Comments from Spring 2018: Note the course had two numbers 127&227R

COMPSCI 227R
Cryptography

Term/Year: Spring 2018
Department: Computer Science

Enrollment: 15
Number of Responses: 14
Percent Response 93.33%

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	1	1	2	10	14	93.33%	**4.50**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.)	0	0	1	1	2	9	13	86.67%	**4.46**
Assignments (exams, essays, problem sets, language homework, etc.)	0	0	0	2	3	8	13	86.67%	**4.46**
Feedback you received on work you produced in this course	0	0	2	2	1	8	13	86.67%	**4.15**
Section component of the course	4	0	1	0	1	5	7	46.67%	**4.43**
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	0	10	2	2	14	93.33%	**10.57**
How difficult did you find this course? (1=very easy; 2=easy; 3=moderate; 4=difficult; 5=very difficult)		0	1	4	5	4	14	93.33%	**3.86**
What was/were your reason(s) for enrolling in this course? (Please check all that apply)	Elective						10	66.67%	
	Concentration or Department Requirement						10	66.67%	
	Secondary Field or Language Citation Requirement						0		
	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	1	1	4	8	14	93.33%	**4.36**

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

EVALUATION OF INSTRUCTORS

Barak, Boaz

	na	1	2	3	4	5	Tot.	Response Rate	Mean
Evaluate your Instructor overall.		0	0	1	2	10	13	86.67%	**4.69**
Gives effective lectures or presentations, if applicable	0	0	1	2	6	4	13	86.67%	**4.00**
Is accessible outside of class (including after class, office hours, e-mail, etc.)	0	0	0	0	1	12	13	86.67%	**4.92**
Generates enthusiasm for the subject matter	0	0	0	1	1	11	13	86.67%	**4.77**
Facilitates discussion and encourages participation	3	0	0	0	1	7	8	53.33%	**4.88**
Gives useful feedback on assignments	8	0	0	0	1	2	3	20.00%	**4.67**
Returns assignments in a timely fashion	6	0	0	0	2	3	5	33.33%	**4.60**

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

COMPSCI 127
Cryptography

Term/Year: Spring 2018
Department: Computer Science

Enrollment: 9
Number of Responses: 7
Percent Response 77.78%

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	0	2	5	7	77.78%	**4.71**
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.)	0	0	0	0	0	7	7	77.78%	**5.00**
Assignments (exams, essays, problem sets, language homework, etc.)	0	0	0	1	2	4	7	77.78%	**4.43**
Feedback you received on work you produced in this course	0	0	0	0	2	5	7	77.78%	**4.71**
Section component of the course	5	1	0	0	0	0	1	11.11%	**1.00**
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	1	7	77.78%	**10.14**
How difficult did you find this course? (1=very easy; 2=easy; 3=moderate; 4=difficult; 5=very difficult)		0	0	1	6	0	7	77.78%	**3.86**
What was/were your reason(s) for enrolling in this course? (Please check all that apply)	Elective						4	44.44%	
	Concentration or Department Requirement						5	55.56%	
	Secondary Field or Language Citation Requirement						1	11.11%	
	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	0	3	4	7	77.78%	**4.57**

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

EVALUATION OF INSTRUCTORS

Barak, Boaz

	na	1	2	3	4	5	Tot.	Response Rate	Mean
Evaluate your Instructor overall.		0	0	0	2	5	7	77.78%	**4.71**
Gives effective lectures or presentations, if applicable	0	0	0	0	2	5	7	77.78%	**4.71**
Is accessible outside of class (including after class, office hours, e-mail, etc.)	1	0	0	0	0	6	6	66.67%	**5.00**
Generates enthusiasm for the subject matter	0	0	0	0	1	6	7	77.78%	**4.86**
Facilitates discussion and encourages participation	2	0	0	0	1	4	5	55.56%	**4.80**
Gives useful feedback on assignments	4	0	0	0	1	2	3	33.33%	**4.67**
Returns assignments in a timely fashion	4	0	0	0	0	3	3	33.33%	**5.00**

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

COMPSCI 227R

Cryptography

Comments

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

Course

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

This course was an excellent introduction to cryptography and the mindset necessary to prove things in a cryptographic context. I'm much more comfortable completing proofs that argue about the existence of theoretical adversaries and building crytographic primitives from mathematical assumptions. The psets were excellent and tied into the lecture notes very well. The notes themselves were comprehensive, and lecture was always engaging and interesting.

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

Very interesting material, Boaz is very enthusiastic

Evaluate the course overall.: **2 (fair)**

The problem sets were generally very good, and I felt like I learned a lot from them. Many of the problems were fun to think about and very educational. I liked the grading system (>100 points per problem set) as well.

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

This class is great at launching you to (close to) the frontier of understanding State of the Art crypto research topics.

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

The course goes through a lot of material.

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

I thought the course covered a lot of material, and I definitely learned a lot in the course. I also feel like there was a gradual progression of the material, so it wasn't too overwhelming.

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

Solid foundation of cryptography and exploration of many interesting concepts

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

Course

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

I recognize this is beyond the control of the course staff, but it's very helpful to have lecture videos for classes like this. On several occasions, I wished I had a video to reference when something I wrote down from lecture became opaque. Overall, no major recommendations!

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

Psets towards the end felt a little like busy work—the ones in the first half of the course were much more interesting. Lecture notes obviously still need to be polished. In general, there is a pattern where the easiest topics are longer than they need to be, and then the difficult parts are incredibly dense (with tons of inline equations, so it's not only difficult to understand but sometimes literally difficult to read).

Evaluate the course overall.: **2 (fair)**

I was hoping to really enjoy this course but unfortunately came away quite disappointed. Below are some suggestions for improvement: I did not learn much at all in lectures since reading was required before lectures and the lectures did not cover much material beyond the readings. Anything beyond the readings that was covered was done so rather hastily towards the end of lecture and in a relatively hand-wavy manner. Having required readings is not a problem, but I would like that if readings are required, lectures to assume the material covered in the readings and to spend more time on topics beyond the readings, carefully and rigorously. I think it is nice that readings (lecture notes) were often compressed/shorter than the corresponding expositions in textbooks (e.g. Boneh-Shoup), but in retrospect I think I would have preferred to simply read the textbooks. For one, the readings (especially later on in the course) had many typos and were often difficult to follow. Also, the lecture notes skipped some details/ lemmas that I would have preferred to read in full to obtain a better understanding of the material. I felt like the course tried to straddle both theoretical and applied aspects of cryptography, as well as cover recent advances in this field. While this is a good goal to have, I feel that the result was a sub-optimal coverage of many topics. I would have preferred, for instance, for the course to focus primarily on theoretical cryptography (including the newer topics), and for the recommendation to be for students interested in applied cryptography to take MIT’s course 6.857, which focuses primarily on applied cryptography. Finally, I got the impression from the class that LWE/lattice-based cryptography is a very active and promising direction of current research, and would have liked to spend more time on it. On the other hand, I felt that the course’s coverage of quantum computing was very lacking (e.g. talking about quantum computing without introducing the tensor product makes things more confusing, not more clear). Perhaps it would have been better to not cover quantum computing and use that time (as well as the time we spent some classes on applied aspects) to more thoroughly cover something like lattice-based cryptography.

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

The pace of the course is too steep. There are too many assignments (quizes, assignments every week). There is not nearly enough time to process all the materials we go over.

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

I think some of the lecture/lecture notes were very math heavy. I thought it was sometimes hard to understand the math, and providing some non-math intuition might be helpful. I found this issue with LWE, a little bit of zero knowledge proofs, and quantum computing.

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.): **3 (good)**

Boaz's lecture notes are still very much a work in progress. It reads very well (when it's complete).

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.): **4 (very good)**

First few problem sets are rather pedantic and longer, later problem sets felt more relevant (maybe shorter too).

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

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

The assignments take way too much time to do properly

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: **5 (excellent)**

Feedback was very timely and appreciated.

Evaluate the course overall.: **5 (excellent)**
Feedback you received on work you produced in this course: **2 (fair)**

Grading on psets was pretty wonky at times, especially towards the beginning of the course (all credit taken off for an answer that is exactly the same as the intended solution), but the extra credit meant this was not as stressful as it would have otherwise been

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

Grading in general was great feedback.

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

I think providing answer keys for missed questions could be helpful.

Section component of the course — Add Comments?

Course

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

Section component of the course: **4 (very good)**

-

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

Course

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

CS121 is probably sufficient, Boaz brings you up to speed in the first few lectures of the class.

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

This course requires proofs far above the level of 121 or 124. I would recommend taking (and doing very well in) 121 and 124. Otherwise, an advanced math course (25/55) is necessary. Programming not required in any form.

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

CS 121 or equivalent, preferably knowledge of number/group theory

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

Experience with proofs.

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

Mathematical maturity Proofs: induction, proof by contradiction, computational complexity big o analysis familiarity with analysis concepts and taking limits and convergence etc. discrete probability

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

Solid problem solving background

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

An understanding of theoretical CS and formal proofs are necessary, and strong understanding of linear algebra is useful.

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

Solid math background

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

Strong math background

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

Course

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

Comprehensive lecture notes, instructive problem sets

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

Interesting material. Low stress grading structure.

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

Well-done lectures, very interesting material, engaged instructor

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

This class is a fantastic introduction to the ideas in cryptography

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

Course

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

This class is pretty good for getting an introduction to cryptography. Boaz's problem sets were good and if you didn't understand the lecture the TFs Chining and Yueqi gave pretty good review sections. If you're interested in cryptography you should take this class.

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

This is truly an excellent introduction to cryptography. Boaz is a great lecturer and his course materials and lectures are very helpful. The class has a seminar-like feel to it due to the small size, and student input is frequently considered when choosing lecture direction and topics to explore (especially near the end of the semester). Keep in mind that this course is truly as difficult as rumored. If you're trying to satisfy the theory requirement as easily as possible, this is absolutely not the right class with which to do so. However, if you are interested in the mathematical and theoretical (not practical) side of cryptography, it won't disappoint you.

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

The course is a bit rough around the edges, but Boaz's enthusiasm is so infectious that it'd be hard not to enjoy the class (and start reading random crypto papers). Course policies also make for a very low-stress environment.

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

This class is a pretty good intro to crypto. Some of the problems on the psets are kind of tricky, but overall the work for the class is pretty chill, and the content is fairly interesting. Overall, would recommend if you're interested in the subject area!

Evaluate the course overall.: **2 (fair)**

This course covers a lot of topics in cryptography, some of which are recent/active topics of research in the field. Unfortunately, this meant that much of the material was covered in a sub-optimal manner (i.e. many details were skipped). There is not too much work, though, and the problem sets had some neat problems.

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

Boaz was very enthusiastic about cryptography and was very happy to talk with any student about what is going on in the class. He really touched upon many of the most exciting points such as fully homomorphic encryption and multi-party secure computation. A little note might be that sometimes his lecture notes are not the most rigorous, so I would suggest supplementing it by another reference. But I really liked Boaz and the class!

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

This class is great at launching you to (close to) the frontier of understanding State of the Art crypto research topics. If you're lucky like my partner and I, we even came out of the course with some crypto related research ideas (incubated from the final project of the course). It also moves really really fast, especially if you are a theory dilettante. That's the way Boaz gets the course to advanced topics by the end fo February... So you may feel you will be weeded out in the first 2-3 weeks if you can't keep up. So form a good group of 2-3 to support yourselves through the semester. Boaz is awesome and generates great enthusiasm for his course. Also your peers in the class without a doubt are some of the smartest students (CS and other areas too) so talk to them about the course topics!

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

This course is ridiculously time-consuming. You might regret taking it if you want to have a relaxed semester

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

A very hard course, but very interesting material.

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

Course

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

I grasp crytography in a much more fundamental way, and I'm more comfortable reasoning about adversaries and proofs regarding their existence. I deeply appreciate the complexity of issues that go into designing a cryptosystem and ensuring that a crytosystem makes the correct theoretical guarantees to provide security.

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

This course was a gateway to the world of cryptography research.

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

I learned a ton about cryptography and feel confident in my cryptography skills now!

Please comment on this person's teaching.

Barak, Boaz

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

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

Boaz was great. He's incredibly accessible and helpful when students struggle to understand a topic. I really appreciated all the time he put into the lecture notes and the class to ensure it went smoothly throughout the semester. I'm hoping to take another class with him in the future.

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

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

Boaz is one of the most enthusiastic professors I've had at Harvard. He is generous with his office hours time and offers help if you are interested in exploring research.

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

Evaluate your Instructor overall.: no answer

Boaz is hand-wavy in lecture at times.. although he is a great guy and an entertaining lecture, having a structured lecture would greatly improve this class. It's lovely to see that he is a great guy but the class would help from more clarity. Also a note for Boaz: it's very likely that students don't read all the lecture notes before lecture.. there is just too much work for this class if you do it right (read lectures, do the quiz properly, do the homework properly)

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

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

wonderful

Comments on the final project

Course

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

I enjoyed the final project substantially, but I think it would be helpful to have at least one "check-in" before the project is due. This would help to clarify expectations and ensure that students are on the right track (and perhaps help with any missing lemmas! :).

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

Think it's pretty good so far!

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

It was good! Although having both a final project and a final exam might have been a little overboard.

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

It's really hard but I'm glad my group got pushed to do the final project. I even am very excited to keep working on the novel part of the project in the semesters to come as a future research project (beyond the survey we did).

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

I liked the way that the project structure was open ended, and it meant that we could really work on something we were interested in.

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

Working on the final project was a ton of fun---do think I got to get more familiar with the area I studied and I'm definitely more comfortable now picking up a crypto paper and reading it.

What did you think of the ratio of theory to practice of crypto in this course?

Course

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

A lot more theory than practice, but since practical crypto is very systems-heavy I liked that there was more theory.

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

I liked the large amount of theory in the course and discussion of practical tools used to create primitives (RSA, Diffie-Hellman, etc.), but I would have enjoyed more discussion of practicalities for private-key crypto (Feistel ciphers, AES, basic cryptanalysis).

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

I didn't really miss applied crypto, except maybe cryptanalysis. I'd take a separate course on applied crypto though...

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

Thought it was pretty good!

Evaluate the course overall.: **2 (fair)**

I would have liked more theory (i.e. the focus to be primarily on theory, as this is a *2*-numbered CS course). I feel like having both theory and practice means that neither can be covered in sufficient detail/depth. In the future, if this course goes towards the more practical side of crypto, perhaps it should have a different course number, or at least have a more descriptive course title, such as "Applied and theoretical cryptography".

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

I thought it was optimal because I like theory and proof of cryptosystems. But sometimes I wish that the proof in class were a bit more rigorous and less hand-wavy, and maybe some solution sketches to problem set problem would be nice since they were quite challenging.

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

I think some of the problem set questions were great. E.g. the dictionary attack question was very memorable and quite practical. Bruce's lecture also helped supplement the practical side of the course. Overall the course skews toward theory (since I guess it's a theory course), so I'd characterize it's currently about 70/30 or 75/25 theory to practice. I'm ok with that ratio, because I'm a systems person and can draw the linkages myself, but maybe students coming from theory may think differently.

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

I love it. I prefer theory more than practice

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

I think it was good.

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

I thought the ratio was good---the theory was beautiful and gave a very broad framework in which to contextualize the practical applications that we saw.

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

i thought it was good - the theory component helps prepare for possibly taking other theory courses in the department and becoming comfortable with reading theoretical crypto papers. I feel like I would have gotten less out of a more explicitly applied class

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

Course

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

Quantum mechanics unit could be reworked; we could've used more time in class to go over the basics.

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

This course is excellent - I would say it could be improved by making section more attend-able for athletes. Section/OHs were always right in the middle of practice time.

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

The PSet grading varied heavily in difficulty between the first few and the last -- the end grading was probably optimal.

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.): **5 (excellent)**

The notes are great.

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

Lecture notes were super useful

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

(Boneh shoup should probably have been linked on piazza?)

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.): **3 (good)**

Psets are great. The exam was a bit long.

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

Problem sets were fair & helped me learn

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

A few typos/mistakes, and high variance in difficulty between weeks

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)**

Early PSet feedback was often less than ideally general/short.

Section component of the course — Add Comments?

Course

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

Section component of the course: **1 (unsatisfactory)**

Section time being during my lacrosse practice made them impossible to attend.

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

Course

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

Familiarity with proofs, via Math 25 or CS 124

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

CS121, CS124, STAT110 mandatory.

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

Mathematical maturity, familiarity with proofs. Knowing more number theory would have been useful.

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

Math on the level of CS121, Math 21, and enough number theory and statistics to answer math background questions.

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

You should have a strong background in both discrete math and computer science

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

Course

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

A difficult but instructive and comprehensive introduction to cryptography. A great addition to any computer scientist's education; useful in both applied and theoretical work.

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

Great class. Rigorous foundations. Starts from first principles and builds out from there. I like this. Others may not. Not over the top time wise. Psets were 10-15 hours per week, done in groups of 2. Grading was very laid back. Psets were often 125 points, but a 100/125 was considered full marks. All the problems were difficult, but I never felt like I was banging my head against a wall. Boaz is very funny (dry sense of humor) and appreciates how difficult the material is. Very responsive on Piazza and to all questions. Very knowledgable and passionate. TFs get the grades done in ~2 days. 100% theory, which I liked. 10/10

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

This is a good class, but you should be warned that it is all math (ie, not programming, and definitely not hacking). Boaz's lecture notes are an invaluable resource.

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

I was skeptical about how much I would enjoy crypto at first, and was relatively reluctant to take this course — I really only took it to satisfy my theory requirement. Now, I am thrilled I took it. Boaz is a fantastic and enthusiastic lecturer who genuinely cares about his students' learning. Some of the material is difficult, especially in the earlier weeks when you're just getting started with the basic abstractions and proof styles, but I powered through and really started to thoroughly enjoy learning as the semester progressed. Boaz tries to tie in the fundamentals of cryptography, the stuff you'll learn in any intro course, with some cool, advanced, and current areas of research like obfuscation and homographic encryption. Take this course — I don't think you will regret it!

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

This class is difficult, but in an incredibly engaging way--expect to gain an incredibly deep understanding of the fundamentals of cryptography and the cryptographic mindset of focusing on the adversary (besides the occasional positive definition). Read the lecture notes well, be able to reproduce any proof that isn't explicitly said to be unimportant to remember.

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

Course

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

Learned how to formally define security and how to achieve security with cryptographic tools.

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

I have a new appreciation for arguments around security vs privacy.

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

What it means to think about systems cryptographically and the adversary's mindset. Also just how _terrible_ a lot of crypto projects are.

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

I feel like I have a strong understanding of the ideas in cryptography

Please comment on this person's teaching.

Barak, Boaz

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

Lectures incorporated student participation very well! Lectures were sometimes hard to follow and could've used more grounding in examples.

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

Very responsive on piazza, which is much appreciated. Great lectures - engaging, clear, and funny. 10/10

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

I generally liked Boaz. Sometimes the longer proofs would be hard to follow but I got a lot out of lecture.

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

Boaz, excellent as always!

Please comment on your Section Leader's teaching.

Sheng, Yueqi

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

Attended all the lectures and was quick to help out the professor when needed.

Chou, Chi-Ning

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

Thanks for doing your best to be helpful!

Comments on the final project if you're doing one.

Course

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

A difficult exercise but worthwhile.

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

n/a

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

I'm still not quite clear on the details, and I hope mine goes well! (But it looks like the work is going positively, and I *think* I'm going to push the field in a useful direction?)

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

Doing the final project was so much fun! I got to think critically about the ideas that we've focused on in the class and apply the results to create a concrete product.

What did you think of the ratio of theory to practice of cryptography in this course?

Course

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

I think the ratio was good.

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

I liked the amount of theory. I think that some of the quantum stuff (where I don't really feel like I got enough quantum to do anything practical) could be substituted for some practice. I think adding a separate practice of crypto course would be great. I would love to learn more.

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

It felt like mostly theory, which was fine, but I would be interested in more practice.

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

Perfect!

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

I could have used a bit more tying things down to practicalities, especially at the end when the material got a lot more heady -- but otherwise very good.

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

I thought that focusing on theory was the right call. In general, it seems that theory both motivates the practice and allows you to engage with it on a deeper level. With that in