

## CSE 107 Course Information

**Lectures:** M and W, 9:30–10:50AM in EBU3B 2154.

**Discussion:** M, 1:00–1:50PM in WLH 2113.

**Staff:**

POSITION	NAME	E-MAIL
Instructor	Mihir Bellare	mihir@eng.ucsd.edu
TA	Sriram Keelveedhi	skeelvee@eng.ucsd.edu

**Course Web Page:** <http://cseweb.ucsd.edu/~mihir/cse107/>. This is the *only* source of all course related handouts such as problem sets, problem set solutions, exam solutions, and notes. Hardcopies of these items will not be distributed. It is your responsibility to configure your computing environment to use the web page.

**Office hours:** See course web page for instructor office hours.

**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, modes of operation, hash functions, digital signatures, asymmetric encryption, RSA, the discrete logarithm problem, public-key infrastructure, key distribution, and various applications. 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 viruses, worms, operating systems security, or security holes in windows or linux. (The techniques we develop have some applications in such areas, but these areas are not touched upon directly.)

This is generally regarded by UCSD undergraduates 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 in CSE 21, 101 and 105.

**Sources of material:** The main source of material is the lectures. There is no textbook. I will provide copies of the lecture slides. I will also attempt to provide course notes (also called class notes) for as much as possible of the lecture material, but this is not a guarantee.

**Office hours, email:** You are encouraged to make use of office hours to ask questions, get help, or otherwise talk about the materiel. You may also use email, but it is much harder to make yourself understood over email, with the result that at times you may be asked to come see a staff member instead.

**Assesments:** The course grade is based on homeworks (also called problem sets, 28% of the grade) and exams (two quizzes, each 18% of the grade, and a final exam, 36% of the grade). Additionally, participation in lectures will impact your grade on the margins.

Note that each homework will have a certain maximum number of points that can differ from homework to homework, and in computing the 28% of your score corresponding to homeworks, we take the sum of all your scores, divide by the sum of the maximum possible scores, and then multiply by 28. In other words, homeworks are weighted according to their maximum scores.

**Exam calendar:** The exam dates and locations are as follows:

EXAM	DATE & TIME	LOCATION
Quiz 1	W Feb 1, 9:30–10:50AM	EBU3B 2154
Quiz 2	M Feb 27, 9:30–10:50AM	EBU3B 2154
Final	W Mar 21, 8–11AM	EBU3B 2154

**Grade determination:** 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. It is possible for all students to get good grades, as for all students to get poor grades.

There will be no assignment or indication of letter grades corresponding to scores on individual assesments such as quizzes. (There is no meaningful way to assign a grade for a quiz. The final grade depends on all the scores, not some interpretation of them as grades.) However, a pass/fail cutoff score will be provided for each quiz. Anyone getting a score strictly less than the pass score on a particular quiz should be viewed as having received an F on that quiz. Various statistics will also be available.

**Exam rules:** Exams are “open-book.” What this means is that you may use *allowed materiels* during the exam. Allowed materiels means your own course notes, the lecture slides and the class notes that are on the web page, *but no other material*. Please note that you are *not* allowed to bring homeworks, your own solutions to them, the solution sets from the web page, or any books. You are *not* allowed to bring electronic devices such as a calculator, computer, cell-phone, iPod, iPad, or palm-pilot. (The exam may require some arithmetic computations, but these are designed to be done by hand.)

You will write answers on the provided exam sheets, and thus should not bring blue books, but you should bring scratch paper.

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. If there is any anticipable

reason for which you cannot take the final exam at the scheduled time, don't take the course. If you do not take the final, you get a zero on it.

If a student has been approved as having legitimately skipped a quiz, then the following procedure will be used in shifting the weight of the quiz to the final. If the student gets a score  $X$  on the final, a score  $Y$  will be computed as their score on the missed quiz, where  $Y$  is a function both of  $X$  and of the statistical parameters of the quiz and the final. That is, it is not necessarily true that  $Y = X$ ; rather, the computation adjusts for the relative difficulty of the two tests as measured by the curve on these tests. (For example, if  $X$  was the class average on the final, then  $Y$  will be set to the class average on the quiz.) The function itself is complex and cannot be detailed in advance.

**Homework Rules:** Homeworks will indicate the due date and place. Late homeworks will not be accepted.

Turn in neat, readable solutions. (Either handwritten or typeset.) If you have more than one sheet, they should be stapled together, not clipped or folded at the corner. If not, points will be deducted. If your name is not on your sheet, points will also be deducted.

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 solutions on your own, in your own words. If you have worked with someone on a particular problem, indicate the name of your collaborator on your solution sheet. 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. In particular, you are not allowed to consult books. You are not allowed to use material from previous years of this course, and you are not allowed to use the Internet to find solutions.

**Obtaining scores or grades, and return of graded material:** Graded homeworks and quizzes are returned in lecture. If you do not go there, you can pick them up outside EBU3B Room 4244 until the end of the last week of classes. After that, these items are discarded.

The final exam is not returned. You can see it during Final Exam Return Week in the CSE department next quarter, according to the calendar that the department will announce later. When you see it, you can file a regrade request if you like, 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.

You can obtain your final grade through Blink at whatever point in time this service makes grades available. (The final grade will not be on gradesource.) Public posting of grades is prohibited by UCSD, so no grade sheet will be posted for the class. Students are expected to obtain their grades directly via blink.

**Solution sets:** Solution sets will be posted on the web page for both problem sets 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.

**Grading policies:** Many 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 your 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.

For problem sets, first write a rough draft, then write a new, final draft to actually turn in. Think about it from the point of view of a grader: how are you making sure that person will understand?

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.

**Grade-related questions:** It is not possible to provide answers to questions such as the following during the course: “What scores do I have to get for the rest of this class in order to get such and such grade?” “What is the cutoff score for such and such a grade?” “What were the cutoff scores, or what was the grade distribution, in previous years the class was taught?”

Information about the distribution of grades in the class, and cutoff lines for different grades, will not be made public, or provided to a student.

**Appeals on scores or grades:** 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. (Any of us will typically be able to tell you who that is for a particular problem.) Such appeals, however, will *only be accepted up to two weeks after the graded item in question is returned*. So look at your returned stuff quick; if you wait too long, it will be too late to complain.

To talk to the course staff, use their office hours. If you cannot make the office hour, make an appointment. E-mail is usually a good way to do the latter.

The final exam is not returned. If you want to look at it you must come to the CSE department next quarter during final exam return week. (The CSE department will announce the times and locations for exam review later.) At that time you can review your exam and make a written report if you have any issues with it. If there are any changes to your grade, you will be contacted.

Sometimes students write to the instructor after receiving their final grades, requesting a meeting to discuss the grade. Don’t. No such meetings will be granted. Changes to your final grade can arise in only two ways. One is regrades, the policies for which are indicated above. Another is that there was a mistake in score entry. You are expected to check your scores via gradesource and, if

there is a mistake, bring to us the assesement in question showing the correct score so that the entry in gradesource can be changed.

**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 in the UCSD General Catalog, 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. You would be surprised how well a grader can remember a single answer across several hundred. 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.