



# Fall 2021 Individual Report COMPSCI 127 - COMPSCI 227(FAS-COMPSCI 127-Cryptography 001,FAS-COMPSCI 227-Cryptography 001) Boaz Barak

Project Title: **2021 Fall Harvard FAS Course Evaluation**

Course Audience: **41**  
Responses Received: **36**  
Response Ratio: **88%**

---

## Report Comments

Note:

The order that the questions appear on this report is not the same as the way the questions were displayed to students. The order has been changed to make the report more readable.

---

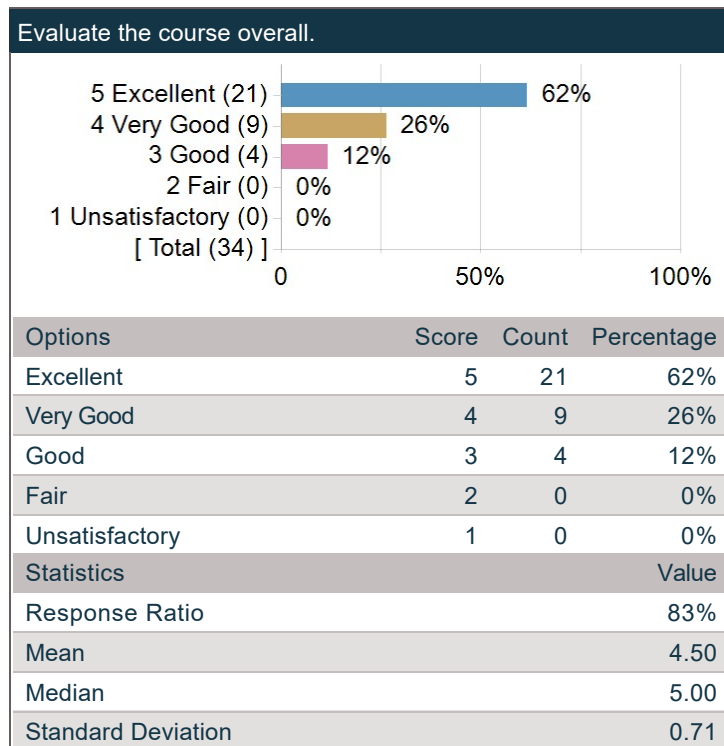
Creation Date: **Tuesday, January 4, 2022**

## General Course Questions

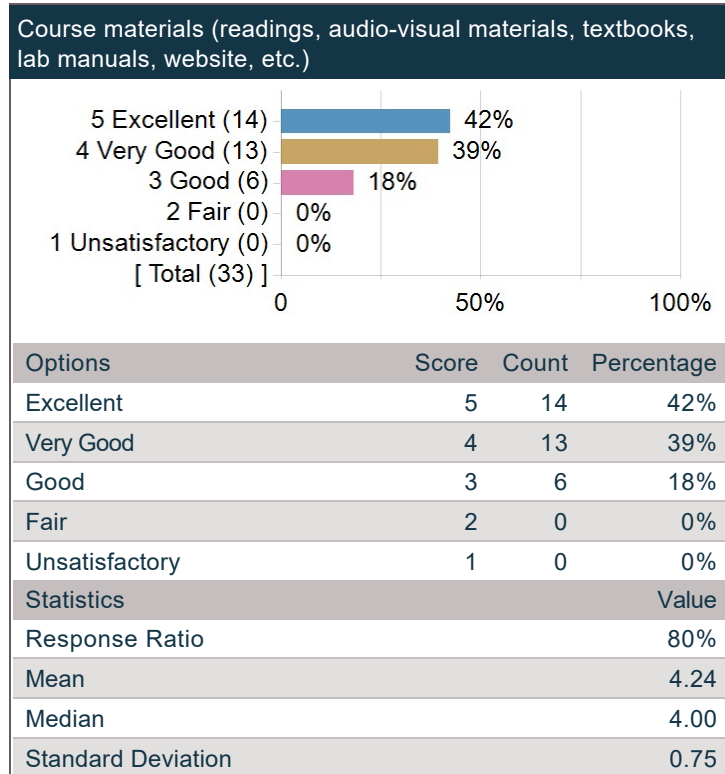
### Course General Questions

	Count	Excellent	Very Good	Good	Fair	Unsatisfactory	Course Mean	Dept Mean	Division Mean
Evaluate the course overall.	34	62%	26%	12%	0%	0%	4.50	3.94	3.96
Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.)	33	42%	39%	18%	0%	0%	4.24	4.07	4.03
Assignments (exams, essays, problem sets, language homework, etc.)	33	58%	36%	6%	0%	0%	4.52	3.75	3.81
Feedback you received on work you produced in this course	31	10%	19%	19%	26%	26%	2.61	3.55	3.62
Section component of the course	10	20%	40%	0%	20%	20%	3.20	3.80	3.90

### Evaluate the course overall.



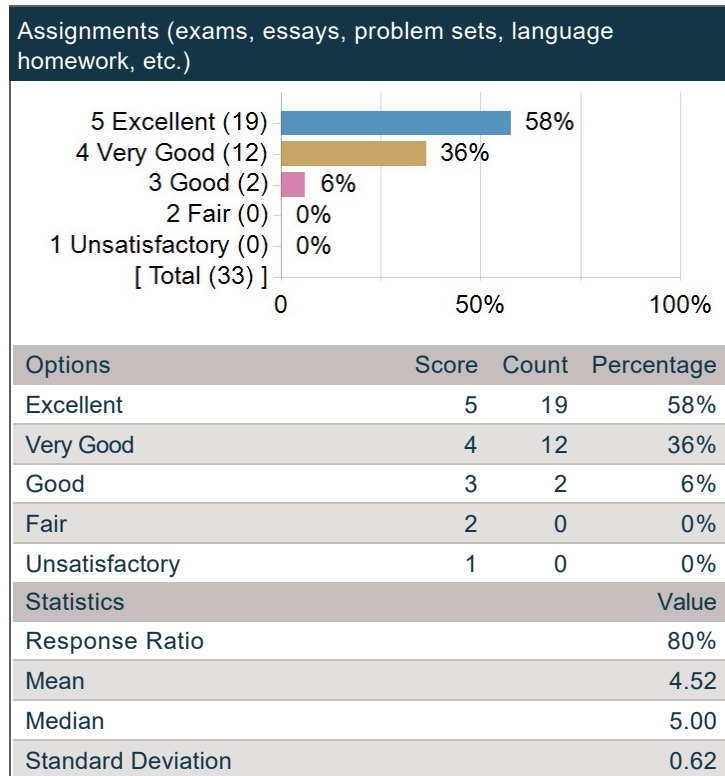
**Course materials (readings, audio-visual materials, textbooks, lab manuals, website, etc.)**



**Add comments about course materials?**

Comments
lecture notes were often tough to follow
The textbook is great, clear, and easy to learn from.
The lecture notes were excellent, and I thought the format of reading the notes before the lecture on Perusall worked extremely well.
I found the Katz–Lindell textbook to be very helpful but it only covered the first half of the course.
Boaz's lecture notes are a phenomenal resource.
Boaz writes the textbook himself, and, while this ensures it always matches the lectures, it also means that he does not have the benefit of a large publishing house helping him edit. There are occasional errors and the proofs are not always laid out in the most readable fashion. Algebra which should take multiple \$\$...\$\$ lines is instead forced into a single paragraph as part of the text.
As mentioned, the lecture notes could be vastly improved. Even grammatical errors and spelling could improve readability a lot.
The lecture notes were of course in progress, and that was communicated to us. This did lead to confusion every once in a while (from a typo or similar), but Perusall and/or class usually cleared it up.
Textbook is a great resource.
Normally, it's a bad sign when lecturers write their own textbook. But Boaz did an incredible job – the textbook is lovely.
don't provide adequate background info on topics needed for course
Some portions are a bit dense for self–reading (though lectures in class helped to clarify the concepts)
Lots of typos
It was nice having professor–written textbook!
Really good lecture notes! It still feels incredible to me that Boaz wrote a whole book for the class! I feel very lucky about this.
Solid overviews of concepts, but often felt very long and difficult to grasp the important concepts. Important summaries/ideas could be better highlighted.

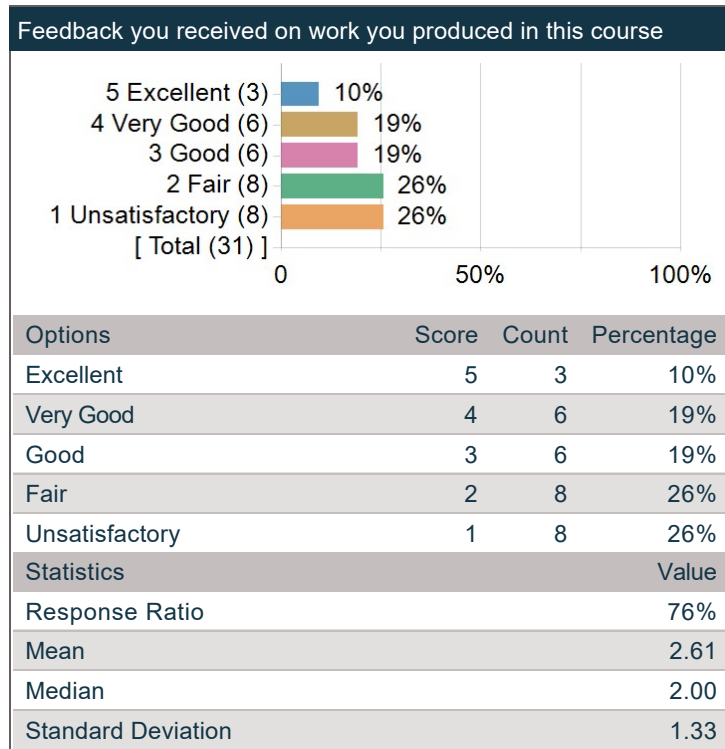
**Assignments (exams, essays, problem sets, language homework, etc.)**



**Add comments about course assignments?**

Comments
Problem sets are well-designed, and the "Problems worth 140 points; 100 points is a perfect score" is a wonderfully humane combination of extra credit, make-up work, and problem choice.
The problem sets are definitely when I actually learn the material well. However, sometimes there would be references to background knowledge that I'm not familiar with. Some extra information on intuition of the background knowledge would be very helpful.
The assignments were fairly well written and were usually quite relevant to the material that week (or the previous week). Sometimes questions were phrased somewhat ambiguously, but in general they were quite good.
Homework were very helpful in understanding the material. Maybe a bit less often would be nice.
The problem sets were genuinely really creative, and I enjoyed doing these problems more than those for any other class.
tough but fair
PSets are great for building understanding, and cover some really cool questions.
The psets were super helpful for understanding the material, and the bonus points were a very good pedagogical tool.
Well-written, interesting, got to the heart of the issues of cryptography.

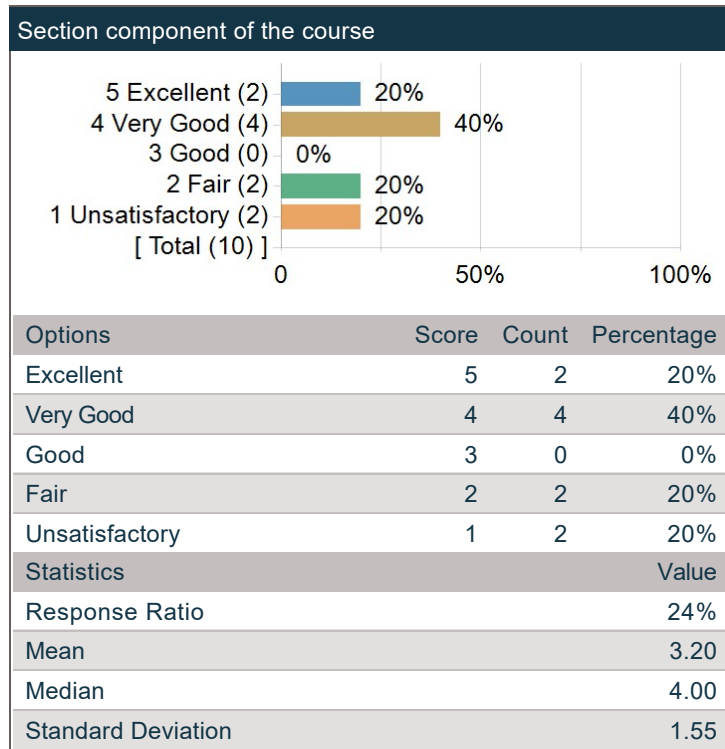
**Feedback you received on work you produced in this course**



**Add comments about course feedback?**

Comments
Very delayed on grading, I have NO idea how I have been doing on psets and lack feedback going into the exam.
The grading was somewhat slow which made it hard to figure out how well I was doing in the course.
Could be more timely
I wasn't able to get back half of my problem sets before the final.
The only feedback we got was on gradescope. It was quite limited, and often very, very late. In the future, I'd really like to see more timely feedback on my assignments, so I can improve using it.
Homework were basically not graded at all after homework 4.
More than half of my homework assignments have not been graded at all (as of December 20).
Feedback took months, and was usually just a grade out of 100. I think I received two individualized comments the whole semester.
Homework is slow to be graded; my regrade request was not handled for the entire semester.
My last graded assignment was released in September.
The HW was graded incredibly slowly. By the end of the semester, we only had our first 4 assignments graded, and the most recent among these was submitted all the way back in Sep 30 (so we didn't receive any feedback for any assignments submitted in the last 2.5 months of the course). This made preparing for exams etc very difficult since this class frequently employs unique methods of problem-solving that students hadn't encountered before (e.g. reduction from one adversary to the other, hybrid argument, etc etc) and we never really got that much practice employing these methods in our proofs since we rarely got feedback.
I have already commented on this — course feedback has been VERY bad. The TFs literally haven't returned us anything since September. I really can't understand how such negligence from the TFs has been permitted throughout ALL semester. And the few grades we got back for the psets had bad grading rubrics which very really not informative.
Very detailed, although far too late to be useful.
Was a little delayed, so sometimes it was difficult to figure out what topics were misunderstood until too late

**Section component of the course**



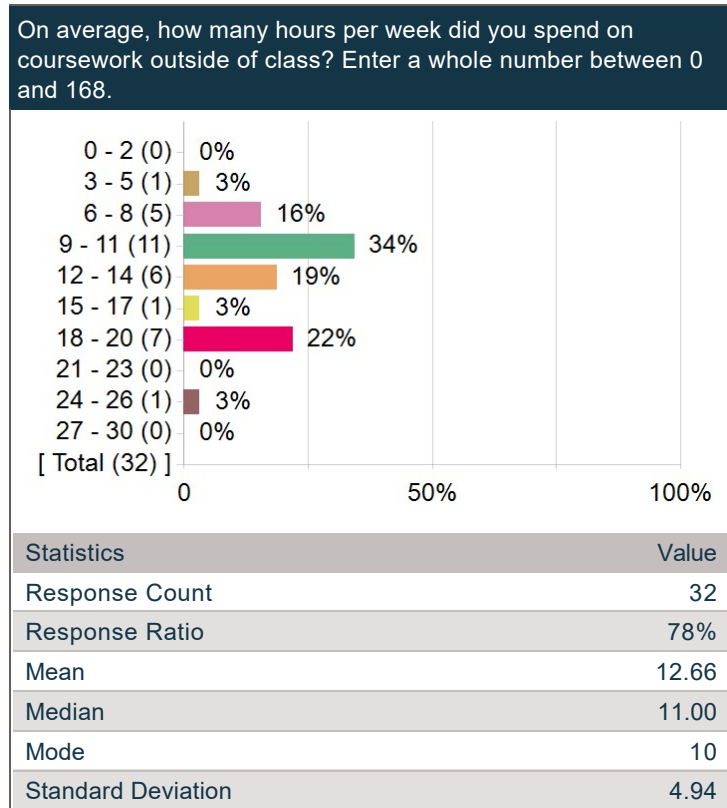
**Add comments about the course section?**

Comments
Richard's lecture on OWF => PRG was really awesome!
There needs to be one.
Well, there was no course section! Which I also don't understand how this has been allowed. Thanks to Emil for holding 2 review sessions though.
Infrequent, but very helpful when there were sections!

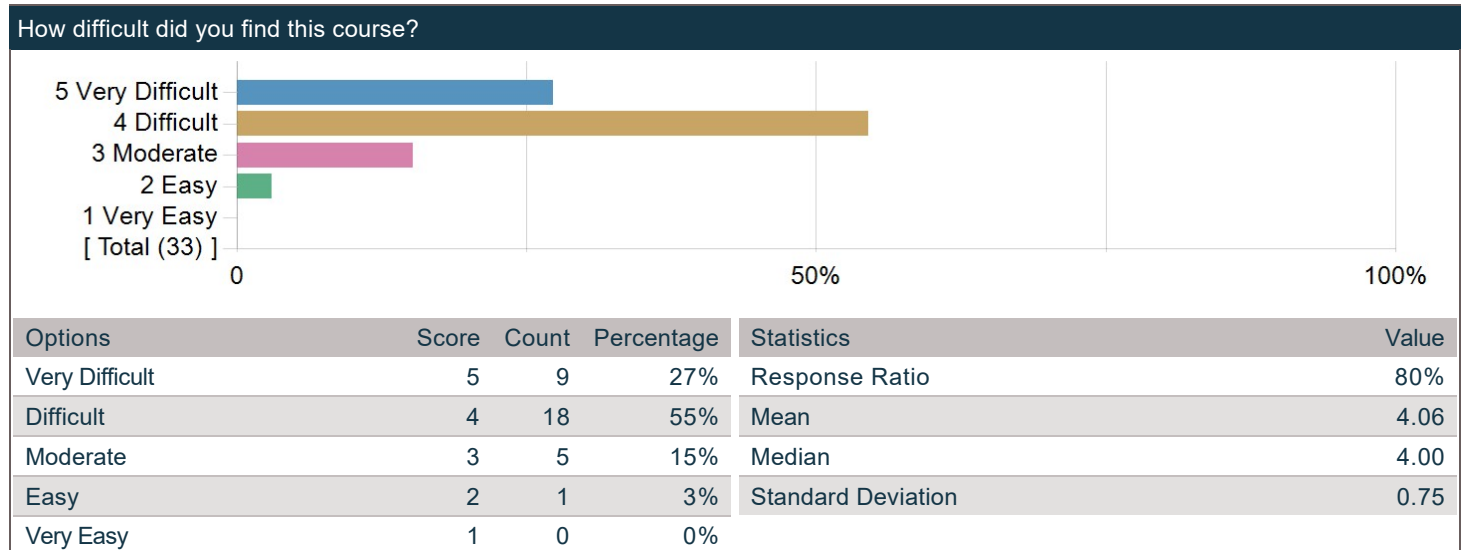
## Requirements - What did this course require of you?

On average, how many hours per week did you spend on coursework outside of class? Enter a whole number between 0 and 168.

Frequency chart and mean excludes students who answered 31 or more hours.



## How difficult did you find this course?

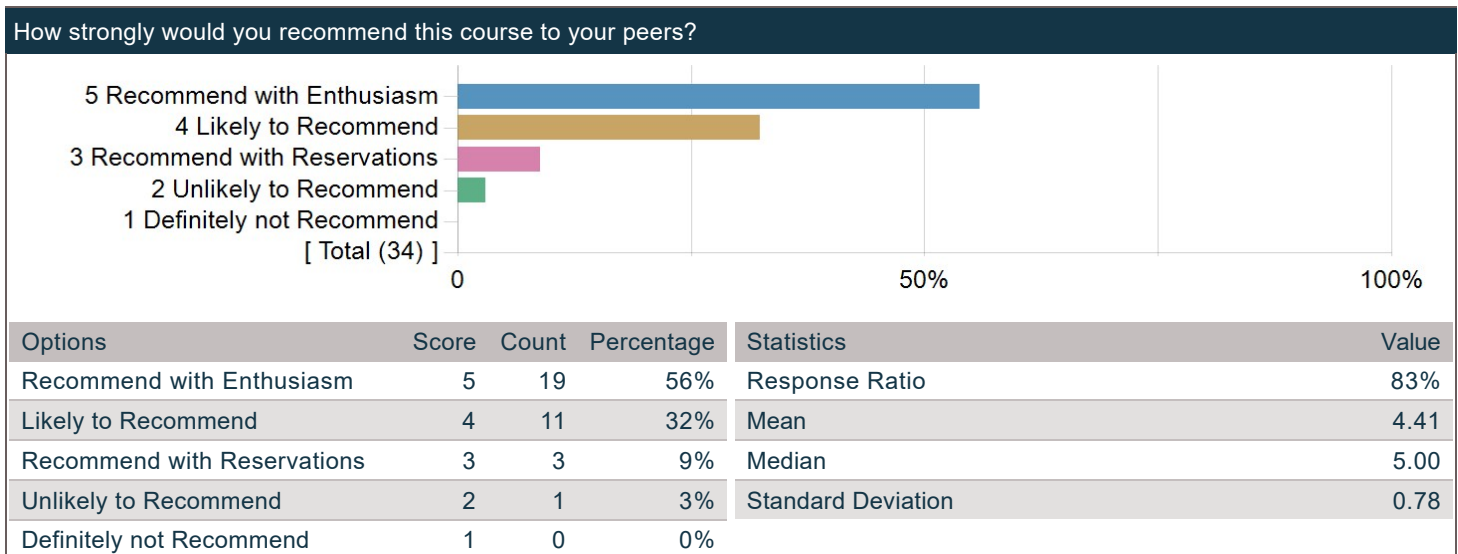


**What was/were your reason(s) for enrolling in this course? (Please check all that apply)**

Options	Count
Elective	19
Concentration or Department Requirement	17
Secondary Field or Language Citation Requirement	5
Undergraduate General Education Requirement	0
Expository Writing Requirement	0
Foreign Language Requirement	0
Pre-Med Requirement	0
Divisional Distribution Requirement	0
Quantitative Reasoning with Data Requirement	0

**Recommendations - Would you recommend this course?**

**How strongly would you recommend this course to your peers?**



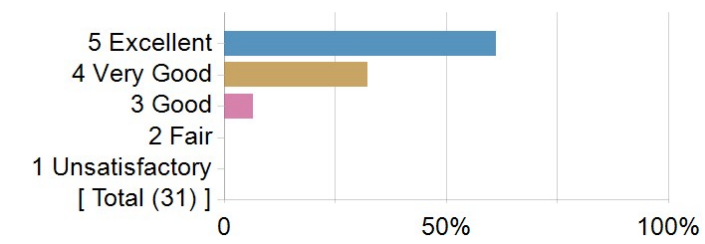
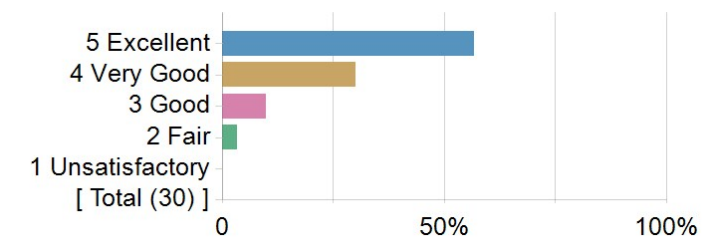
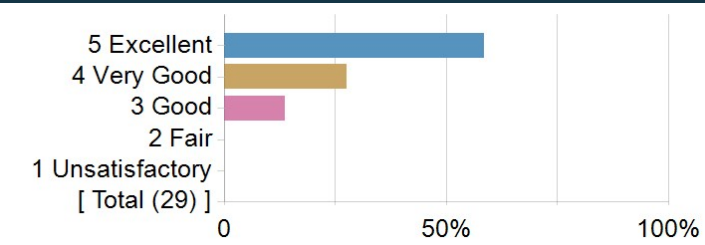
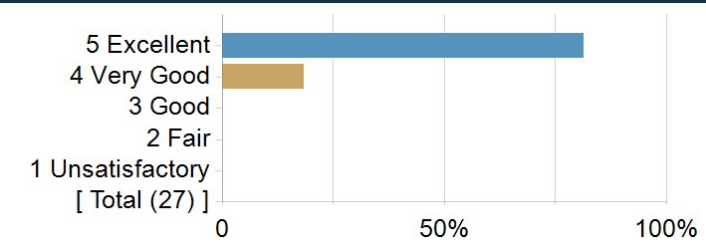
**Evaluation of Instructors**

**General Instructor Questions**

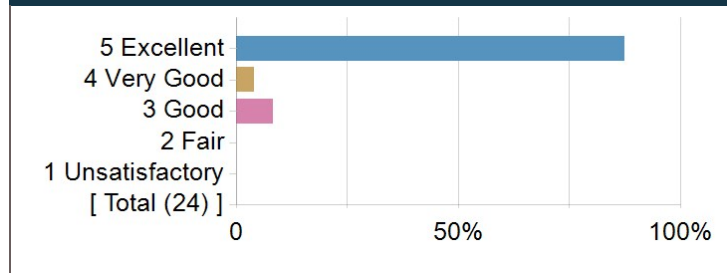
	Count	Excellent	Very Good	Good	Fair	Unsatisfactory	Instructor Mean	Dept Mean	Division Mean
Evaluate your Instructor overall.	31	61%	32%	6%	0%	0%	4.55	4.31	4.32
Gives effective lectures or presentations, if applicable	30	57%	30%	10%	3%	0%	4.40	4.22	4.20
Is accessible outside of class (including after class, office hours, e-mail, etc.)	29	59%	28%	14%	0%	0%	4.45	4.05	4.22
Generates enthusiasm for the subject matter	27	81%	19%	0%	0%	0%	4.81	4.43	4.41
Facilitates discussion and encourages participation	24	88%	4%	8%	0%	0%	4.79	4.26	4.30
Gives useful feedback on assignments	7	57%	14%	0%	29%	0%	4.00	4.11	4.17
Returns assignments in a timely fashion	8	0%	13%	13%	13%	63%	1.75	3.95	4.04



**Instructor**

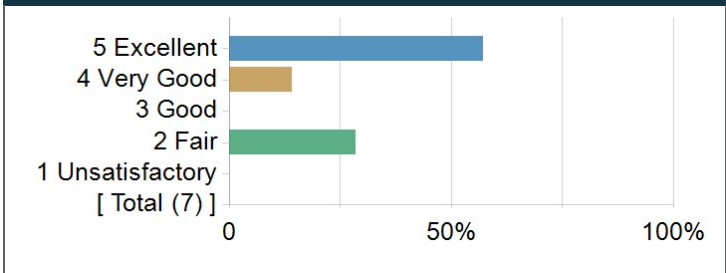
1. Evaluate your Instructor overall.				2. Gives effective lectures or presentations, if applicable			
							
Options	Score	Count	Percentage	Options	Score	Count	Percentage
Excellent	5	19	61%	Excellent	5	17	57%
Very Good	4	10	32%	Very Good	4	9	30%
Good	3	2	6%	Good	3	3	10%
Fair	2	0	0%	Fair	2	1	3%
Unsatisfactory	1	0	0%	Unsatisfactory	1	0	0%
Statistics			Value	Statistics			Value
Response Ratio			76%	Response Ratio			73%
Mean			4.55	Mean			4.40
Median			5.00	Median			5.00
Standard Deviation			0.62	Standard Deviation			0.81
3. Is accessible outside of class (including after class, office hours, e-mail, etc.)				4. Generates enthusiasm for the subject matter			
							
Options	Score	Count	Percentage	Options	Score	Count	Percentage
Excellent	5	17	59%	Excellent	5	22	81%
Very Good	4	8	28%	Very Good	4	5	19%
Good	3	4	14%	Good	3	0	0%
Fair	2	0	0%	Fair	2	0	0%
Unsatisfactory	1	0	0%	Unsatisfactory	1	0	0%
Statistics			Value	Statistics			Value
Response Ratio			71%	Response Ratio			66%
Mean			4.45	Mean			4.81
Median			5.00	Median			5.00
Standard Deviation			0.74	Standard Deviation			0.40

**5. Facilitates discussion and encourages participation**



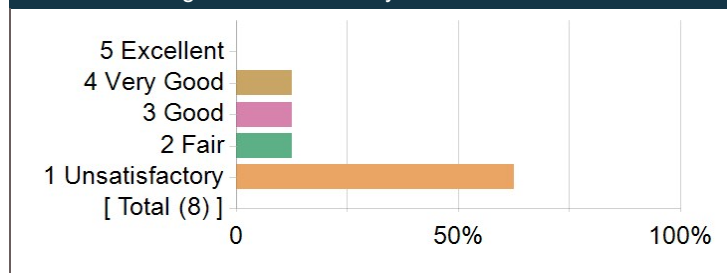
Options	Score	Count	Percentage
Excellent	5	21	88%
Very Good	4	1	4%
Good	3	2	8%
Fair	2	0	0%
Unsatisfactory	1	0	0%
Statistics			Value
Response Ratio			59%
Mean			4.79
Median			5.00
Standard Deviation			0.59

**6. Gives useful feedback on assignments**



Options	Score	Count	Percentage
Excellent	5	4	57%
Very Good	4	1	14%
Good	3	0	0%
Fair	2	2	29%
Unsatisfactory	1	0	0%
Statistics			Value
Response Ratio			17%
Mean			4.00
Median			5.00
Standard Deviation			1.41

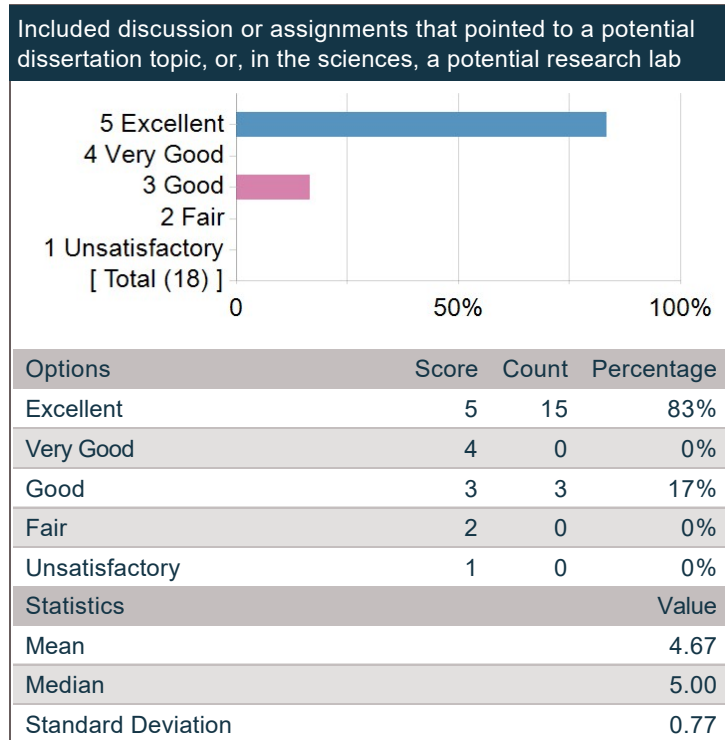
**7. Returns assignments in a timely fashion**



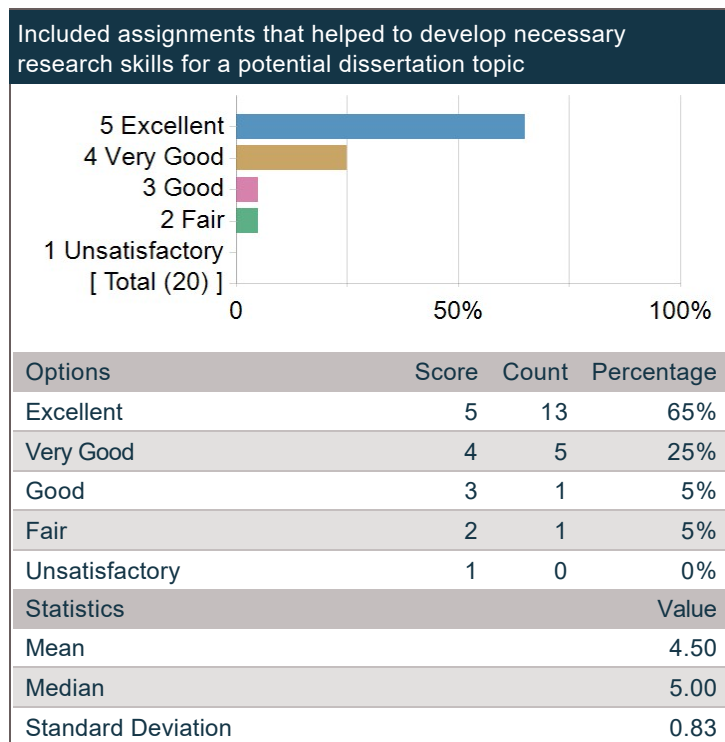
Options	Score	Count	Percentage
Excellent	5	0	0%
Very Good	4	1	13%
Good	3	1	13%
Fair	2	1	13%
Unsatisfactory	1	5	63%
Statistics			Value
Response Ratio			20%
Mean			1.75
Median			1.00
Standard Deviation			1.16

## GSAS Module Questions

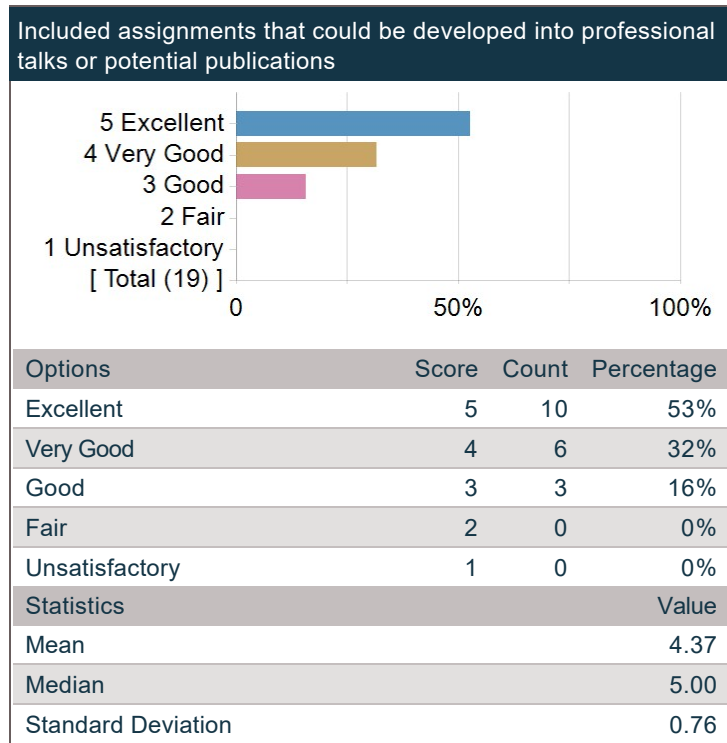
**Included discussion or assignments that pointed to a potential dissertation topic, or, in the sciences, a potential research lab**



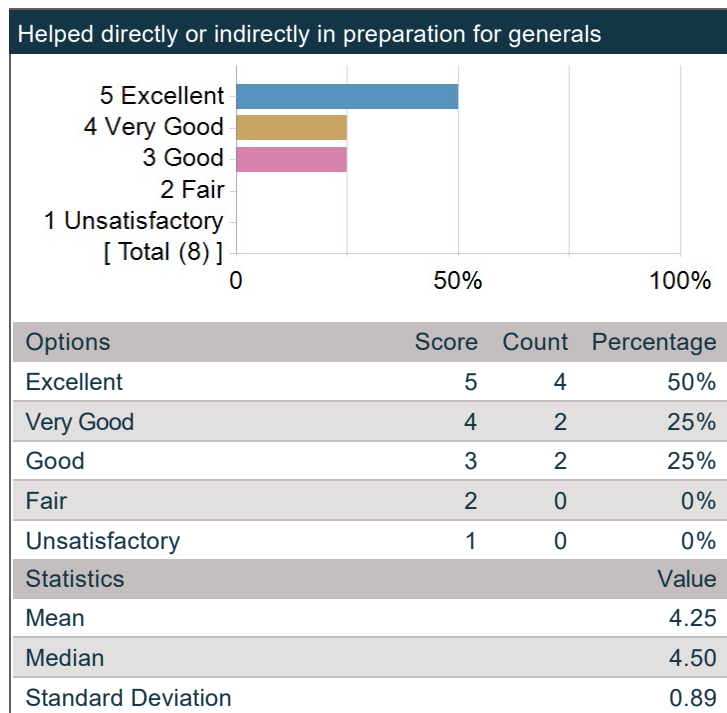
**Included assignments that helped to develop necessary research skills for a potential dissertation topic**



**Included assignments that could be developed into professional talks or potential publications**



**Helped directly or indirectly in preparation for generals**



## Comment on aspects of the course as they relate to professional development, including preparation for future teaching.

Comments
For this class's final project, Boaz put my group in contact with Amit Sahai, an expert on multi-linear maps. Using the advice of Boaz and Amit, my group was able to create the first ever (potentially secure) ciphertxts using witness encryption. See <a href="https://arxiv.org/abs/2112.04581v1">https://arxiv.org/abs/2112.04581v1</a> .
Boaz did a really good job of approaching this course from a research perspective — always linking to the actual papers on Perusall and commenting on the research developments of the field. Also, the final project really helped in learning more about research in cryptography. I do wish we had had more guidance / supervision on the final project, since we literally did it on our own.
Sorry, one thing that I would change about the course that I forgot to mention before: please don't change the class to please the "crypto bros". It is great as it is, and sometimes it felt that Boaz wanted to bring cryptocurrencies into the table, but it just felt forced and I also think that this is a controversial topic. Similarly, the Eli Ben-Sasson felt unnecessary and was essentially a business talk, which I don't think matches the spirit of the class.
Very useful learning about the frontiers of research in cryptography. Did not help with prep for future teaching

## General Course Questions - Comments

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

Comments
learned a LOT
The content is among the most interesting math content in CS imo. The homeworks are mostly actually enjoyable to do in that they are properly challenging and actually help further your understanding of the concepts seen in class. It covers a lot of actually cool stuff that I think will be more relevant as crypto takes over the world.
The content in this course is great, cryptography is very interesting mathematically and Boaz's textbook is quite good. I enjoyed class, loved the STARK guest lecture, and felt I learned a lot.
It was awesome how fast this class moved and how many different topics we covered. This was definitely one of my top 5 classes of all time.
Very interesting. I really enjoyed the problem sets. The final project was also very fun and interesting.
Awesome material, Boaz is a great prof, psets were a good balance — they rly helped my learning but weren't too much work.
Barak Boaz is very passionate about the material. The class did a good job of linking material together as we looked at more advanced topics later on.
Lecture notes are good, staff are supportive and care for students
The material was wide-ranging and never dull, even as the same themes — thinking in terms of adversaries, compiling less-secure algorithms into more-secure ones — were reiterated. Problem sets were never impossible but were always challenging, and really ensured that you understood the material.
The professor is clearly an expert in the field. The depth and breadth of the content is unparalleled in any other cryptography course. I also like the connections between real-world examples of how crypto systems are broken with the content we learned in class. It builds intuition on why cryptography terminologies are defined the way it is.
The material is taught quite well – it's clear in lecture that Boaz is very knowledgeable, and he does a good job of sharing that with us.
Interesting material, relatively accessible course staff, difficult but manageable problem sets
Very interesting topics, great professor, engaged class.
The course moves quickly and covers a LOT of state-of-the-art content. Boaz's textbook is also excellent.
Very well done psets and course material was very interesting. Especially the breadth made me feel well versed to read cryptography papers and the project was a good way to put those skills to the test.
This course does an excellent job of introducing the broad and evolving field of cryptography. Beginning with the typical topics in a crypto course (private key and public key crypto), this course then pivots into some of the more cutting-edge topics like homomorphic encryption. It really gives a solid overview of the field as a whole, its history, and where it may head in the next decade.
Additionally, this course does a great job of equipping students with the tools for thinking like a cryptographer. The homework assignments are excellent in this aspect. They require a student to think through some of the thornier aspects of cryptographic proofs and protocols and then end result is a solid grasp on the material.

Comments
Provides a broad overview of cryptography while maintaining rigor. The course is well taught, the lecture notes are throughout, and the homework is very helpful for gaining further understanding of the material.
very interesting material
Pretty well paced throughout, touching on topics from the foundation of modern cryptography to the state of the art research.
Covers a broad range of topics; latter half of the course is incredible.
The subject matter is phenomenal. The course textbook is, although a bit rough in places, a fantastic resource.
1. I thought the breadth and depth of the course was amazing. To anyone interested in the theory behind how majority of modern communications and systems security works, I think this is a great course. 2. I liked the structure of the course where 2/3 covers fundamental cryptographic objects, and the last 1/3 covers a wide range of modern topics. 3. Guest lectures! 4. Professor Barak is the one to learn the course from, of course.
Very interesting topics and great lecture notes.
The material is REALLY cool, and Boaz is obviously very enthusiastic about it, and he really cares that we like it and enjoy it. Also, the pssets were super helpful — they REALLY helped me in grasping the concepts and they never felt frustrating. So they were hard enough to make me feel that I was really learning the material, but not enough that it would feel like too much. Also, I really liked that the pssets had bonus points — it made me feel not anxious about the pset and strive less for "perfection" and more about actually learning the material. This is a really good learning pedagogy, I think, and similarly for the hints. I also liked reading the notes before class, and Perusall proved to be a really useful place of discussion.
Covers a lot of content, very solid overview of a lot of cryptography. Fairly low stress with additional opportunities for credit on homework and such.
Thorough, exciting tour of modern and (post?)–modern cryptography

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

Comments
some lectures were SO hard to follow– e.g. quantum computing if you didn't already have mastery of the subject before.
Faster turnaround with grades would be very useful. It is hard to know how we are doing in the class and to avoid recurring mistakes if we don't get grades in a timely fashion.
While quantum is interesting, the amount you can touch on in a few lectures isn't that much. I would've preferred to learn more about ZK proof systems more :)
There was way too much homework for this class. I really appreciated when we'd have 2 weeks to do a homework instead of 1, and I thought that was a more reasonable pace. And I thought it was absurd that we had a homework due with 6 days notice one day before the project was due. It made it so that we didn't have as much time to work on the project in that final week as we should have. If you make any changes to the homework load for future iterations of the course, I would especially recommend lightening up toward the end so that students have more time to work on projects.
The teaching staff this year was incredibly poor. An assignment handed in on Oct 7 still has not been handed back.
The textbook is clearly still a work in progress, and had a number of errata. The extent to which you were supposed to engage with it was also unclear: are three comments on every reading enough for a perfect participation grade? Five? Twelve?
The lecture notes could be improved a lot. There are many typos and grammatical errors that would confuse students. There are also not enough TFs/office hours. Many of the time slots I would have class/research and wouldn't be able to attend the office hours. In addition, the TFs also were not able to grade half of my problem sets.
The flipped classroom nature of the course was quite frustrating. I often spent hours reading the lecture notes, taking notes from them, and looking for typos in them, only to arrive in class and write nothing down, as it had all been covered in the notes. That being said, the lectures usually did take a different approach (a more high-level approach, usually), which gave me another way to look at the problem.
Having to read lecture notes before class is annoying and I would be willing to sacrifice a number of things to not have to do that.
Maybe choose one final project or final.
Minor nit – it would be nice to have explicitly the "security game" for PRG, PRF, CPA–secure private key, CPA secure public key, CCA secure private key, CCA secure public key, etc. all written out (for most of these you can infer it pretty easily, but having it explicit would be nice).
The course notes were a little messy and especially as a first experience the mistakes made it really difficult to learn.
This course moves at a very quick pace and so I do wish that we had received feedback on assignments more rapidly. I know it's

Comments
tough with larger assignments and a significant class size, but it really would have been super helpful if we could have received feedback in a more timely manner so that we could incorporate feedback into future homework.
expects students to learn a lot of material outside of class
Perhaps more time could have been spent on going through proofs in the private key section in class. I felt it was not easy to get used to the adversarial way of thinking until later on in the course
A bit of more explanation in the first half, though you eventually pick up everything you need to know.
The course would benefit from more frequent sections.
<ol style="list-style-type: none"> <li>1. Grading of assignments are about 2 months behind. Especially when the type of questions asked are very similar across problem sets, I think having the problem sets not graded was quite annoying.</li> <li>2. Having problem set, project, final exam all due on the same week was somewhat brutal.</li> </ol>
In dire need of a section component.
<p>The course staff — please hire TFs who actually care about the class next time. Boaz was fantastic but the teaching staff was absolutely not matching the same expectations. I have probably never seen such uninvolved TFs in any class that I have ever taken. First of all, we have received NO grades and NO feedback since the end of September, despite having turned in weekly psets since then! This is really bad pedagogically, and it has really been bothering me. I think that the expectations for TFs should be very explicitly stated at the beginning of the semester, and the professor should make sure that they are fulfilled. Does Boaz know that no psets have been graded (still!) since pset 3? And if so, why were there no follow-ups with the TFs? Also, there have been no sections at all for this course during all semester (except for 2 review sessions), despite it being asked explicitly in our mid-semester feedback forms. Especially given that we don't really go through the proofs in class, sections for CS 127/227 just feel like a basic need. For example, it was very unclear to everyone how to <u>actually</u> do a ZK proof, and we could only rely on pset solutions because i) ours were not graded and ii) no sections existed where we could go over it. Also, some of the TFs did not seem to be understanding the material at all, and I stopped attending office hours because I felt that they were as lost as I was, so I had to go ask classmates instead. I think that asking for i) grading our psets, ii) holding sections, and iii) knowing the material is the bare minimum that TFs need to satisfy. And I think that it is a shame for the course because Boaz did a really good job, and everything on his end was fantastic.</p>
Would have preferred less reading/material, felt like a very intense grind throughout and difficult to absorb concepts. No group project, since at the time of proposal we do not know enough to conduct original research.
Possibly a student-led component?

## Requirements Comments - What did this course require of you?

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

Comments
CS121, STAT110, strong technical background.
Some proof-based math, any CS theory class would probably be useful as background but not necessary. Basic probability at the level of the first half of stat 110.
Basic probability theory, being able to write proofs. Honestly, if you're willing to learn, you can pick up most constructions without too much outside work. Of course for the more advanced stuff, group theory is always nice :)
Being comfortable reading and writing proofs.
Probably CS 121 and STAT 110 would be useful. Number theory and linear algebra could also be useful.
Mathematical maturity, some familiarity with probability.
familiarity with theorem proving and computer science theory topics
Strong mathematical foundation, some theoretical CS/algorithms knowledge may be useful (some similar ideas)
A lot of math, especially some statistics. No programming/CS at all.
COMPSCI 121, or some other theory course. Some idea of group theory would be helpful but not necessary. I'm not the best at math (MATH 25A), so the problem sets took me quite a while (11 hrs/wk). However, I do have some CS intuition which helped. Not to mention a lot of the theorems in cryptography are unproved! I think if you did MATH 25 and above and take COMPSCI 121, you are in good shape. Some people in the class I know didn't even take COMPSCI 121 or something similar.
Students should be prepared to prove things; preparation from a CS 120, 121, or 124 background is probably good to have.
CS 121/CS 124
CS 121 is nice to have, but isn't strictly necessary.
A strong background in logical proof-writing and exposure to theoretical computer science. Exposure to linear algebra and abstract algebra is extremely helpful.
Being very comfortable with proofs.
need strong bath ground in number theory for later half of courser
Comfort with mathematical proofs, some basic statistics.
Statistics
Familiarity with mathematical reasoning, statistics at the level of Stat 110, familiarity with some basic notions from complexity theory.
1. Very strong probability background. Lots and lots of probability. 2. Majority of the problems are reductions, so courses like CS 121 or 124 would help quite a bit.
Some number theory and theoretical cs (120 or 124)
Mathematical maturity and theory CS.
Very strong mathematical maturity and background. CS 121 helpful as well.
Some familiarity with general topic in CS theory



## Recommendations Comments - Would you recommend this course?

**What did you take away from your experience in this course? What did you learn? How did this course change you?**

Comments
I learned about the mathematical underpinnings of cryptography. This course changed how I think about computational security and taught me about state-of-the-art crypto subjects that I think will be increasingly relevant as cryptocurrency technology becomes ubiquitous.
Don't roll your own crypto.
The material was just so interesting. I am now incredibly interested in learning more crypto, and I gained a very strong appreciation for the beauty of cryptography as a field and for the cryptographic perspective.
The formal definitions of security in computation. In addition, how we can reduce one definition to another and thinking critically on ways to break security of a proposed cryptosystem.
While I had some notions of cryptographic primitives, this class really helped formalize them, which was great.
It was like solving logic puzzles! I learned a lot about security and how to think from an attackers perspective.
This is one of the greatest courses I've ever taken at Harvard (after Math 55). A really interesting subject matter, taught by a world expert (who freaking invented indistinguishability obfuscation).
Mainly, how to think like a cryptographer and what the field of cryptography looks like. I feel that I have a solid understanding of topics like private and public key crypto, zero-knowledge proofs, fully homomorphic encryption, and multi-party secure computation.
I largely took this course due to my interest in information theory. This course gave me an interesting perspective on how the concepts from information theory can be applied to conceal information.
Boaz is very knowledgeable and passionate about this field, and it was such a wonderful experience learning from someone who has played a part in several recent developments of the field. Cryptography turned out to be a much richer field than I originally realized, and this course helped me to appreciate the theoretical foundations that give much of the protocols we use today their security guarantees.
This is honestly the most interesting course I have taken so far at Harvard. It gives you an entirely new way of thinking about things, and shows you how far people have come in the past hundred years in the field of cryptography, how they can build things that one would not imagine were possible. I think I will forever take with me a line Boaz said in one of the later lectures, that at the start, the greatest failure in cryptography was the failure of imagination.
1. Fundamentals of cryptographic systems. 2. Enough knowledge to understand how modern communication systems work!
Really cool new topics and ideas that are relevant to almost all parts of contemporary life. The problem solving strategies we learned in class and the assignments were often very cool and useful.
Cryptography is SO cool — I really, really like it and I would like to pursue it further, and this is thanks to Boaz. Also, I feel so privileged to have learned it from someone like Boaz, who is literally a giant in the field. I feel that this is what makes Harvard worth it — being taught a topic by a star in the field and who has written a whole book about it. And Boaz really did a great job of making us feel enthusiastic about cryptography and connect us to the research in the field. For example, I really liked the activity in the last day of class where we looked at the most recent papers on ePrint and read them — it was at that moment when I realized how much I had learned! In a nutshell, courses like this is what makes me feel so lucky about my educational experience at Harvard.
Interesting to understand the core concepts behind mathematical security in cryptography. A very exciting field!
Very cool topics!

## Instructor Comments

Please comment on this person's teaching. (Your response to this question may be published anonymously.)

Comments
Very enthusiastic. Sometimes the lectures were a bit chaotic and the stuff is written on the board was hard to read. Someones also the explanations of certain topics were unclear. But would always stop when people had questions.
Great at teaching, wrote a great textbook.
I liked his jokes. I like the way he structured the course to have a lot of bonus points.
Boaz is awesome. Very enthusiastic about the material, great lecturer, and a funny guy.
I love Boaz! I do feel like there's a disconnect between the proofs in lecture and the lecture notes though. Boaz's lecture is clearer (at least for me) and builds intuition/the big picture better than the lecture notes. I especially like the small group sessions when we would discuss about security of different proposed systems. I would suggest making sure everyone has a chance to explain their proofs though, or even a rough sketch. I feel like it was mostly one or two people giving proofs during class even though I had a rough sketch of the proof.
Boaz is a great teacher; he really knows the subject, having done research in it, and he spreads that with us in an engaging manner. My only comment would be it seems he's really busy, so maybe if he had slightly more time he could stay after a little to answer questions.
Boaz is absolutely the best professor. He is so fascinated with the topic that even people who find it boring become fascinated. He gives great lectures and I love that each pset has a ton of extra credit because it makes the class way less stressful.
The textbook is REALLY good. The lectures were pretty good. The content was REALLY good.
Lectures are the greatest part of this course. The readings are dense and Boaz always explains the more difficult concepts in easier to understand ways.
Great teacher, definitely enthusiastic about the topic and is very good at conveying that enthusiasm.
Boaz generates so much enthusiasm, and he has made me love cryptography. One thing though is that I feel there is too much hand-waviness going on in class. Even though Boaz is very good at conveying "high level ideas", the rigour cannot be overlooked, and sometimes explanations felt too sketchy and less mathematical.
Very interesting presentations. Loved the slide presentations, the whiteboard presentations were a bit harder to follow — would appreciate clearer delineation for these presentations.
Very engaging lectures