Course Information

Lectures: M, W and F, 10:00–10:50AM in CENTR 216.

Discussion: W 4:00–4:50 in CENTR 113.

Staff:

Position	Name	E-Mail
Instructor	Mihir Bellare	mihir@eng.ucsd.edu
TA	Wei Dai	weidai@eng.ucsd.edu
TA	Igors Stepanovs	istepano@eng.ucsd.edu

Course Web Page: `http://cseweb.ucsd.edu/~mihir/cse107/`. This contains copies of the slides.

Office hours: See course web page.

Piazza: Being on the class Piazza `piazza.com/ucsd/fall2018/cse107` is mandatory. Homework announcements will be made here. You are limited to three posts per 24h day. (Answering other students' questions does not count.)

Pre-requisites: CSE 21, 101, 105.

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.)

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 successful student has typically done well (B- or better) in CSE 21, 101 and 105.

Sources of material: The main source of material is the lectures, and the course syllabus and content is determined by the lecture slides, which will be handed out in class and also put on the webpage. There is no textbook. Lecture podcasts are available via `podcast.ucsd.edu`.

Interaction: Use Piazza or Office Hours to interact rather than send direct emails to instructors. Strive to communicate clearly. If your communications and questions (on Piazza or in Office Hours) are not mathematically well-formed, we may simply say so and stop there. Since you are limited to 3 Piazza posts per day (as above, answers to questions by other students do not count in your quota), it is to your advantage to formulate queries carefully and precisely.

The purpose of Office Hours and Piazza is to help understand the materiel, not to help solve homework problems.

Quizzes and final exam: Quizzes are held in Discussion section, making Discussion section mandatory. There will be 6–8 quizzes over the quarter. There will be no quiz on October 3rd. For all other Discussion sections, there will be a quiz unless otherwise indicated.

The final exam is on Friday December 14, 2018, 8am to 11am.

Exams (this term covers both quizzes and final in what follows) are "open allowed materiel." The allowed materiel is the slides, and nothing else. Thus you may bring with you hardcopies of the slides that were handed out and are also on the webpage. 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.

There are no makeup exams under any circumstances whatsoever. The only acceptable reason to miss a quiz is that the student has a personal health problem at the time and can provide the instructor with adequate documentation to verify this. For a student with such a medical excuse, arrangements will be made to shift the weight of the quiz to the final. (A score on the quiz will be calculated as a mean-preserving function of the score on the final.) The final is mandatory. If you do not take it, you get a zero on it.

Grade determination: The course grade is based on homeworks (also called problem sets), the quizzes and a final exam. Denoting your percentage scores on these as P,Q,F, we compute your raw score RS and total score TS via

$$\begin{aligned} \mathrm{RS} &= \frac{10}{100}\cdot \mathrm{P} + \frac{45}{100}\cdot \mathrm{Q} + \frac{45}{100}\cdot \mathrm{F} \\ \mathrm{TS} &= \frac{90}{100}\cdot \mathrm{RS} + \frac{10}{100}\cdot \mathrm{DS}\,, \end{aligned}$$

where DS is your discretionary score, to be explained. Your grade is determined by your total score TS. Now let us explain. In computing the raw score, homeworks weigh 10%, quizzes 45% and the final exam 45%. In determining P, problem sets are weighted according to their maximum scores, not equally. Your total score is 90% your raw score RS and 10% your discretionary score DS. 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 participation in class or discussion, answering Piazza posts by other students, or impressing instructors in personal interactions. Actions that may decrease your discretionary score DS below RS include requesting exceptions to policies stated here or on the slides, asking administrative questions already answered here or on the slides, requesting actions already denied by policies here on the slides and asking for special consideration. The latter includes asking that your grade depend on things beyond your performance. An example is "Please pass me because I am graduating this quarter." This is not appropriate because it is effectively asking for unfairness, that you be treated differently from other students.

The class is *not* graded on a curve. There is no fixed correspondence between letter grades and particular scores, nor is the grade distribution dependent in some fixed way on statistics such as the average or standard deviation.

Homeworks: 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 your own course notes, the class notes, and solutions to past homeworks or quizzes from this class. In particular, you are not allowed to consult books. 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.

Solution sets: Solution sets will be handed out for both homeworks and exams. You are encouraged to read them even if you got the problem right, and definitely if you did not. They tell you not only how to solve the problem but how to formulate your answers, something which influences your score. They will not be posted online.

Grading policies: Some of the problems (on problem sets or exams) will involve proving things. You must 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 turning it in. Try to make sure there is an argument with a clear flow. If you paper 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.

Write top to bottom, left to right on the page, because that is how people read. Don't scatter information all over. If you do, you lose points.

Be as concise as possible.

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 be penalized. 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 and return of graded material: The final exam is not returned. You can see it by request in the first week of the subsequent quarter, and request a regrade at that time, but you cannot take the graded exam with you.

Homework and exam scores may be viewed via `http://www.gradesource.com`. You will be able to see statistics and ranking. Your own scores will be identified by a secret 4 digit number that will be emailed to you some time in the quarter. The email address used for you will be the one on Blink.

If you feel that you were mis-graded on anything, first look at the solutions. If you still feel you were mis-graded, contact the person who graded the problem in question. (This will be indicated on the webpage.) Regrade requests, however, will only be accepted up to one week after the graded item in question is returned.

Academic honesty: 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.

Students sometimes try to modify their graded exams or homeworks after they are returned, and then bring them back to us for regrades, thinking we won't notice that they have been modified. We might make copies of graded exams before returning them, and you would be surprised how well a grader can remember a single answer across several hundred in any case. Students have been caught doing this and reported. Don't modify your exam or homeworks after they are handed back. Also don't copy from others during exams or bring in un-allowed materials. Finally, don't use materiel from previous years of this course. Most importantly, don't use the Internet to find solutions. Don't search for solutions to homework problems on the Internet or use websites that archive solutions.

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, 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 book, 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, 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 feel the way they understand is through examples, and ask for more examples. You need to understand the theory, meaning the definitions, not just the examples. Examples can only illustrate and no example or number of examples conveys a full understanding of the theory. Limit your requests for more examples.

Some students want a recipe for success. One hears: "I am willing to work but I don't know what to do in this class to be successful." There is no recipe we will give, and none that works for all students. It is part of the learning process and challenge to figure out what works for you and how to be successful.

Do make use of instructor and TA office hours to ask questions. But here's one lesson. The students who do well are ones who ask questions about the slides and lecture materiel, not about the homework. If you have trouble with homework, trace it back to something you don't understand in the slides, and ask about the latter.

If you feel that you understand lecture materiel and the slides but can't do the homework, you have created a contradiction. If you can't do the homework, then, by definition, you do *not* understand lecture and slide materiel. Adopting the attitude that you do understand but cannot do the homework is unproductive. It makes it harder for you to help yourself, and makes it harder for us to help you. Instead, if you can't do a homework, draw the conclusion that you actually don't understand the materiel, even if you think you did. Then, try to pin-point what you do not understand, for example that you lose it at this particular point in the slides. This is better because now you know what you have to do and where you can get help.

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.