
Course Information

Instructor: Prof. Kevin Fu
Room CS358, 545–4006, kevinfu@cs.umass.edu
Office Hours: Tues 3–4PM by appointment

Teaching Assistant: Robert Lychev
Room CS 207, 577–2129, rlychev@cs.umass.edu
Office Hours: Fri 11:00-12:00, or by appointment

Student email list: cmpsci-591d-01-spr08@courses.umass.edu
Web page: <http://prisms.cs.umass.edu/cs591d/>

1 Overview

Applied cryptography spans many disciplines including computer systems, computation, mathematics, and law. This course aims to teach students both the foundations of cryptography and the humility of building practical cryptographic systems. Topics will include fundamentals of cryptography, applications, attacks, and theory. The class will draw on material from public key cryptography, number theory, usable security, hash functions, symmetric cryptography, RFID security, secure storage, cryptographic protocols, electronic voting, law, theoretical notions of security, and cryptographic attacks. Students will be evaluated based on a team project, class participation, problem sets with hands-on labs, and quizzes.

Intended audience. This 3-credit course is intended for undergraduates with demonstrated interest in applied cryptography, as well as graduate students who would like to learn more about applied cryptography. We expect the average student to spend an average of 7–8 hours outside of lecture per week. Some weeks will have more deadlines than others, so plan ahead.

Prerequisites. A “B” or better in CMPSCI 311 (algorithms) and CMPSCI 377 (operating systems) or equivalent. Number theory may be helpful (e.g., MATH 471), but is not necessary.

Lectures. Lectures will be held in Hasbrouck 137 on Mondays and Wednesdays from 2:05PM to 3:20PM. Show up on-time with proper tools for note taking. Use of laptop computers in class may be restricted if distracting. A schedule of topics will be posted on the Web.

2 Textbook and reading

The textbook for the course is *Cryptography: Theory and Practice, 3rd edition* by Douglas Stinson. Notify the course staff if you have trouble locating the book. Note that the 3rd edition is nearly a complete rewrite of the book; do not use older versions of the book. We will assign reading and homework from both the book and research papers.

3 Grades and methods of evaluation

Grading will be as follows:

| | |
|------------------------|-----|
| Homework | 35% |
| Team project | 30% |
| Three in-class quizzes | 30% |
| Class participation | 5% |

3.1 Homework

There will be no more than five homework assignments during the semester. The homework will consist of a mixture of individual and team assignments. Assignments will vary by topic, but may include mathematics, programming, and essay writing. We will assign you to a 2- or 3-person team. Individual work for team assignments will not be accepted. Group assignments must include a paragraph explaining, for each team member, their contributions and duties.

3.2 Team project

A major part of this course is a team project. We will assign you to a team of 2–3 people. One goal of this course is to expose you to the realistic joys and challenges of working in teams. As such, you will be responsible for organizing team meetings around your many schedule constraints. Effective teamwork is essential.

A list of project ideas appear on the course Web site. Projects are carried out in the same team as your homework. There are four components to your project grade: a project proposal, a midterm status report, a final project report, and a project presentation. The due dates for each of these milestones appear on the course Web page.

Project proposal (10%). Your proposal should explicitly state the problem your project will address, your project’s goal and motivation, related work, the methodology and plan for your project, and the resources needed to carry out your project. Be sure to structure your plan as a set of incremental milestones, and include a schedule for meeting them.

Status report (10%). Your status report should contain sufficient preliminary results and critical thinking to show that your project is on the right track. You should include your original proposal with instructor comments, along with any surprising results or changes in direction, schedule, etc. You should also have a refined version of the problem statement and goals, as well as a more developed related work section.

Final report (40%) and project presentation (40%). A final report describing your research problem, your contributions, and analysis will be required. Present your research problem, analysis, and results to the class in a brief presentation and also in a final report. The presentation may include a system demo if appropriate. The final report must include a paragraph explaining, for each team member, their contributions and duties in the project.

3.3 Quizzes

There will be three in-class quizzes (**Mon, March 3; Wed, April 2; and Wed, May 7**). There will be no final exam. Quizzes are closed book. Students may bring a single sheet of paper of notes (8.5 inch x 11 inch), but the sheet must be **hand written, not typed, and not photocopied**. We will inspect your “legalized cheatsheet” and disallow non-conforming sheets, so make sure to follow the rules carefully. Simple calculators are allowed, but any device capable of networking is not. See the oral examination policy regarding missed quizzes.

3.4 Class participation

Students can participate in class in several ways. At the beginning of each class, students will have the opportunity to report on the latest news in applied cryptography and computer security. Intellectually stimulating questions also qualify. Students can also engage in discussion on the class online forum. Quality rather than quantity counts most in this subjective evaluation.

Students may volunteer to scribe a lecture. The effort would lead toward credit to class participation. Scribe notes are due one week from the date of the lecture being scribed. The notes must be written in \LaTeX . See the TA or the Web site for assistance with \LaTeX if necessary. The grade will depend in part on how much effort is required by the TA to edit and revise the submitted notes. Low-quality scribe notes will not be graded.

If you are scribing, talk to the lecturer to resolve any questions you may have about the lecture, and ask for any material that may help you prepare the scribe notes.

4 Policies

We will respect general university policy on class absences¹ to ensure you follow correct procedure for obtaining excused absences.

4.1 Lateness

Each student is granted **two “penalty free” late passes** for the homework. You need not provide any excuse. A free late means you may turn the homework in by 8AM on the day of the **next class** without penalty. We are strict about the deadlines (8:01AM is late). Any late homework beyond your two freebies will earn a grade of zero. If you plan to be away during a deadline, you should submit your problem set early. A late team homework would debit a freebie from each member. Late freebies may **NOT** be used for any of the term project assignments. A late term project assignment will have a 20% grade reduction for each late weekday (8:01AM).

4.2 Oral exams

If you are unable to attend a quiz, you may **pre-arrange** an oral exam. Note that sleeping through a quiz does not qualify, and you would receive a grade of zero. Unless you obtain an excused absence per university policy (see footnote), you may not arrange an oral exam after the quiz begins.

¹http://www.umass.edu/registrar/gen_info/class_absence.htm

4.3 Collaboration and plagiarism

You may discuss material with others, but your writing must be your own. When in doubt, contact the instructors about whether a potential action would be considered plagiarism.

If you do discuss material with anyone besides the instructor or TA, acknowledge your collaborators in each write-up. If you obtain a key insight with help (e.g., through library work or a friend), acknowledge your source and write up the summary on your own. In most of your write-ups, we will expect to see citations.

Again, we cannot emphasize enough that you must cite all your sources properly. You must remove any possibility of someone else's work from being misconstrued as yours. We also consider the facilitation of plagiarism (giving your work to someone else) as plagiarism as well.

Never misrepresent someone else's work as your own. It must be absolutely clear what material is your original work. Plagiarism and other anti-intellectual behavior will be dealt with severely. Investigating plagiarism is a pleasant experience for neither the instructor nor the student. Please help us by avoiding any questionable behavior.

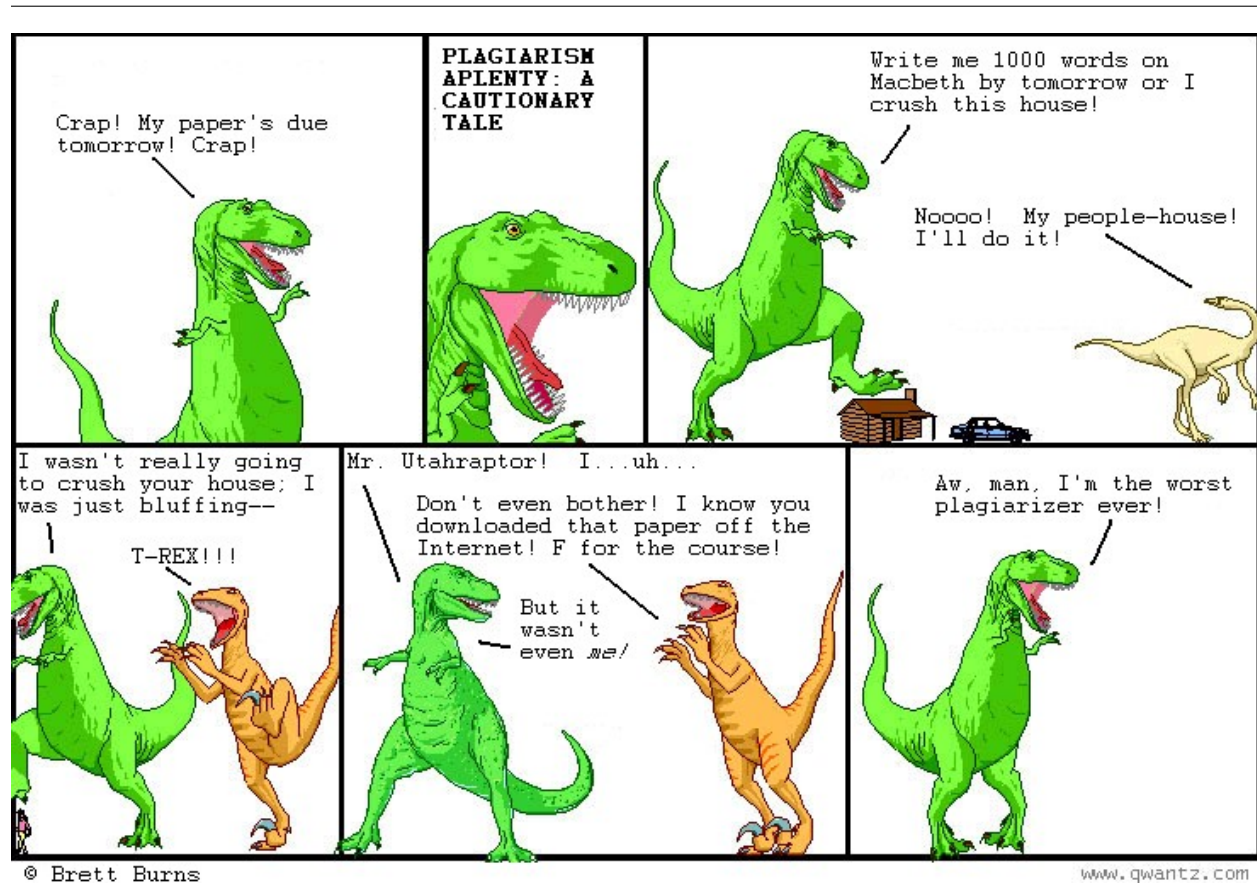


Figure 1: Dadasaurus Rex with permission from Leonard Richardson (<http://www.crummy.com/features/dada/>).