

---

## Course Information

Instructor: Prof. Kevin Fu  
Room CS 230, 545-4006, [kevinfu@cs.umass.edu](mailto:kevinfu@cs.umass.edu)  
Office Hours: Mondays 10:20-11:20, but appointments recommended

Teaching Assistant: Andres Molina-Markham  
Room CS 226, 545-0067, [amolina@cs.umass.edu](mailto:amolina@cs.umass.edu)  
Office Hours: Fridays 11:30-12:30, or by appointment

Primary email: [cs466-staff@cs.umass.edu](mailto:cs466-staff@cs.umass.edu)  
Web page: <http://prisms.cs.umass.edu/cs466/>

## 1 Overview

This course aims to teach students both the foundations of cryptography and the humility of building practical cryptographic systems. The assignments will involve a blend of both theory and programming. 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, secure storage, cryptographic protocols, electronic voting, theoretical notions of security, and cryptographic attacks. Students will be evaluated based on a group project, class participation, problem sets with hands-on labs, a midterm, and a final exam.

**Intended audience.** This 3-credit course is intended for undergraduates with demonstrated interest in applied cryptography. We expect the average student to spend an average of 7-8 hours outside of lecture per week. But this workload may vary depending on your background. For instance, students who have not yet mastered algorithms or low-level computer architecture will likely require more time. Some weeks will have more deadlines than others, so plan ahead.

**Prereqs.** CMPSCI 311 (algorithms) or equivalent is a prerequisite. Number theory (e.g., MATH 471) or systems courses (e.g., CMPSCI 377 or CMPSCI 460) may be helpful, but are not necessary.

**Lectures.** Lectures will be held in LGRC A310 on Mondays and Wednesdays from 9:05AM to 10:20AM. 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. Students are expected to have read the assigned reading material before the start of lecture.

**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. We have put one copy of the textbook on reserve in the library.

**Getting help.** Please email `cs466-staff@cs.umass.edu` if you have general questions (e.g., homework, absences, etc.). By using this staff email address rather than individual staff member email addresses, you will receive a response more quickly by the first available staff member.

## 2 Grades and methods of evaluation

Grading will be as follows:

Homework	35%
Team project	25%
Final exam	20%
Midterm	15%
Class participation	5%

**Homework.** There will be regular homework assignments—approximately once per week. 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.

We encourage the open discussion of material from lecture; however, we **strictly forbid** the discussion or sharing of actual solutions. These verboten activities include the copying of solutions from other students, from materials found online, or materials from previous semesters. See our full anti-plagiarism policies at the end of this document.

**Submission procedure.** You must submit your work via SPARK by the deadline listed in each assignment. We do not accept homework, labs, programming assignments, etc. by any other means (e.g., email does not count). Check with the TA regarding file formats that are accepted. If you have special circumstances and wish to request deviation from this submission procedure, consult with the TA well ahead of the deadline. Last minute requests will not be looked upon favorably.

### 2.1 Team project

A major part of this course is a team project. This year all term projects will involve applications of cryptography on a low-power microcontroller with a RISC-like instruction set. 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.

Details about the project will be distributed later in class. 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.

## 2.2 Exams

There are two exams. There will be one in-class midterm exam (**Wednesday, October 27**) and one final exam (date TBA). Exams are closed book. Students may bring a single note card (4 inch x 6 inch or smaller, double sided), but the note card must be **hand written, not typed, and not photocopied**. We will collect note cards a couple days in advance of each exam. Students must submit the note card by the lecture preceding the exam for the note card to qualify. Calculators and other computing devices are **not allowed** during exams. See the oral examination policy regarding missed exams.

## 2.3 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. Quality rather than quantity counts most in this subjective evaluation. Occasional pop quizzes in lecture will contribute to your class participation grade.

Students may also volunteer to scribe certain lectures. Check with the lecturer if you're interested in this opportunity. 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  $\text{\LaTeX}$ . See the TA or the Web site for assistance with  $\text{\LaTeX}$  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.

## 3 Policies

We will respect general university policy on class absences<sup>1</sup> to ensure you follow correct procedure for obtaining excused absences.

---

<sup>1</sup>[http://www.umass.edu/registrar/gen\\_info/class\\_absence.htm](http://www.umass.edu/registrar/gen_info/class_absence.htm)

### 3.1 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. A homework assignment cannot be “double delayed” by stacking freebies; at most one late freebie per student per homework is allowed. 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** team 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).

Budget your freebie usage carefully! If you use it up early in the semester, you may find yourself wishing you had held on to it until a more important schedule conflict.

### 3.2 Oral exams

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

### 3.3 Collaboration and plagiarism

Plagiarism may result in penalties ranging from a zero on an assignment to automatic failure in the course. CMPSCI 466 uses an anti-plagiarism policy borrowed from CMPSCI 377. If you have any questions as to what constitutes unacceptable collaboration, please talk to the instructor right away.

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.

**Solutions.** You may not collaborate in any way when constructing your solutions; you must work alone on your solutions. All homework and lab projects in this course are to be done by you. Violation will result in a zero on the assignment in question, probable failure in the course, and initiation of the formal procedures of the University. We do check for plagiarism.

You are not allowed to look at or in any way derive advantage from the existence of solutions prepared elsewhere. You may not look at code prepared by someone else for the programming assignments. You may not purchase solutions off the Internet or hire people to do the assignments.

**Facilitation.** We consider the facilitation of plagiarism (giving your work to someone else) as plagiarism as well. Showing your solution to another student is considered facilitating dishonesty and you will be referred to the Academic Honesty Board. This can result in holding up your graduation, or having a notation put on your transcript.

You are expected to exercise reasonable precautions in protecting your own work. Do not let other students borrow your account or computer, do not leave your program in a publicly accessible directory, and take care when discarding printouts.

**Academic honesty.** Acts of cheating and plagiarism will be reported to the University Academic Honesty Board. You are responsible for knowing, and will be held to, the University Academic Honesty Policy. This policy is available online:

[http://www.umass.edu/dean\\_students/codeofconduct/acadhonesty/](http://www.umass.edu/dean_students/codeofconduct/acadhonesty/)

**But we encourage responsible discussion.** Discussion of course material is not considered cheating and is strongly encouraged. If you receive substantial help from another person other than the instructor or TAs, you must acknowledge them in your work. If you use any published or unpublished source in any of your own work, you must give full citation. We consider incomplete acknowledgment as plagiarism. In most of your write-ups, we will expect to see citations. If you have questions about these policies, please check with the instructor.

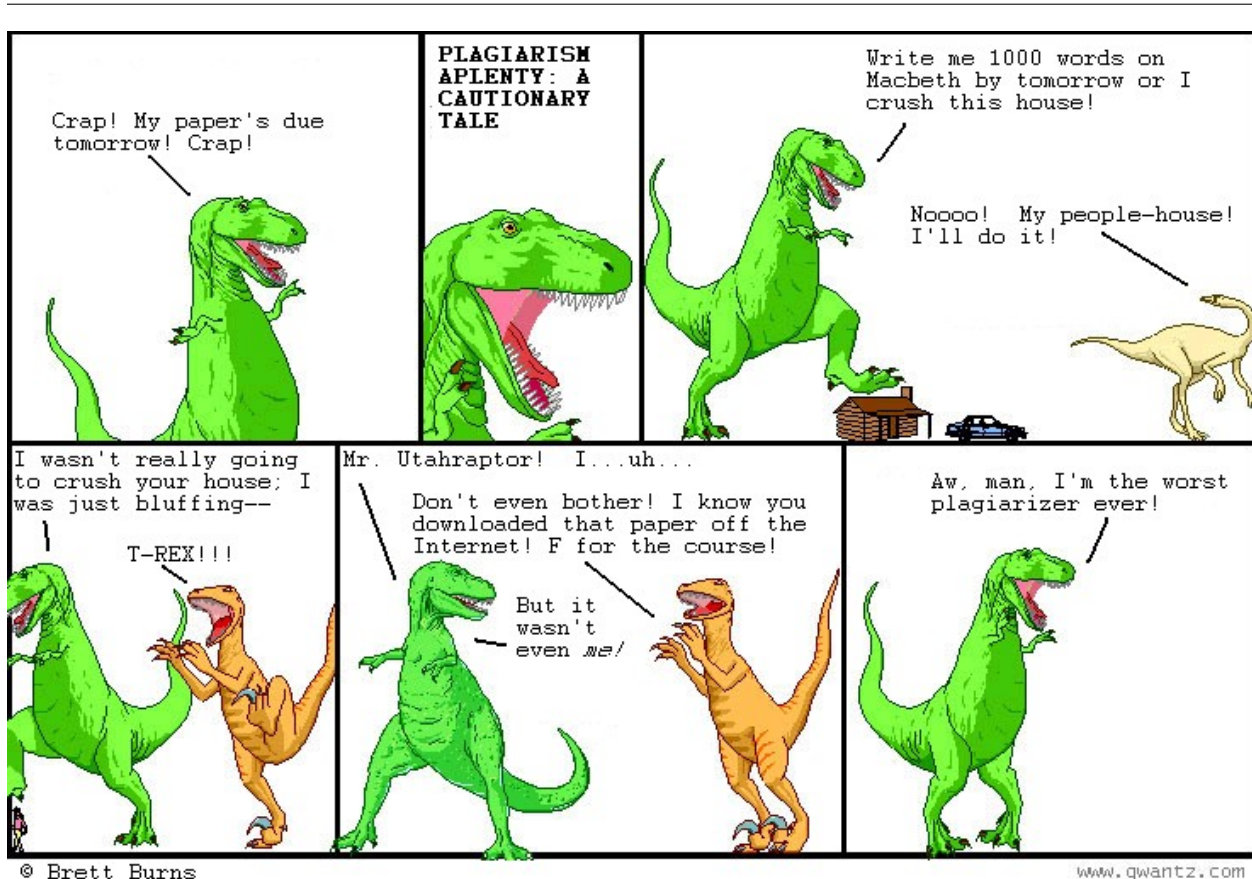


Figure 1: Dadasaurus Rex with permission from Leonard Richardson (<http://www.crummy.com/features/dada/>).