

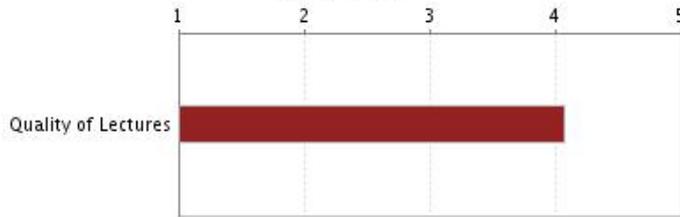
# Teaching Evaluation Summary (Spring 2009-2010)

Instructor: **Barak, Boaz**  
Subject: **COS**  
Catalog & Section: **433, L01**

# Ratings Summary

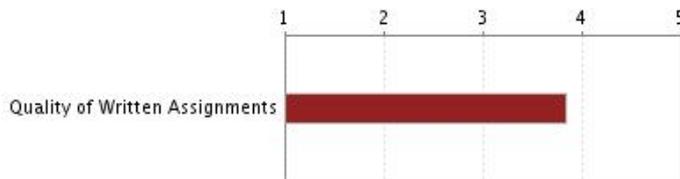
Course Title: **Cryptography**  
Enrollment: **30** Responses Incl Declines: **30**  
(Declined: **4**)

## Lectures



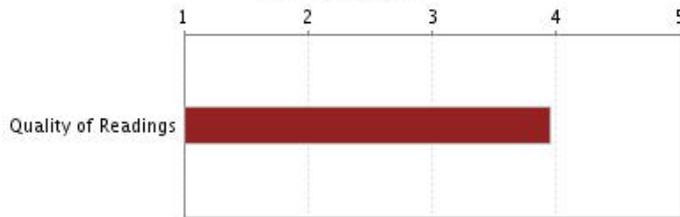
	Mean	Excellent	Very Good	Good	Fair	Poor	N/A
Quality of Lectures	4.08	7	12	5	0	0	0

## Papers, Reports, Problem Sets, Examinations



	Mean	Excellent	Very Good	Good	Fair	Poor	N/A
Quality of Written Assignments	3.84	6	12	4	3	0	0

## Readings



	Mean	Excellent	Very Good	Good	Fair	Poor	N/A
Quality of Readings	3.95	7	6	6	1	0	4

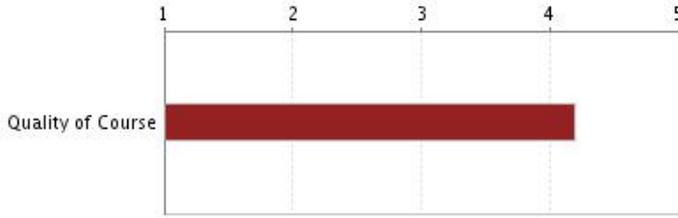
# Teaching Evaluation Summary (Spring 2009-2010)

# Ratings Summary

Instructor: **Barak, Boaz**  
 Subject: **COS**  
 Catalog & Section: **433, L01**

Course Title: **Cryptography**  
 Enrollment: **30** Responses Incl Declines: **30**  
 (Declined: **4**)

## Overall Quality of the Course



	Mean	Excellent	Very Good	Good	Fair	Poor	N/A
Quality of Course	4.20	11	9	4	1	0	0

Reasons for taking course	Class Year	Expected grade	Hrs/wk outside class	Percentage attended		
Professor	3.85	Freshman	3.85	A 73.08	< 1 0.00	< 20% 0.00
Distribution Requirement	3.85	Sophomore	7.69	B 19.23	1-5 0.00	20-40% 0.00
Departmental	42.31	Junior	34.62	C 7.69	5-10 26.92	40-60% 3.85
Certificate Program	7.69	Senior	34.62	D 0.00	10-15 34.62	60-80% 0.00
General Interest	42.31	Graduate Student	19.23	F 0.00	> 15 38.46	80-100% 96.15
				P 0.00		

## 1. Self-evaluation

### Why did you take this course? How would you describe your level of engagement in the course?

- Interested in cryptography and theoretical CS. Somewhat engaged: it usually only takes half my concentration to follow the class, so I give that much.
- I was very interested in the subject and am looking for a challenge.
- I took this course because I'm interested in the material
- Low, I could have been much more engaged overall.
- I was interested in the subject. I was trying to do well in the class but I wasn't too stressed out about it.
- I'm very interested in cryptography, so I was very excited to take this course. I was quite engaged.
- I took this mostly for general interest. I was forced to be relatively engaged in this course in order to stay on top of things.
- I took this class to satisfy my theory distribution requirement for COS.
- I took this course because I enjoyed COS 340 and I wanted to improve my reasoning about probability and math in general. I was fairly engaged in the course.
- Cryptography is relevant to a significant amount of computer science and electrical engineering - I wanted to have a background in this area.
- I took this course because I'm interested in systems and network security. I thought a formal basis in cryptography would be useful for future graduate studies and/or employment in the software industry.
- This course was a lot of work.
- I like the subject material.
- I was really interested to learn in cryptography, and I spent a fair amount of time per week working on it.
- I took this course because I needed a theoretical computer science course, and because it looked really interesting. I was not as engaged in lecture as I should have been, and did miss some information, but I feel I learned to work with a lot of it by doing the problem sets.
- I took this course after the subject was introduced to me in COS 340. I thought it sounded fun and interesting and when I mentioned it to my advisor there were no objections. I felt that I devoted most of my time during the week working on this course than for all of my other courses combined, but often felt lost.
- I got curious about this course. I have been totally into it for the entire semester.
- I took the course because I needed a theory course, and because it's potentially relevant to my research.
- This subject has long interested me, and I've taken prior courses on it. This course filled the departmental theory requirement and came very highly recommended. It did not disappoint. I spent more hours in any given week on homework and studying for this class than I did for either of my other classes.

## 2. Lectures - Boaz Barak

### How would you describe the overall quality of the lectures? Please comment, as appropriate, on how well the instructor presented the subject matter, stimulated your intellectual curiosity and independent thinking, and contributed to your knowledge of the subject matter.

- Clearly taught, sometimes funny. Sometimes repetitive, though (specifically claiming that crypto requires new intuition, and generally in stating a hardness assumption, defining a security standard, stating a system that meets that standard, and doing reductions.)
- The lectures were great. I would have liked to get the notes in advance so that we could review what would be covered in the lecture, but it's not a big deal
- The lectures were quite good.
- Good lecturing. The professor is very smart but sometimes goes quite fast
- Boaz was a great lecturer. He really knows his stuff and did an excellent job of explaining some incredibly non-intuitive subjects.
- They were sometimes a bit dry.
- Lectures were generally very well taught. The material was very complicated and it definitely made a huge difference to have the lecture notes to review both during and after the lectures. The lectures in the middle on the Goldreich-Levin theorem were definitely the hardest to follow; I think the most improvement could be made on those lectures. In those lectures in particular, Professor Barak sometimes got bogged down in the details, and I lost any sense of what the main idea of what we were doing was. Generally though, I thought the lectures were quite good.
- The lectures overall were very clear and well-taught. Prof. Barak even made some funny jokes on occasion. I also appreciated greatly the typed lecture notes, so I could fully devote my attention to what Prof. Barak was

saying, rather than furiously scribbling down every formula on the board.

- The lectures were very high quality. Boaz is fun, honest (about when assumptions might not be well founded), funny, and a great lecturer.
- Lectures were pretty good in general. The lecture notes were almost better than the lectures themselves. Sometimes it was hard to understand Boaz's points. Also, sometimes it seemed the class would go on without people understanding concepts.
- Boaz is a good lecturer. Clear, prepared, and always prepared to answer questions.
- Probably the biggest problem with lectures is that Professor Barak writes too small on the whiteboard. Seriously, it took me like three weeks to be able to recognize a right bracket (}) instead of just seeing an incomprehensible squiggle.
- The lectures were presented clearly but sometimes went too quickly for me to appreciate the calculations involved. I found the material less interesting than I had expected.
- Boaz gives really dense lectures, which can be understood in full detail if prerequisites are met.
- The lectures were good. The lecture notes were well-structured and relevant to the assignments. One thing I'd like to see improved is to make a bit more effort to elicit student feedback. In some cases the lecture moved faster than I could follow, but didn't want to interrupt the lecture to say so. Prof. Barak did sometimes stop to see if we were following, but if we didn't respond he'd sometimes continue, when sometimes the non-response was a sign that we were all confused.
- I really enjoyed the lectures. This is a course where I consistently felt after a lecture that I knew more and understood more than I had before the lecture. I felt that there was a good tradeoff between intuition and formalism, but here as in other areas of the course, I would have liked to see fewer ad-hoc constants, since it's sometimes hard in retrospect to tell which constants are ad-hoc and which are really intrinsic to the setup of some particular problem. For example, we'd often prove that a probability is less than 0.01 by showing that it's asymptotically  $2^{-n}$  but it seems like it would be better just to say that we want to prove that the probability is asymptotically negligible.
- The lectures were fine, but sometimes confusing. There were lots of good jokes and examples to keep our attention, which was very helpful.

### 3. Papers, Reports, Problem Sets, Examinations

**Please comment on the guidance of the instructor(s) in preparing you to do written work, comments in response to written work, and the overall value of the papers, reports, exams, and problem sets to the course.**

- The problem sets were interesting, good practice, and an appropriate amount of work. They could have used much more proofreading, though: almost every problem set needed clarifications and/or corrections after it was released, on account of which I got into the habit of waiting until the day they were due to start them.
- The problem sets were very hard, but I found them useful for learning the material
- Were pertinent.
- The problem sets were challenging. They were very helpful for understanding the class material.
- Problem sets were tough, but the extra credit made them a lot less stressful. Also, they explicitly did not include any busy work sort of exercises and this was very nice.
- The problem sets were very difficult, but I got a lot out of them.
- The problem sets were extremely instructive and I learned a ton from them. That being said, they were a TON of work. Not sure if it was worth it.
- The problem sets were grueling, and I don't think I did particularly well. I feel that part of the problem was the Wednesday afternoon due date, which did not mix well with my own procrastinating ways. Also, there were a tremendous number of typos in the homeworks, many of which were not just cosmetic but actually messed up the problems. One or two of the problems even seemed to be flawed, i.e. the answer presented by the TA's afterwards did not seem to satisfy the constraints of the problem.
- I learned a lot from the problem sets. The grading was sometimes a bit inconsistent, and the sets were longer than I would have liked, but they covered the material. Better explanation of bonus points would have been nice.
- The problem sets were good, however I wish they were more thoroughly proofread. Sometimes mistakes in the problem sets would cost us a fair bit of time.
- It would have been useful to get the official solutions to all the homework problem sets.
- Problem sets were far too time consuming. I understand that many graduate students take the course, but for undergraduates taking 4 other courses, we can't be expected to put in 30 hours a week. The 'bonus points' idea was a nice thought, but basically just meant the final was 100% of the course grade because it seemed like everyone ended up with 100 on the HW. In summary, way too time consuming to be reasonable. Exam seemed to be much more math-intensive than the problems sets and wasn't really representative of the course.
- Problemsets, and the final, were excellent. Difficult, but manageable, so that students get an excellent sense of the material.
- The problem sets were both challenging and interesting. Though difficult, I got a lot out of them. The only

frustrating aspect is that it seems as though Prof. Barak never proofread the assignments, resulting in frustrating typos all over the place.

- I often found myself completely lost on problem sets. Only through long hours of collaboration and discussion with others did I really understand many of the problems, and I felt that the material I learned in the text or in lecture did not immediately aid my ability to construct a proof or help me understand what I needed to do.
- Problem sets are very instructive. It teaches material taught in class, and beyond. I like this idea.
- The problem sets were extremely well structured and I had a lot of fun doing them. One minor problem was the fairly high rate of typos. More thorough proofreading would avoid the frustration of discovering we're being asked to prove the wrong thing.
- I really enjoyed the problem sets even though they were very long and time-consuming. I found them enlightening and helpful, if often challenging. I appreciated the system whereby many extra credit points were available, allowing lapses for very hard problems and giving the teaching staff reason to be harsh on technicalities and on style, which improved my own mathematical writing and my thinking about rigor.
- The level of rigor expected in the problem sets was noticeably higher than the level of rigor used in the lecture. It would have been nice to see fewer results in lecture, maybe putting off some information until precept, but at the level you would expect to see our work at. This was most damaging in the first few weeks of the course, but as we got a sense of how much you wanted in the problem sets, I think we just adapted.
- Too many homeworks. (9 or 10 would've been more than enough).
- Problem sets increased knowledge and understanding of the material. However they were very hard and the preceptors were unwilling to help much with the problems. They would give very insufficient hints which would result in no one (or very few people) solving some of the problems.

#### 4. Readings

**Please comment on the quality of the readings in the course. Did the readings present the subject matter clearly? To what extent did the readings stimulate your intellectual curiosity and independent thinking?**

- Some of the additional readings were very helpful, especially the extra lecture notes/slides
- Elucidated the material, plenty of them.
- The professor gave out lecture outlines. Very detailed and helpful. I did not do the extra reading.
- The lecture notes were the main readings I used for the course and they were very helpful.
- Generally only fair to middling.
- Professor Barak provided a ton of readings, which was extremely helpful to understanding the material. The readings were generally excellent, and it was great to have such a variety, so that if one source didn't work, we could use a different one.
- I may not have done terribly many of the readings. The lectures seemed clear enough for the assignments.
- The handouts were really clear, and great to study from.
- Not worth reading.
- Readings are ok. Not that much textbook reading, more lecture notes. But I guess the problem is that the subject matter is fairly young, so finding textbooks is impossible on its own.
- Again, the biggest issues with the class handouts is that it seems like Prof. Barak did not proofread the handouts, resulting in typos, which are especially frustrating in formulas.
- I found that sheer volume of reading that was suggested or given to us was overwhelming. This course had a graduate "feel" to it. I found that not have just one, singular text book for the entire semester was frustrating, although perhaps that's how this subject goes. The reading from the two text's themselves were clear, though, but I did not get much of an intuition from them on how to prove many of the things we were asked.
- Lecture notes are key components of the reading, and they save my life. Notes are clearly written out, and usually given in much more detail than what is covered in the class.
- I appreciated the volume of suggested reading, though I didn't do all of it (that would have taken all my time, instead of just half of it, due to the volume alone). I had used the Goldreich books before, but I was not familiar with Katz and Lindell and enjoyed it very much.
- I wish things had been proofread a little better/been presented more exhaustively in the notes and assignments.

#### 5. Overall Quality of the Course

**Please comment on the overall quality of the course. What worked particularly well and in what ways might the course be improved?**

- Choice and breadth of content were very good. Lectures were clear. Precepts: Sushant's were usually good, although not essential for the course. <...>  
Overall a very fun course.
- I had a good feeling when I finished the class - I learned a lot
- I loved this course.
-

- Generally a good course. Lectures could use some work and perhaps the problem sets could be a little less rigorous but otherwise good.
- The course was a ton of work and very hard, but I learned more in the class than in any other class I took at Princeton. It was very interesting; I learned a lot of new material, and also how to think in different ways.
- I learned a lot, so regardless of my grade I can look back and call this semester a success.
- Workload needs to be seriously rethought. I know Boaz tried to make it better, but its still ridiculous.
- Great course, for theoretically inclined computer science majors. Students get sense of both classical crypto concepts (CCA, CPA, PRF...), and new stuff like zero-knowledge proofs, identification protocols, homomorphic encryption etc.
- This is a challenging course in which you will learn a lot of cool stuff.
- My largest complaint in this course is that I feel I was not properly advised in taking it. I don't think I was mathematically mature enough to take the course, and I don't think I was well-warned, as the first couple of problem sets were not too difficult and by the time I knew what I was getting myself into it was too late to make a change. The prerequisites for this course are simply COS 340, and considering that I received a C in that course and yet no one told me that taking this course would be a bad idea, I had no reason to not take it. Basically, the course itself doesn't need to many improvements; except the readings for each week could be trimmed and more selectively chosen, but I think that students should be more thoroughly advised when considering it.
- This course is very nice one. Cryptography is presented as a solid chunk.
- This is a great course!
- Some of the grading was less careful than it might have been, and some of the feedback less useful. I think the course would benefit from a lower student-to-AI ratio, given that useful feedback would take a very long time and a lot of effort to produce.