Course Information

Lectures: Videos on Canvas.

Discussion: Tu 1:00–1:50, Zoom. Link is posted on Canvas.

Staff:

Position	Name	E-Mail
Instructor	Mihir Bellare	mihir@eng.ucsd.edu
TA	Hannah Davis	h3davis@eng.ucsd.edu
TA	Wei Dai	weidai@eng.ucsd.edu
Tutor	Zijing Di	zidi@ucsd.edu

Course Web Page: `http://cseweb.ucsd.edu/~mihir/cse107/index.html` and `https://canvas.ucsd.edu/courses/18846`. Lecture videos and slides can be found here.

Office hours: See Canvas.

Piazza: Being on the class Piazza `piazza.com/ucsd/fall2020/cse107` is mandatory. Announcements may be made on Canvas and/or Piazza.

Course content: This course is an introduction to modern cryptography. Cryptography, broadly speaking, is about communicating in the presence of an adversary, with goals like 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 designs.

This is not a computer-security course. We will *not* cover topics like malware, operating systems security, or browser security. (The techniques we develop have some applications in such areas, but these areas are not touched upon directly.)

Pre-requisites: CSE 21, 101, 105.

Should I take this course? This is generally regarded by students as a challenging course. It is theoretical and mathematical in nature, and calls for ability to understand abstract concepts. The

grading standards are high. The drop rate is usually high. Take 107 if you are strong at theory and math.

If you have a grade lower than a B- in CSE 105 or CSE 101, I would gently suggest that you reconsider taking CSE 107. In the past, students with grades lower than B- in 105 or 101 have usually ended up either dropping 107 or got an F.

If you are not doing well, it does not necessarily mean there is something wrong with the class, or with you. It may just mean that this is not a good match for you. See it in a positive way, as a hint to move on and find better matches. It may help to make that choice quickly, rather than wait and hope things get better.

Grade determination: The course grade is based on homeworks (also called problem sets), quizzes and a final exam. Denote your percentage scores on these as H,Q,F, respectively. In determining H, homeworks are weighted according to their maximum scores, not equally, and analogously for Q, and, in both categories, the lowest one is dropped.

We compute your raw score RS, and associated total score TS, via:

$$\begin{aligned} \text{RS} &= \frac{15}{100} \cdot \text{H} + \frac{60}{100} \cdot \text{Q} + \frac{25}{100} \cdot \text{F} \\ \text{TS} &= \frac{90}{100} \cdot \text{RS} + \frac{10}{100} \cdot \text{DS} \, , \end{aligned}$$

where DS is your discretionary score, to be explained. In computing the raw score, homeworks weigh 15%, quizzes 60% and the final exam 25%. Your total score is 90% your raw score RS and 10% your discretionary score DS. Your grade is determined by TS.

How is DS computed? Its default value is RS. Thus, if you do nothing to either increase or decrease it (which is likely true for most students), then TS is just RS. However it is possible to increase DS, and also possible to decrease it, relative to its default value RS. Actions that may increase your discretionary score DS above RS include answering Piazza posts by other students, creating positive impressions through interactions or posts, spotting mistakes or bugs in what we post. Actions that may decrease your discretionary score DS below RS include extraneous communications (Piazza or direct, see below), requesting exceptions to stated policies, asking administrative questions that are already answered, requesting actions already denied by policies, asking for special consideration.

We do not at this time give a fixed correspondence of scores to grades. Grade cutoffs for quiz scores will be posted, showing what range of scores corresponds to what grade for that quiz.

The grading is reflective of the curve, but not determined by it. That is, the grade distribution is not fully determined by statistics such as the average or standard deviation, but is influenced by it.

As per university rules, a P means a C- or above.

Quiz, Final Exam and Homework rules: All exams (exam means either a quiz or the final exam) are "open allowed materiel." The allowed materiel is the course materiel on Canvas and nothing else. Quizzes are available within a certain window, and have a certain time limit, that will be indicated and can vary across quizzes.

There are no makeup exams. We understand that you may miss a quiz. The first time this happens,

it is considered covered by the policy of dropping the lowest quiz score. Beyond that, if health issues result in missing quizzes, let the instructor know, and the weight of the quiz will be moved to the final.

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. 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 what is 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.

Grading policies: The problems are mathematical, and involve proving things. You should write 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 is not responsible for spending lots of time to decipher your solutions. If what you write does not make sense to a grader in a small amount of time, you will lose points. It will not help to come back later and explain what you meant. You are expected to write in such a way that what you mean is clear the first time it is read.

Regrades: Request quiz regrades on Canvas. (Do not post on Piazza; Canvas will let us know if you have made a request.) You are allowed a total of two quiz regrade requests across the quarter, and at most one per quiz. (The latter means that if you got a regrade on a quiz, you cannot request another one.) A regrade request for a quiz is only accepted up to one week after the quiz has been graded. Before you make a regrade request, look at the solutions, look at the grading policies above, keep in mind that the grading standards are high and keep in mind that you have a limited number of regrades and may not want to exhaust them too soon.

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 instructors via private Piazza posts.

Organization: This version of the class is fully online. Canvas is the main resource, with Piazza and Gradescrope as auxiliary resources. On Canvas, the content is divided into modules. In each module, you will find lecture videos and copies of the slides. Problem sets and quizzes are usually one per module, but sometimes two modules will be covered together. The Syllabus section indicates what videos to watch by when. Lectures will not be given at class time. Instead, you may watch videos whenever you like, at your own pace, subject to completing the indicated quota. Discussion sections and office hours will be on Zoom. Their times will be announced.

As a default, Zoom meetings will turn off your video and mute your microphone when you join. If you want to say or ask something (encouraged!) you have two options. One is to use the raise-hand feature in Zoom. Then, the host(s) will unmute you and turn on your video. The other is to use the Zoom chat. The hosts will try to monitor this, and respond verbally to questions on it.

Communication and behavior: You communicate with the instructors, TAs and other students in many ways. This includes Piazza posts (public or private), emails, Canvas communications and possibly more. Please confine communications to course materiel and keep them polite and appropriate in content. If you are worried about your performance or grade, contact course staff privately rather than do public posts.

We welcome corrections, like pointing out mistakes we have made, or bugs in questions or code.

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.

With online exams, it is tempting to get help from friends, or to use the Internet to find solutions. We have various measures in place to test for this. We encourage students to follow the rules and avoid difficulties.

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 is not likely to work well. Here's the alternative, which I call sequential access. There is a homework due. Ignore it. Instead, watch the videos, and read the slides, for the chapter in question, sequentially, beginning to end, and make sure you understand everything there. If you don't, 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 will also leave you lost 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 will not work well. But if you have studied prior to the quiz, watched the videos 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.

Students who enter with the goal of only wanting to pass may find that they do not do so. Students who enter wanting an A and willing to work for it may find that they get it.