Course Information

Meets: Tu and Th, 9:30AM–10:50AM in WLH 2206.

Course Web Page: `http://cseweb.ucsd.edu/~mihir/cse207`. Slides of lectures are available here.

Instructor: Mihir Bellare

Office: EBU3B 4244

E-mail: mihir@eng.ucsd.edu

TA: Igors Stepanovs

E-mail: istepano@eng.ucsd.edu

Office hours: See course web page.

Piazza: Being on the class Piazza `piazza.com/ucsd/fall2019/cse207/home` is mandatory since various announcements and updates could be made here.

GradeSource: `http://www.gradesource.com/reports/871/31176/` Here you can find your scores and class statistics.

Contents: This course is an introduction to modern cryptography. Topics include block ciphers, hash functions, pseudorandom functions, symmetric encryption, message authentication, RSA, asymmetric encryption, digital signatures, key distribution and protocols. We will introduce the "provable security" approach, defining security for various primitives and then proving that schemes achieve the defined goals. We adopt a "theory brought to practice" viewpoint, focusing on cryptographic primitives that are used in practice and showing how theory leads to higher-assurance real world cryptography.

This is *not* a computer security course. We will not be covering topics like operating systems security, browser security and malware.

Sources: There is no text that covers all the material of this course, and there is thus no prescribed or required text. The main source of materiel is lecture and the associated slides. The web page also has pointers to various books on the subject, parts of which might be useful references.

Pre-requisites and enrollment: The formal pre-requisites for this course for graduate students are

((CSE 202) AND (CSE 200 OR CSE 227)) OR CSE 107.

Recall CSE 202 is Algorithms, CSE 200 is Computability and Complexity, CSE 227 is Computer Security. For these, grade should be B+ or better. Undergraduate algorithms (CSE 101 or equivalent)

or theory (CSE 105 or equivalent) may be substituted for 202, 200, respectively, with grades of A- or better. CSE 107 is Undergraduate Cryptography and needs a grade of A- or better. In particular the needed background includes computer algorithms, probability theory, randomized algorithms, some basic complexity theory (eg. $\mathbf{P}, \mathbf{NP}$, $\mathbf{NP}$-completeness, reducibility between problems) and, most importantly, general "mathematical maturity." The latter means being comfortable and adept with mathematical language, definitions and proofs.

Since the registration system cannot check pre-requisites, all graduate students start on the wait list and I try to determine whether or not you meet the above pre-requisite condition. Those determined to do so will then receive a clearance email from the department, allowing them to enroll. If you feel you have the background but have not been cleared, send me email, with details on the courses you took and grades you got.

For undergraduate students, CSE 107 with an A- or better is a necessary but not sufficient condition to be allowed to enroll in CSE 207.

Assessments and grade determination: The course assessments are homeworks.

Denote your percentage score across all homeworks (in determining this, homeworks are weighted according to their maximum scores, not equally) by HS. Your total score is then $\text{TS} = 0.9 \cdot \text{HS} + 0.10 \cdot \text{DS}$ where DS is your discretionary score, to be explained. Your grade is determined by your total score TS.

How is DS computed? Its default value is HS. However it is possible to increase DS. Actions that may increase your discretionary score DS above HS include participation in class, answering Piazza posts by other students, or personal interactions. Try to ensure the instructor and TA know your name and have made a name-to-face association.

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.

A comprehensive exam may be offered if there are enough MS students who want to take it. It would be offered as the final exam of the course. It is a 3 hour, in class, exam, with a closed book segment (you cannot bring course materials, such as slides, homeworks and notes, with you) and an open book segment (slides permitted, but nothing else). Note that the comprehensive exam does not influence your course grade.

Rules and grading policies: Homeworks will be handed out in class. Solutions will be handed out in class as well. Neither will be made available electronically. Copies of the handouts will be available outside Room 4244 in case you don't get them in class, up to one week after the handout date.

Cheating, including failure to abide by the course rules, is taken very seriously. Academic dishonesty cases are prosecuted in conjunction with the Academic Integrity Office and can result in probation or dismissal. Students have been caught cheating in graduate courses in this department in the past, and have been so prosecuted.

The homeworks are "open allowed materiels." This means you may use the course slides, solutions to prior homeworks (both the ones handed out and your own), but *nothing else*. In particular you may not search the Internet for solutions, use materials from prior years of this course, or use books or papers in the academic literature. You may use the Internet, books and academic

papers for things that do not pertain directly to homework solution. This could be understanding course materiel and background. As an example, if, during a homework, you need to look up some mathematical fact or definition (algebra, combinatorics, probability), that is fine, since this does not relate directly to the homework solution. Late homeworks are not accepted.

Homeworks may be either individual or collaborative. The homework will indicate which is the case. Individual means you must work alone. Collaborative means you may work with at most one other student in the class, but must write your solutions on your own in your own words. (It is fine to change partners from one homework to another, but on a particular homework you can have at most one partner.) You may not consult with anyone other than your partner, the instructor or TA. You must name your partner on your solution.

Mathematical writing: This course involves mathematical abstraction and proofs. Being able to deal with these is one of the important things to learn. You will be graded based on the correctness, clarity and accuracy of mathematical exposition. Make sure what you write makes sense. Define notation before you use it. Answers that "don't make sense" will not get much credit. Your solutions should have a logical flow from beginning to end. Remember, you are graded on what you write, not on what you think you "meant." So make sure you write what you mean. Write top to bottom, left to right on the page. Don't scatter information all over. Be as concise as possible.

Mathematics is a language. Learn its grammar and semantics, and get used to using it correctly. Like any language, its goal is communication, and when properly used, it is a precise and unambiguous tool to this end. When you mis-use the language, you will not be understood, and you will lose points.

Read through whatever you write before turning it in. Try to make sure there is an argument with a clear flow. If your writeup 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 articles under *Mathematical and technical writing* available via `http://cseweb.ucsd.edu/~mihir/education.html` provide more information about mathematical exposition. You are encouraged to look at them.

If you want a re-grade, first look through the solutions. If you still want a re-regrade, see the instructor or TA. You will be expected to have read and understood the above mathematical writing criteria.