COMPSCI 127
Cryptography

Term/Year: Spring 2016
Department: Computer Science

Enrollment: 19
Number of Responses: 10
Percent Response 52.63%

Unless otherwise indicated in the question text, the following scale is used for responses:
1=unsatisfactory; 2=fair; 3=good; 4=very good; 5=excellent.

GENERAL QUESTIONS

	na	1	2	3	4	5	Tot.	Response Rate	Mean
Evaluate the course overall.		0	0	1	3	6	10	52.63%	**4.50**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.)	0	0	0	1	3	6	10	52.63%	**4.50**
Assignments (exams, essays, problem sets, language homework, etc.)	0	1	0	0	1	8	10	52.63%	**4.50**
Feedback you received on work you produced in this course	0	0	1	4	5	0	10	52.63%	**3.40**
Section component of the course	8	0	0	0	1	0	1	5.26%	**4.00**
On average, how many hours per week did you spend on coursework outside of class? (1=<3; 2=3-6; 3=7-10; 4=11-14; 5=>14)		0	1	3	2	3	9	47.37%	**12.22**
How difficult did you find this course? (1=very easy; 2=easy; 3=moderate; 4=difficult; 5=very difficult)		0	0	3	4	2	9	47.37%	**3.89**
What was/were your reason(s) for enrolling in this course? (Please check all that apply)	Elective						8	42.11%	
	Concentration or Department Requirement						3	15.79%	
	Secondary Field or Language Citation Requirement						4	21.05%	
	Undergraduate Core or General Education Requirement						0		
	Expository Writing Requirement						0		
	Foreign Language Requirement						0		
	Pre-Med Requirement						0		
How strongly would you recommend this course to your peers? (1=definitely not recommend; 2=unlikely to recommend; 3=recommend with reservations; 4=likely to recommend; 5=recommend with enthusiasm)		0	0	1	1	8	10	52.63%	**4.70**

EVALUATION OF INSTRUCTORS

Barak, Boaz

	na	1	2	3	4	5	Tot.	Response Rate	Mean
Evaluate your Instructor overall.		0	0	1	2	6	9	47.37%	**4.56**
Gives effective lectures or presentations, if applicable	0	0	0	0	4	6	10	52.63%	**4.60**
Is accessible outside of class (including after class, office hours, e-mail, etc.)	1	0	0	0	3	6	9	47.37%	**4.67**
Generates enthusiasm for the subject matter	0	0	0	0	1	9	10	52.63%	**4.90**
Facilitates discussion and encourages participation	2	0	0	0	2	6	8	42.11%	**4.75**
Gives useful feedback on assignments	7	0	0	0	2	0	2	10.53%	**4.00**
Returns assignments in a timely fashion	7	0	1	1	0	0	2	10.53%	**2.50**

Unless indicated in the question text, the following scale is used for responses: 1=unsatisfactory; 2=fair; 3=good; 4=very good; 5=excellent.

What were the strengths of this course? Please be specific and use concrete examples where possible.

Course

Evaluate the course overall.: **5 (excellent)**

The material was presented logically and coherently, and the psets reinforced the concepts well.

Evaluate the course overall.: **5 (excellent)**

Very thorough review of crypto through modern concepts. The breadth achieved while still maintaining depth was really great.

Evaluate the course overall.: **4 (very good)**

The only crypto course at Harvard, so absolutely invaluable! The lectures are thorough and rigorous! The course also covers some cutting edge material!

Evaluate the course overall.: **5 (excellent)**

The course covered an enormous amount of material. It started from essentially probability theory and built all the way up towards research topics in crypto. The second half was like a topics seminar which was cool. I definitely got a thorough introduction to cryptography and a lot more!

Evaluate the course overall.: **5 (excellent)**

Excellent all around, no complaints, I liked the fast paced nature.

Evaluate the course overall.: **4 (very good)**

The principal strength of this course was in its intent: a relatively fast-paced overview that managed to teach a vast number of cryptographic concepts in a relatively short amount of time with significant success. Another strength of the course was the way in which the instructor constantly emphasized the practical relevance of the material, connecting even the most abstract topics to actual use cases and contemporary issues. There was even a class near the end of the course devoted to discussing the societal impacts of the issues at hand.

Evaluate the course overall.: **3 (good)**

Learned a lot about the theoretical framework behind cryto, and where it is used in the real world.

Evaluate the course overall.: **5 (excellent)**

This class provided fantastic preparation to broadly engage with cryptography in various settings in the future. Learning cryptography in this class felt similar to gaining fluency in a language and a way of thinking, and I think that the course did a very good job at familiarizing us with the terminology of the field and the way of thinking often used in the field.

How could this course be improved? Please use concrete examples where possible and provide constructive suggestions.

Course

Evaluate the course overall.: **5 (excellent)**

The course is built to be small and hard, more or less! Notes require thorough interaction to digest, and problem set exercises are many steps away. I don't personally find this a problem, but expanding it may be hard.

Evaluate the course overall.: **4 (very good)**

As with any new course, some of the assignments were buggy. However,

Evaluate the course overall.: **5 (excellent)**

I think that the screws could be tightened a bit in this course, so to speak. This means things like more rigorous proofs in the lecture notes, fewer typos in notes and problem sets, consistent release of pset solutions and grades.

Evaluate the course overall.: **4 (very good)**

The course might be improved by having a stronger section component in which more detailed constructions are worked out to flesh out the more abstract concepts discussed in the classroom. In particular, it might have been nice to see (outside the context of the lectures, which formed a pretty coherent whole as it was) more details of popular cryptosystems like AES, or bitcoin.

Evaluate the course overall.: **3 (good)**

Would have liked some detail on a few practical examples of algorithms we think are secure, that are actually used in the real world. Way too many typos on problem sets, lecture notes, and exams.

Evaluate the course overall.: **5 (excellent)**

It would be very helpful if somebody (the TFs, maybe?) read through (and preferably tried to solve) the problem sets in advance to catch errors in the questions. It wasn't /always/ a problem, but some of the errors on the problem sets led to a considerable amount of wasted time (which wasn't necessarily useful for learning). This might not be a realistic proposal, but it would be great if possible.

Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.) — Add Comments?

Course

Evaluate the course overall.: **5 (excellent)**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.): **4 (very good)**

The KL book (2nd edition) was somewhat difficult to find.

Evaluate the course overall.: **5 (excellent)**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.): **3 (good)**

Typos!

Evaluate the course overall.: **5 (excellent)**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.): **5 (excellent)**

The lectures notes were generally helpful enough that I didn't need to use the textbook, though when I looked at that on the final it also seemed good. The lectures notes could do with some editing/revising/completing but were generally solid.

Evaluate the course overall.: **4 (very good)**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.): **5 (excellent)**

The lecture notes of the course were really quite excellent. They also contained a panoply of links to useful outside readings and papers.

Evaluate the course overall.: **3 (good)**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.): **4 (very good)**

Lecture notes were very helpful, but had too many typos.

Assignments (exams, essays, problem sets, language homework, etc.) — Add Comments?

Course

Evaluate the course overall.: **5 (excellent)**
Assignments (exams, essays, problem sets, language homework, etc.): **5 (excellent)**

Loved the psets.

Evaluate the course overall.: **5 (excellent)**
Assignments (exams, essays, problem sets, language homework, etc.): **5 (excellent)**

challenging and the exercises made sure you thoroughly understand the material

Evaluate the course overall.: **4 (very good)**
Assignments (exams, essays, problem sets, language homework, etc.): **5 (excellent)**

The assignments were sometimes buggy, but that's expected with a new course. Overall, though, the staff was extremely responsive on Piazza.

Evaluate the course overall.: **5 (excellent)**
Assignments (exams, essays, problem sets, language homework, etc.): **5 (excellent)**

The design of putting a lot of problems on the problem set and making it out of 100 points is great because it gives the students peace of mind regarding their grades and also is such that they voluntarily do more work and learn more. Some of the earlier problem sets had questions which took a long time but this improved throughout the semester.

Evaluate the course overall.: **4 (very good)**
Assignments (exams, essays, problem sets, language homework, etc.): **5 (excellent)**

The problem sets really helped in understanding the cryptographic concepts at play, and the exam was a fair evaluative mechanism.

Evaluate the course overall.: **3 (good)**
Assignments (exams, essays, problem sets, language homework, etc.): **1 (unsatisfactory)**

Too many typos. Some of them were obvious but others meant that I spent several hours on a problem only to find it was false because of an obscure typo.

Feedback you received on work you produced in this course — Add Comments?

Course

Evaluate the course overall.: **5 (excellent)**
Feedback you received on work you produced in this course: **4 (very good)**

fairly thorough commentary

Evaluate the course overall.: **5 (excellent)**
Feedback you received on work you produced in this course: **3 (good)**

The problem sets went ungraded for a long time which prevented there from being much feedback. The quizzes were a good way of ensuring that you knew what was going on.

Evaluate the course overall.: **4 (very good)**
Feedback you received on work you produced in this course: **2 (fair)**

I did not receive very much feedback at all on most of the problem sets, and the problem sets were not graded until near the end of the term.

Section component of the course — Add Comments?

Course

Evaluate the course overall.: **5 (excellent)**
Section component of the course: **N/A**

didn't go to enough

Evaluate the course overall.: **4 (very good)**
Section component of the course: **N/A**

I did not attend enough sections to comment.

In your opinion, what preparation or background is necessary to take this course?

Course

Evaluate the course overall.: **5 (excellent)**

Nothing is required, though a basic background in writing mathematical proofs helps.

Evaluate the course overall.: **5 (excellent)**

mathematical maturity and a reliable intuition for paranoia

Evaluate the course overall.: **5 (excellent)**

Some experience with theoretical CS and comfortability with probability.

Evaluate the course overall.: **5 (excellent)**

Mathematical maturity and some complexity background

Evaluate the course overall.: **5 (excellent)**

Some experience with proofs. I found prior exposure to algorithms useful.

Evaluate the course overall.: **4 (very good)**

I would certainly suggest having linear algebra and familiarity with proof-based mathematics. A good background in group theory is extremely helpful. Some knowledge of number theory is also quite useful, but not required.

Evaluate the course overall.: **3 (good)**

Strong mathematical background, at least Math 122 and preferably Math 123 and Math 124. Additionally, strong theoretical CS background including CS121 and CS124.

Evaluate the course overall.: **5 (excellent)**

"Mathematical maturity", whatever that means. Some prior knowledge of complexity is very useful but not strictly necessary.

What would you like to tell future students about this class?

Course

Evaluate the course overall.: **5 (excellent)**

This is a great class for learning the internal mathematical structure of public and private key crypto. The psets are challenging but low-pressure, which is great.

Evaluate the course overall.: **5 (excellent)**

With Barak, this course is very challenging. But it's extremely rewarding to meet the ideas, especially in the latter half of the course, and to have the mode of thought used to analyze them thoroughly.

Evaluate the course overall.: **4 (very good)**

Excellent course! Boaz is an extremely kind professor who understands that the material he's teaching can be incredibly difficult.

Evaluate the course overall.: **5 (excellent)**

This class was a whirlwind through cryptography, starting from scratch and going through modern research topics including quantum computing, fully-homomorphic encryption, obfuscation, etc. The class was rather fast paced and involved (though the grading structure on the problem sets and final exam was quite generous) so be prepared for that. Boaz is a great professor to get to know, he's really cool!

Evaluate the course overall.: **5 (excellent)**

Cryptography with Boaz was a phenomenal experience for anyone who is both interested and is ready for the mathematical arguments and proofs. We covered a healthy amount of standard undergraduate crypto (private key, public key crypto) as well as really interesting and exciting recent topics and developments. I would highly recommend this class for anyone interested in the topics who has the background for it.

Evaluate the course overall.: **5 (excellent)**

The class was great. Prof. Barak made it more akin to a combination of undergraduate class, graduate class and graduate seminar, teaching the basics, but quickly moving on to advanced topics. I very much enjoyed taking the course, but it was a fair amount of work.

Evaluate the course overall.: **4 (very good)**

If you are interested in the theory of cryptography, contemporary developments in cryptography, or even contemporary applications of cryptography, seriously consider taking this course if you don't mind putting in a fair bit of work. You will not regret it!

Evaluate the course overall.: **3 (good)**

Instead of psets, class contained typos. Would not take again. There are very large numbers of typos on the psets and even the final exam. Some are obvious, but there are usually one or two problems on every pset (other than the one from the textbook) that I'll spend several hours on, only to realize I was solving the wrong problem because it was stated incorrectly. If you're willing to do that, read on. Overall, you will learn a lot of theoretical crypto. Most of this class is figuring out how to build algorithms that are secure with respect to X based on other algorithms that we already knew were secure with respect to Y (or showing such a construction is impossible). For instance you will learn how to build secure encryption algorithms given a secure random number generator. However, the class does not usually describe in detail the algorithms that are actually used in practice.

Evaluate the course overall.: **5 (excellent)**

This year's iteration of the course was one of the best classes I've taken at Harvard. Boaz chose to give a doable but fast-paced introduction to cryptography (definitions of private key and public key crypto and basic constructions and applications for each) in the first half of the course, and spend the second half talking about extremely cool advanced topics such as lattice-based cryptography, zero-knowledge proofs, fully homomorphic encryption, and obfuscation. Boaz is awesome. Take this class.

What did you learn? How did this course change you?

Course

Evaluate the course overall.: **5 (excellent)**

I learned public and private key cryptography; the course changed me in that I did not know much concretely about these topics beforehand.

Evaluate the course overall.: **4 (very good)**

This course was fantastic at giving me a high level perspective of computation from a cryptography perspective.

Evaluate the course overall.: **5 (excellent)**

new exposure to the concepts and methods of a field is always great

Evaluate the course overall.: **5 (excellent)**

I learned a ton of cryptography!

Evaluate the course overall.: **5 (excellent)**

The course taught me a totally new way to think about certain types of arguments and ideas. It also introduced me to cryptography (both standard and modern topics) in a fantastic way.

Evaluate the course overall.: **5 (excellent)**

I feel like I got a good overview over the field of cryptography.

Evaluate the course overall.: **4 (very good)**

I learned a lot about cryptographic concepts. The most important thing I learned, and which definitely changed the way I look at the world, was that no deterministic encryption is CPA-secure.

Evaluate the course overall.: **3 (good)**

Learned the framework for theoretical crypto.

Please comment on this person's teaching.

Barak, Boaz

Evaluate the course overall.: **5 (excellent)**
Evaluate your Instructor overall.: no answer

The lectures were very effective and interesting, if a bit messy at times.

Evaluate the course overall.: **5 (excellent)**
Evaluate your Instructor overall.: **4 (very good)**

Lectures were great at delivering intuition---keeping up sometimes a little difficult, but while kept up, very good. Anecdotes and informal statements about things are great.

Evaluate the course overall.: **4 (very good)**
Evaluate your Instructor overall.: **5 (excellent)**

Excellent, bright! It can sometimes be difficult to follow the writing (especially when new syntax is used).

Evaluate the course overall.: **5 (excellent)**
Evaluate your Instructor overall.: **5 (excellent)**

Boaz was a great professor. He really wanted to make sure that the students in the class were enjoying it and learning a lot. He encouraged participation a lot and generated great enthusiasm for cryptography.

Evaluate the course overall.: **5 (excellent)**
Evaluate your Instructor overall.: **5 (excellent)**

Excellent all around.

Evaluate the course overall.: **4 (very good)**
Evaluate your Instructor overall.: **5 (excellent)**

Boaz managed to explain somewhat confusing cryptographic concepts and proofs in a way that made sense, and by encouraging students to think through concepts in depth both in the problem sets and in the course of instruction, he helped us to develop the sort of problem-solving skills that cryptography requires.

Evaluate the course overall.: **3 (good)**
Evaluate your Instructor overall.: **3 (good)**

Very effective lecturer, but he is too careless with typos in his lecture notes, psets, and quizzes, making them much harder to understand.

How well did you like the format of reading the lecture notes before each lecture?

Course

Evaluate the course overall.: **5 (excellent)**

I enjoyed that format; I think it's efficient, and allows for maximal efficiency in-class.

Evaluate the course overall.: **4 (very good)**

I think it worked really well.

Evaluate the course overall.: **5 (excellent)**

Great! It made sure we could cover a lot more stuff, and lectures were very good for getting a clear intuition. Sometimes a little hard to keep up, but that's my own issue.

Evaluate the course overall.: **4 (very good)**

I thought the format was good -- it helped me understand the material more throughly ajen presented in class.

Evaluate the course overall.: **5 (excellent)**

This is generally a great format for learning the material quickly and ensuring that no one falls behind. I thought it worked well.

Evaluate the course overall.: **5 (excellent)**

Reading through the lecture notes before lecture (along with the quizzes) were a great way to get a first pass at the information in class. It was especially helpful when the lecture went over the material again at a higher level (leaving the highly technical details to be worked out in the writeup).

Evaluate the course overall.: **5 (excellent)**

The lecture notes were very useful. I liked the format. However, some of the lecture notes were not complete, so if that part happened to get skipped (or mistakes were made) in lecture, there was a gap in my understanding that was not filled. I particularly noticed this with DSA on the final, which was not covered in great detail in the lecture notes and the proof in lecture was a bit of a mess.

Evaluate the course overall.: **4 (very good)**

It was generally useful. It certainly helped in understanding the material. I think the quiz format could be improved; sometimes the questions were not entirely clear, and the quizzes were not released and due at regular times, which was occasionally confusing.

Evaluate the course overall.: **3 (good)**

I thought it was generally a good idea, it helped me to understand what was happening in lecture. I think they should be differentiated a bit more, with the lecture notes having theoretical background, and the lectures focusing more on practical applications.

Evaluate the course overall.: **5 (excellent)**

I think this is a very good model for running a course - I liked it both in this class and in a previous class that had a similar policy. In particular, it was very useful to be able to have two passes through the material in order to digest it better.

This was the first time I taught this course at Harvard. Any words of advice for future iterations?

Course

Evaluate the course overall.: **5 (excellent)**

Please release the quizzes at least 12h or so in advance; it was sometimes tough when quizzes came out the morning they were due, and I had other classes before CS127.

Evaluate the course overall.: **4 (very good)**

I think having more carefully written notes and problem assignments, with solutions, would make the course much more effective and give it a further sense of rigour.

Evaluate the course overall.: **5 (excellent)**

I like the difficulty level and the speed and informality/closeness. It would be hard to expand, but maybe that's not what's desired.

Evaluate the course overall.: **4 (very good)**

Keep up the great work! Sometimes when writing proofs on the board, the speed at which they're presented is too fast and it can be easy to lose track. The donusts were great!

Evaluate the course overall.: **5 (excellent)**

Go through some of the more delicate proofs more carefully. I think it would have been useful to have these done out very carefully in the lecture notes as a reference. But perhaps this is what I should have used the textbook for (I usually relied only on the lectures notes since they were complete enough).

Evaluate the course overall.: **5 (excellent)**

This course was one of my favorite classes that I took at Harvard. I've really learned a tremendous amount about crypto and new ways to think. The lecture notes and assignments were great for learning and working through the material. The only drawbacks are the typos that can make the problems hard to understand/solve, though hopefully they will naturally get fixed with each iteration. I'd highly recommend getting a small group of motivated students (as we did this iteration), because that let us put in a lot of time learning/solving and get through a lot more material overall (to some really great material at the end).

Evaluate the course overall.: **5 (excellent)**

I thought it was fine as is.

Evaluate the course overall.: **4 (very good)**

I thought the course did very well for a first time course; it had a coherence of instruction that many such courses lack. I cannot think of any particular advice for future iterations that I have not already mentioned.

Evaluate the course overall.: **3 (good)**

The lectures were very effective, and I understood most of the material of the course. However, the written component (lecture notes, psets, and final) is often written very confusingly, and has a lot of typos on top of that.

Evaluate the course overall.: **5 (excellent)**

Having some of the course staff check the problem sets for errors beforehand (preferably by trying to solve the problems and seeing if they make sense) would be extremely helpful to avoid some frustration on the students' part (it wasn't awful, but it could definitely be better). You might also want to include more links to useful reading material in the lecture notes, particularly for the topics not in Katz-Lindell. In any case, this course was amazing - thank you so much for teaching it!