Meetings: Douglas Hall 212, Monday and Wednesday, 5:30 - 6:45pm.

Instructor: Ted Krovetz. Office: 5008 Riverside Hall. Email: tdk@csus.edu.

Office Hours: Monday and Wednesday 3:30 - 5:30pm. (Unofficial hours are listed at http://ical.krovetz.net, but check before coming because they occasionally get cancelled on short notice.)

The second and third books are optional. Reading will be assigned with the homework. You are responsible for all assigned reading.

Webpage: Handouts, homework assignments, solutions and score reporting will be available at the course webpage: http://gaia.ecs.csus.edu/~krovetz/courses/252/.


Goals: To give an appreciation of (i) the basic use and construction of cryptographic primitives, (ii) the complexity-theoretic assumptions made in their use, (iii) the fragility of secure network protocols, and (iv) experience using cryptography and cryptography toolkits in programming.

Prerequisite: Fully classified graduate status in Computer Science, Computer Engineering, or Software Engineering. (Or consent of the instructor.) You are expected to know the fundamentals of probability, network programming, proof methods and C or java programming.

Announcements, Questions and Feedback: Electronic communication will take place using an online forum at http://gaia.ecs.csus.edu/~krovetz/courses/forums. You are responsible for checking the “Announcements” forum at least once a week. The “Course Questions” forum is intended for students to ask questions about anything course related, including homework help. You are encouraged to read and answer other students’ questions. The only rule is not to give away solutions. You are also welcome to ask questions during office hours and class. If a question is of a personal nature, you may e-mail the instructor directly (other e-mail questions may be ignored, and so should be posted to the forums). The third forum is “Feedback”. Polite and constructive feedback about any aspect of the course is encouraged. This is a good way to influence how the course is taught. Any messages posted to the wrong forum will be silently deleted. You may use these forums anonymously by not logging in.

Waitlist: If warranted, a waitlist will be created during the first week. At the end of the first week, the people on the waitlist will be placed randomly into an ordered list. As space becomes available in the class, people present at lecture will be admitted to the course according to the random list. To remain on the waitlist, you must do all assigned work.

Homework: Homework will be assigned and solutions will be posted on the course webpage. A new assignment will appear shortly after each previous one is due. No late homework will be accepted. Most homework will not be graded and will not be handed-back quickly (so keep a copy if you want one). Come to office hours if you need help understanding the solutions. Homework solutions are a good study guide for quizzes and exams. Each student will make a 15 minute presentation at the end of the semester.

Many students dislike the fact that they are asked to do homework without knowing whether it will be graded. The following analogy might help. Imagine that your boss has asked you to have a well-written report of your group’s activities ready at each weekly staff meeting. Most weeks you will not be called upon to present your report, but sometimes you will. You doubtless would not complain to your boss that most of your reports do not see the light of day; you would instead strive to make sure that when it does, it is brilliant. The same should be the case for your homework. It is part of your job as a student to do it well and on time each week.
Unless stated otherwise on an assignment, you may solve the homework on your own or in groups, using whatever resources help you understand the problems, but each person must prepare written solutions on their own. No copying allowed, from any source. For each homework, please list any sources of help (eg, people, other texts, web sites, etc). Failure to do so will be considered plagiarism. The more work you complete on your own, the better your eventual grade will be.

Final Exam and Quizzes: You will learn the most in this class from doing and understanding the homework. To gauge how well you are understanding the homework, quizzes will be given which ask questions similar or related to those seen on the homework. Quizzes will be given every two to four weeks, with at least one week’s notice in the forums. There will be a final exam, but no midterm. The final will be held in the same room as the lectures at the time listed in the final exam schedule at http://www.csus.edu/webpages/schedule.htm. There will be no early or late makeup exams or quizzes (so do not ask).

No notes, books or calculators are allowed during quizzes unless notified otherwise. If paper or a Scantron sheet is ever needed, it will be stated in the forum announcement. One letter-sized double-sided sheet of hand-written notes will be allowed during the final exam.

Grading: Quizzes and homework will together be worth about 60% of your grade (with the mix depending on how many of each are graded), while the final is worth about 40%. To allow for a bad or missed day, your lowest quiz and lowest homework score will be dropped. Your grade will be calculated in several ways, the highest of which will be your assigned grade. A raw score will first be calculated based on a weighted average of your homework, quiz and exam scores.

Raw Percentage. Raw scores of 85% or higher get an A, 70% or higher get a B, 55% or higher get a C.

Class Rank. Raw scores in the top 10% of those completing the course (rounded to the nearest whole person) get an A, top 30% get a B, top 60% get a C. For example, if there were 22 people in the class, the top two people would be guaranteed an A.

Standard Deviation. Raw scores more than 1.5 standard deviations above the mean for those completing the course get an A, more than 0.5 standard deviations above the mean get a B, within 0.5 standard deviations above or below the mean get a C.

If the class is not large enough to have a statistically significant number of students, only the first two rules will be guaranteed. These are minimum grades. If a class does very well collectively, or the course material is advanced, higher grades may be given. Also, an F may (at the instructor’s discretion) be assigned to anyone getting fewer than half the available points in any of the grading categories (eg, quizzes, homework, final exam). D grades and +/- modifiers are not given.

Advice: If you wish to do well in this class try to do all of the following:

- Attend class. Although attendance is not mandatory, those who skip class usually do less well on homework, quizzes and exams.
- Ask and answer questions in class. One of the best ways to learn is through a dialogue guided by questions and answers. Questions are often asked of you in class – you should try to answer them. And, you should ask questions when something does not make sense. Do not be afraid – you will benefit through your participation and the class will be more dynamic and interesting.
- Ask questions outside of class. Office hours and the forums are usually underused. Please seek help if you are not understanding how to solve homework problems. That’s what the forums and office hours are for.
- Do your homework. Only through practice will you be able to do the problems on a quiz or exam. Also, the homework part of your grade is the most in your control and is usually worth an entire grade.
- Study the solutions and your book. The posted solutions and the worked-out problems in the book are your examples of how to correctly solve problems – study and emulate them until you understand.

Academic Integrity: You are responsible for reading the CSU Sacramento policies on academic honesty found at http://www.csus.edu/admbus/umanual/UMA00150.htm. Questions on the policy may be part of the first quiz.

Regrading: If you believe you lost points on some work even though your solution was correct, resubmit the entire work, within a week of when it was first returned to the class, to the instructor with a letter describing your concern. Double check that your proposed solution was correct before resubmission.