

David Molnar (dmolnar@eecs.berkeley.edu)  
Teaching Statement

Computer science makes it possible for one person to do work that previously required a hundred people – if it were possible at all. The advent of computers has changed society, so much so that to detail the effects of the Internet or the effect of error correcting codes, to take just two examples, is to dive into cliché. My teaching philosophy follows from the imperative I see to share knowledge about computer science with a wide audience. For those who will not be trained as computer scientists or programmers, we need to demystify our field and help them make informed decisions. Part of the way we can do this is by showing our students that computer science has a direct impact on their lives, even if they do not need to program themselves. For those who do work in the field, our responsibility is to help them achieve the limits of their potential. Here I believe we need to show students the breadth of problems in our field, and to always be up front with them about the limits of what we know. The most exciting words to me are “I don’t know,” because they offer an opportunity to push the boundaries of our knowledge. I have acted on this philosophy through a combination of teaching in the classroom, research mentoring outside the classroom, and engaging with the public.

I have taught both core and elective courses. For elective courses I served twice as an undergraduate teaching fellow for a graduate-level course in cryptography taught by Michael O. Rabin at Harvard. Cryptography traditionally comprises the study of secret codes and ciphers, but “modern” cryptography expands this to include much more. For example, our course covered “zero-knowledge proofs,” which are methods of demonstrating the truth of a statement, without giving the means to turn around and prove the statement to others. I jumped at the chance to show others how such seemingly impossible feats can be made practical. A key challenge when teaching this elective course is that modern cryptography requires a wealth of background, ranging from number theory to computational complexity. I designed and taught enrichment sessions for students who had the desire to learn, but lacked specific material. I also encouraged students from other areas, such as government, to take the class and I worked with them to identify and address shortcomings on a more individual basis. I invested this work because I believed it was important to make the knowledge available to all who were interested.

For teaching in a core course, I served as a teaching assistant in an undergraduate algorithms course taught by Satish Rao at the University of California, Berkeley. I had responsibility for three sections of students, each of which met once per week. Core courses present several challenges not found with electives. First, the scale: the number of students enrolled in the class was larger by an order of magnitude than my previous teaching work. Second, engagement: while almost all participants in my cryptography course had chosen to be there, this class formed part of the undergraduate curriculum, and so some students viewed it merely as a hurdle in the way of a degree. Finally, we had students who both worked full-time and went to school, which led to large demands on

their time outside class.

To deal with the issues of scale and engagement, I used techniques that involved students actively in their learning. During our weekly sections, I followed the suggestion of a teaching course provided by Berkeley and split students into groups to discuss homework problems. Afterwards, each group sent a representative to the board to explain their approach to the problem. Midway through the course, I asked students to fill out index cards with anonymous feedback, as well, listened to their suggestions, and I acted on them where appropriate. For example, I added additional material on applications to bioinformatics, and I reduced the amount of group work in section following numerous student requests. For students who worked, I made myself available at flexible times. I also reminded them that their schedules were different from others in the class, and so therefore they should not mistake other students' progress as "effortless."

In addition, I used role-playing to lead students to discover aspects of the material for themselves. In section just prior to covering the classic "max-flow/min-cut" theorem, I began by drawing a flow graph for oil pipelines in a fictional country, with the "source" being oil fields and the "sink" a coastal shipping port. As students entered, I assigned them to the "Ministry of Oil" team or to the "Freedom Fighter" team. The "Ministry of Oil" team's assignment was to find the maximum oil flow from fields to shipping. The "Freedom Fighter" team's assignment was to find a set of oil pipelines to destroy in order cut off the oil fields from the port, destabilizing the fictional country's oil export. We made the simplifying assumption that the higher a pipe's capacity, the harder it would be to destroy, making the assignment to find the minimum weight set of pipelines that separated source from sink. After both teams worked out their answer, I asked them to share their answers with the entire section. We then compared the flow amount found by the Ministry of Oil with the sum of the weights of the pipelines target by the Freedom Fighters. Miraculously, the two turn out to be equal – just as the max-flow/min-cut theorem states they must be! Having invoked the proper sense of wonder, we could then discuss the proof of the theorem.

My teaching work was recognized by others as effective. Both semesters serving as a teaching fellow for cryptography, I received the Derek Bok Certificate of Distinction in Teaching, given to teaching fellows whose evaluations averaged greater than 4.5 on a 5 point scale with at least seven respondents. My second time as a teaching fellow for cryptography, I won the Distinguished Teaching Award from the Division of Engineering and Applied Sciences at Harvard (now School of Engineering and Applied Sciences). This award is competitive, with recipients nominated from among all teaching fellows in all classes taught in the engineering and applied sciences. In the core course, my teaching ratings were above average. This indicates room for improvement, which I plan to make by refining my techniques for engaging students and working with larger classes.

Beyond the classroom, I have spent a significant amount of time mentoring undergraduate students. I have acted as the direct supervisor for six undergraduates as a graduate student. At Berkeley, I have been fortunate to have excellent students to work with, but I have also learned to understand that dif-

ferent students may need to try different projects to find one that is a match with their background and interests. For example, one student I mentored on a project that involved program analysis turned out not to know what a library was, much less how to extract individual functions from it to perform a small scale test of our analysis. That same student, however, excelled once given a project in cryptography more in tune with his interests and background in mathematics. He and another student then took a suggestion of mine and ran with it all the way to a research paper published at Public Key Cryptography, an internationally recognized conference.

In addition, I was part of a team of mentors for the 2008 SUPERB-TRUST program at Berkeley. This program offered a research experience in computer security for under-represented students. Working with faculty mentor David Wagner, and with additional graduate student mentors, I guided nine undergraduates in a project that used tools that exercise programs looking for software bugs, then reported these bugs to developers. I wrote software to support the project, and I answered student questions on a daily basis. By the end of the summer, our students had filed over 90 bug reports to open source software developers, of which at least 14 were fixed. After the project formally ended, I stayed in touch with several of the students, and I helped them prepare a paper on their work for submission to an international refereed workshop on software security. Our work resulted in a successful experience for nine undergraduates from smaller schools and under-represented backgrounds who otherwise may not have had an opportunity to do research in computer science.

Finally, I have worked to make the results of my research accessible to the general public. In particular, my work on privacy and security in radio frequency identification devices (RFID) has attracted wide interest. An RFID is a small chip with a radio attached to an item and used to identify the item for an inventory system. The use of RFID raises privacy concerns because, without special precautions, these chips can be read remotely by anyone with a compatible reader, and they can be "cloned" to create new chips are indistinguishable from the old. One of my research projects focused on the use of RFID in library books, which happened just as Berkeley Public Library and San Francisco Public Library were evaluating RFID for possible use. Because of my expertise, I was invited to speak at public hearings on RFID held by both libraries. I also worked with the Electronic Frontier Foundation and American Civil Liberties Union to help them understand the public policy implications of RFID and limitations of the technology.

I followed the library RFID work with engagement on RFID issues in identification documents more generally. With Ari Juels and David Wagner, I wrote a paper aimed at both researchers and non-specialists that critiqued aspects of the United States deployment of "e-passports" and suggested changes. Our paper formed part of a formal comment to the State Department by the Electronic Frontier Foundation. I then gave testimony to the California Legislature on several occasions regarding these issues, and I arranged for demonstrations related to RFID security issues to educate the public about potential problems and solutions with RFID. I did this because I believe the public needs access

to computer science research and knowledge to make informed decisions about policy.

Looking forward, I am eager to continue teaching, mentoring, and exposition. In teaching, I am interested in pursuing a mix of courses aimed at specialists and non-specialists. For example, I am interested in developing a course similar to “Bits,” offered at Harvard, or “The Efficient Universe,” offered at Princeton, where computer science insights and techniques are explained in a way that makes them accessible to students in other areas. For courses aimed at computer scientists, I am interested in teaching both theoretical courses, such as algorithms, and more systems-oriented courses, such as introductory computer science or operating systems. My research in computer security needs both approaches, so I am interested in courses that have both styles of learning. To attract graduate students to my research agenda, I plan to teach a special topics course in my field of computer security focusing on research projects and pushing the boundaries of the field. In all these cases, I plan to explore more ways of helping students take control of their own learning. For example, I hope to find different ways of pursuing group work that avoid the tragedy of the commons where one or two students perform all the work. By teaching, mentoring, and public engagement, my goal is to demystify our field, and to spread understanding of the benefits that attend an education in Computer Science. Working as a professor is an ideal way for me to meet this goal.