that is helpful, but with the goal of learning first and solving the problems second. **It is worth reading the posted homework solutions, even if you received full credit**. Often the

clarity of explanation or details of implementation are different from the way you were thinking about things in ways that can improve your learning.

Don't hesitate to ask for help. This class is largely conceptual, and the concepts tend to build on one another. **If you are having trouble understanding the material, it is important to catch up rather than risk falling further behind**. We can help.

Office hours are a particularly useful mechanism for learning material and working through difficulties on problem set assignments. Moreover, if you have questions about the course or problem sets, please use Piazza as opposed to emailing an individual TA or lecturer—that will give you a better chance of getting a speedy response.

This class has great material, so HAVE FUN!