Course Information

Lectures: Tu, Th 3:30pm–4:50pm, CSB 002.

Discussion: M 4:00pm–4:50pm, CSB 002.

Canvas: https://canvas.ucsd.edu/courses/39753

Gradescope: https://www.gradescope.com/courses/439782 Integrated with Canvas and you are automatically enrolled via Canvas.

Piazza: Integrated with Canvas and you are automatically enrolled via Canvas.

Quizzes: October 13, 2022; November 3, 2022; November 29, 2022. In class.

Final Exam: December 5, 2022, 3pm–6pm.

Pre-requisites: CSE 21, 101, 105.

Staff:

Position	Name	E-Mail	Office
Instructor	Mihir Bellare	mihir@eng.ucsd.edu	CSE 4244
TA	Rishabh Ranjan	riranjan@ucsd.edu	
TA	James Yuan	z2yuan@ucsd.edu	
Tutor	Shravan Konduru	skonduru@ucsd.edu	

Office hours: See Canvas.

Waitlist and enrollment: Moving from the waitlist into the class, and being added to Canvas, are done by automatic university processes. The instructor has no control over these, and cannot add students to Canvas or move them from the waitlist into the class. Canvas is expected to automatically add you to the Canvas class 24hrs after you add yourself to the class list or waitlist.

Certification of commencement of academic activity: (#FinAid) The Affirmation quiz on Canvas also functions as the #FinAid certification. Complete as soon as possible, but no later than the Canvas due date.

Course content: This course is an introduction to modern cryptography. Cryptography, broadly

speaking, is about communicating or computing in the presence of an adversary. Core goals include preservation of privacy and integrity of communicated data. We will cover symmetric (aka. private key) and asymmetric (aka. public key) cryptography, including block ciphers, symmetric encryption, hash functions, message authentication, authenticated encryption, asymmetric encryption, digital signatures, RSA and discrete-logarithm-based systems, certificates, public-key infrastructure, key distribution, and various applications and protocols including commitment and secure computation. The course will emphasize rigorous mathematical formulations of security goals in the style of "provable security," and aim to train students in spotting weaknesses in schemes.

Grade determination: The course grade is based on homeworks (also called problem sets) and exams (three quizzes and a final). Denoting your percentage scores on these as P,Q1,Q2,Q3,F, we compute your total score TS via

$$\text{TS} \quad = \quad \frac{10}{100} \cdot \text{P} + \frac{17}{100} \cdot (\text{Q1} + \text{Q2} + \text{Q3}) + \frac{39}{100} \cdot \text{F} \; .$$

Now let us explain. In computing the total score, homeworks weigh 10%. Each quiz weighs 17%, so that quizzes are 51% overall. The final exam is 39%. In determining H, Homeworks are weighted according to their maximum scores, not equally.

We do not at this time give a fixed correspondence of total scores to grades. Grade cutoffs for individual quiz scores will be posted, showing what range of scores corresponds to what grade for that particular quiz. This serves to give an indication of where you are. If you are not sure how you are doing, ask!

The grade is reflective of the curve, but not entirely determined by it. That is, statistics such as the average or standard deviation influence, but do not fully define, the grade cutoffs.

Quiz, Final Exam and Homework rules: Exams (this means quizzes and final) are in-person, in class. They are "open allowed materiel." This means you may bring with you, to the exam, the allowed materiel. The allowed materiel is the course slides, and nothing else. Thus, what you may bring with you to class is hardcopies of the slides. (These will be handed out, and are also on Canvas.) It is OK if you scribbled a few notes on them as long as this was done during lecture, but your slides should not be annotated beyond that. Nothing beyond the slides is allowed. In particular you may not bring homework solutions (either your own or the ones handed out in class). You are also not allowed to bring electronic devices such as a cellphone, calculator, computer, or tablet. You will write answers on the provided exam sheets.

Sometimes health or other emergencies result in missing a quiz. In that case, contact the instructor with an appropriate justification. Arrangements will then be made to shift the weight of the quiz to the final. (Makeup exams will not be available.)

You may discuss the homework problem sets with other students in the class, but in groups of size no more than two. However, you must write your code and solutions on your own, in your own words. If you have worked with someone on a particular problem, indicate the name of your collaborator in your solution. (Working with a partner does not impact your score, so take advantage!) It is forbidden to discuss a homework with a person other than your partner or a course staff member, whether this be a student currently in the class or a non-student.

In doing homeworks, you are forbidden from referring to any resources other than those on Canvas.

In particular, you are not allowed to use materiel from previous years of this course, and you are not allowed to use the Internet to find solutions.

Regrades: Before you make a regrade request, look at the solutions, and also at the grading policies below. Then, if you still want a regrade, contact a TA. A regrade request for a quiz is only accepted up to two weeks after the quiz has been graded.

Grading policies: The problems are mathematical. We seek clear, logical mathematical arguments. Be neat and precise. It is not (just) a question of getting the "right answer"; the number of points you get will also depend on the quality of mathematical writing.

Read through whatever you write before submitting it. Try to make sure there is an argument with a clear flow. If your answer says lots of different things, you are *not* going to get points just because one of them is right; indeed, you will get *less* points for a jumble which sort of includes something right than for something clear even if not the entire answer.

The grader expects to be able to make sense of what is written without too much time or effort. Strive to write in such a way that what you mean is clear the first time it is read.

Practice problems: Practice problems for quizzes and exams can be found as exercises in the slides and lectures. Solutions to these will not be posted, but you can check your answers with course staff via private Piazza posts.

Organization: Lectures and Discussion are in-person, in class. Lectures are podcast for later viewing. Canvas is the main off-line resource, with Piazza and Gradescope as auxiliary resources. On Canvas, the content is divided into modules. In each module, you will find copies of the slides. There is a Problem Set / Homework module. Homeworks use `PlayCrypt`, a Python-based system in which you will create attacks.

Communication: Announcements, such as availability of a homework, updates or corrections, may be made on Canvas and/or Piazza. You can likewise communicate with the instructors, TAs and other students using Piazza. Please strive to keep communication polite. If you have questions or concerns, including with regard to your performance or grade, contact course staff via private Piazza posts rather than public posts.

Academic integrity: Above, we indicated numerous rules for both exams and homeworks. Cheating, including deviation from these rules or from general rules of academic conduct such as described in the UCSD Policy on Integrity of Scholarship, will be taken very seriously. Academic dishonest cases are prosecuted by the university and can result in probation or dismissal.

How to do well in CSE 107: Some students operate in a mode I call random access. You look at the homework (perhaps just before it is due), see that you don't know how to do it, then scan through the slides to see if you can spot some example that looks similar, and try to use that. If, that fails, you might ask for help, saying you do not know how to do the homework.

This random access mode of operation has limited success. Here's the better alternative, which I call sequential access. There is a homework due. Ignore it. Instead, read the slides, for the chapter

in question, sequentially, beginning to end, and make sure you understand everything there. If necessary or helpful, review the lecture podcast. If you don't understand something, ask for help. Once you have understand everything, do the homework. It will feel a lot easier.

What's the difference? If you look at the homework and try to map back to the materiel, your mapping will be imperfect at best. The understanding needed may not be the obvious one. And an example cannot be understood in isolation. In the sequential mode, you aim to understand the materiel as a coherent whole. It pays off.

Random access mode may also reduce success on quizzes. You may think that because quizzes are open course materials, you can look up solutions in the slides in the same random access way as for homework, scanning for an example that matches the problem. This may not work well. But if you have studied prior to the quiz, attended lecture or watched the podcasts, and read the slides sequentially and understood them, then you will find the quiz quite accessible, and may not even need to look at the slides during the quiz.

Some students have the view that the problem is out there, not in here. The grading is too harsh, the course is too hard, and so on. This view impedes your progress. A better view is that the grading and class are what they are; how do I learn and adapt to do well? When you have that view, you will often make progress and do better.

Students who do well in CSE 107 are typically not assessment and grade oriented. They have a genuine interest in the materiel and in learning. They enjoy challenges. They do not give up easily in the face of setbacks. They like to understand things, even things not on the homework and quizzes.

Set a high bar. Students who enter with the goal of only wanting to pass may find that they struggle to do so. Students who enter wanting an A and willing to work for it may find that they get it.

The materiel is theoretical, and a good performance in CSE 105 helps to succeed in CSE 107.