Spring 2020 Course Report COMPSCI 127 - COMPSCI 227(FAS-COMPSCI 127-Cryptography 001,FAS-COMPSCI 227-Cryptography 001) Boaz Barak

Project Title: **2020 Spring Harvard FAS Course Evaluation**

Course Audience: **36**
Responses Received: **31**
Response Ratio: **86%**

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, December 15, 2020**

Course Questions

Considering only the first half of the course (on campus), what were the strengths of this course? Please be specific and use concrete examples where possible.

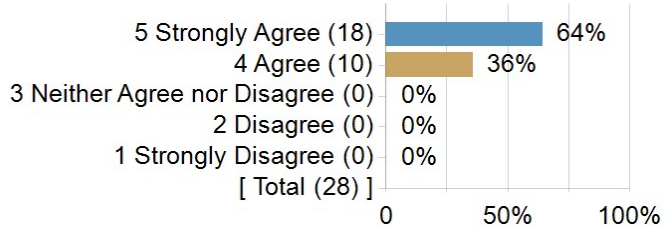
Comments
Interactive lectures and group dynamic of class
Learned a lot from the problem sets, lectures, and textbook, and exercises during lecture kept me engaged! also really built a solid foundation for cryptography + reduction proofs.
Lectures were very good at giving the students ample opportunities to discuss among themselves and engaging with the material.
How much we cover. By doing the readings before class, Boaz gets to talk about whatever he thinks is cool. That is great :)
Overall, the lectures were good, the TFs were helpful and friendly, and the material was interesting and engaging.
Interesting material, homework problems helped in understanding, lectures managed to not be the same as the lecture notes, lecture notes pretty comprehensive
This course covered fascinating and rigorous material, was engaging, and had problem sets that were well designed for us to engage with the nuances of what we learned in class. Expecting students to read the material before class allowed classes to be much more discussion–based (at least for a lecture) and allowed lectures to bring the material together.
Boaz and the student community in this class made it really enjoyable. Boaz also posted a lot of extra resources, which was really nice as I approached this class with less of a math background.
I really liked how Boaz encouraged participation throughout lectures. I also really liked the sense of community and collaboration built into the course.
Great course staff, good lecture notes, interesting HWs
Boaz was SO accessible. There were a lot of tricky aspects to this class and a lot of the concepts and proofs were counterintuitive, and Boaz was always available during and after class, in office hours, etc. to give his thoughts, often in ways that were substantially different from what he did in class, complementing them and helping us understand more.
This course was very good and I learned a lot. The Psets were of high quality.
I loved this course! Cryptography is so interesting, and Boaz works so hard to really make the course the best experience of the students. I enjoyed the problem sets because they were basically like fun puzzles, and that worked really well.
Interesting, engaging lectures
The problems were mostly very interesting and good puzzles to think about. The TFs and teaching staff were very accommodating and supportive
The content was very interesting – The definitions covered of PRGs, PRFs, Comp. Security and some of the constructions of CPA–secure schemes were enlightening. I really enjoyed the depth of the material and the homework's – They really worked on our understanding of the critical definitions.
This course had many strengths— the professor, Boaz, is a wonderful instructor and human being and clearly cares about the educational outcomes of his students. His enthusiasm for the topic was one of the greatest strengths of the course. The other students also significantly affected the course— the group this year was great; all the students were engaged in the content.
Interesting content, well taught, good notes provided
Engaging lectures; problem sets really support learning the material
Material is taught at a fast pace, so I found the course a great personal challenge Book was well written, easy to follow material
I really enjoyed the material, and it was presented well. Some of the lecture notes were rather dense, and they were sometimes confusing, but they taught a lot. Alec's section (I had a conflict during Leor's, so I couldn't compare them) did a great job of clarifying material, too.
Great support in terms of conceptual help and homework help.
Lectures were really good, and I enjoyed working on problem sets in Winthrop's library
Really engaging lectures, clear formatting of lectures, great interaction with the class during lectures. Lecture notes were a great resource. Lots of support from course staff.
A very balanced class in terms of difficulty. Boaz is engaging.

Considering only the first half of the course (on campus), how could this course be improved? Please use concrete examples where possible and provide constructive suggestions.

Comments
quizzes were slightly stressful and at times confusing.
My main concerns with the course were the disconnect between the reading and the lecture, since the lecture assumed a good understanding of the reading, but that is a course feature emphasized at the outset, so I can't complain too much.
I wish there are more resources for how to phrase reduction proofs in crypto. While I ended up getting better when I heard about "belly proofs", I struggled in the first couple of weeks.
The lecture notes were insufficient, I needed to read the optional textbooks to really understand the concepts. The course also moves extremely fast, which isn't necessarily bad but makes workload heavy.
The homeworks could be a bit long at times
Having an explicit homework review for common mistakes (perhaps independence, messing up reductions) would have been helpful in the beginning of the course. Though during remote learning I was able to review homework comments more thoroughly, having a dedicated review (like Alec's one about joint independence at the end) would have been more helpful to me than sections I couldn't attend.
I wish that office hours were held at more accessible locations. The undergraduate math lounge is not a good place to have office hours given the lack of outlets and smaller space; I often had to ask people to leave to be able to sit for the office hours. Similarly the river house dining halls were inconvenient for students who didn't live in the river. Yard during the day would be more convenient.
Hopefully the lecture notes will be even better than they were this year
There was a good deal of disconnect between the lectures and the book. It would have been nice to feel that all the material in lecture was either in the book or cited somewhere else, and conversely, that we covered most of the important material in the book (at least in terms of what was on problem sets, etc.).
It was already very good. I do not have suggestions on how to improve.
Sometimes there are errors in the textbook that make it harder to parse.
The course could have used some extra polish – we were occasionally assigned problems that no one from the teaching staff knew if they were solvable or not, and typos (critical, "main point"–shifting typos) in the problem sets were not uncommon. That said, the teaching staff was always very generous with bonus points and support for anything that came up
I am happy with the way it is, but it is quite fast paced. Therefore, people without adequate mathematical training or a strong TCS background may find it hard to follow. It’s worth it in the end, but it may make sense to spend some more time really drilling home the basic definitions.
The textbook could be improved; it's clearly a work in progress and the typos sometimes made statements and theorems difficult to parse.
Having us read notes in advance and then cover the same material in lecture didn't seem efficient
I wish we had an intermediate step between learning the course material and doing the pset questions. I often feel like the pset is a big jump, so something in the middle to ease me in would have been appreciated.
The first few three or so problem sets were really quite difficult in a much less fun way than the remaining problem sets. This may have been intentional to try to weed people out, but I much preferred the problem sets after those first three, and I don't feel I learned less. I suppose it's possible that I just adjusted to the style of thinking in the course and that's why it became easier, in which case there's no need for a change. Also, the lecture notes could be made slightly more clear in some parts. The amount of material covered per lecture is good/reasonable, but sometimes I felt there were some important concepts that required a logical leap for me to make to understand the key point of the concepts, and not just in a "it's good to be thinking hard about the material" way.
Having organized powerpoints were better than the whiteboard lectures in terms of helping me understand the material as the whiteboard lectures tended to have either missed details or confusing notation.
The course was challenging but I think that's kind of the point.
The lecture notes were sometimes confusing, but the fact that they existed at all was a huge plus so this isn't a major issue.

Overall, there was instructional continuity between the first and second half of the semester.

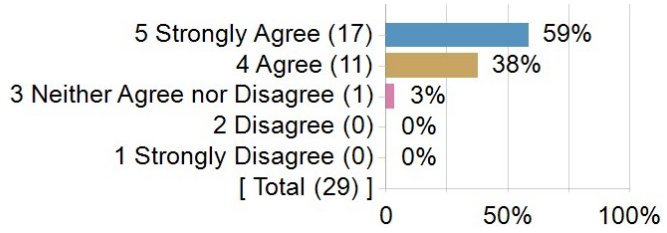
Overall, there was instructional continuity between the first and second half of the semester.



Options	Score	Count	Percentage
Strongly Agree	5	18	64%
Agree	4	10	36%
Neither Agree nor Disagree	3	0	0%
Disagree	2	0	0%
Strongly Disagree	1	0	0%
Statistics			**Value**
Response Ratio			78%
Mean			4.64
Median			5.00
Standard Deviation			0.49

Although the second half of the course was delivered in an unanticipated format, I was able to meet key learning goals for this course.

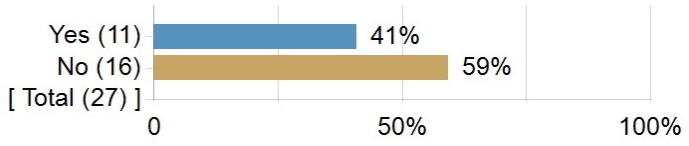
Although the second half of the course was delivered in an unanticipated format, I was able to meet key learning goals for this course.



Options	Score	Count	Percentage
Strongly Agree	5	17	59%
Agree	4	11	38%
Neither Agree nor Disagree	3	1	3%
Disagree	2	0	0%
Strongly Disagree	1	0	0%
Statistics			**Value**
Response Ratio			81%
Mean			4.55
Median			5.00
Standard Deviation			0.57

Were there any particularly creative solutions that the faculty or teaching staff used to facilitate remote learning?

Were there any particularly creative solutions that the faculty or teaching staff used to facilitate remote learning?



Options	Count	Percentage
Yes	11	41%
No	16	59%

If so, please describe.

Comments
using the chat feature extensively to ask/answer questions among students and the teaching staff during lecture
glad that office hours notes were published!
We used Edstem extensively, and it was great.
Boaz and the course staff were incredibly dedicated and effective instructors in remote learning. This was certainly helped by using ipads. Having Boaz's lecture presentation notes before lecture allowed me to "look back" to previous frames like one would on a larger whiteboard, and this was very helpful. Recording all office hours and sections was also incredibly helpful considering everyone's new schedules.
I really appreciated how TFs recorded office hours and sections and shared scribes. I feel like the course was actually more accessible after it went online.
Boaz made very effective use of Zoom features to make online classes still feel interactive and engaging!
We had access to the recordings to lectures and office hours, which was very helpful.
Everything was recorded which was extremely helpful.
Recorded office hours!
GoodNotes works really well, and recording the lectures via Zoom was very nice! The chat also was great, because it kept a transcript of all questions asked.
The course was executed well online – I just can't think of anything particularly notable.
The lecture format (writing notes over prepared slides on a tablet) was really good and allowed for real board work type stuff. Lectures remained interactive using Zoom chat which was great.

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	1
Undergraduate General Education Requirement	0
Expository Writing Requirement	0
Foreign Language Requirement	0
Pre-Med Requirement	1
Divisional Distribution Requirement	0
Quantitative Reasoning with Data Requirement	0

Transition to remote instruction

In this course, what aspects of remote learning worked well?

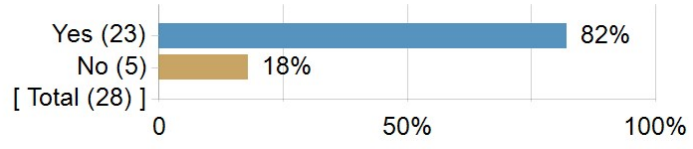
Comments
The fact that the material is entirely theoretical and the class is in a lecture format allowed the class to maintain its academic quality even after transitioning to remote learning
reviewing past concepts
The lectures were mostly the same since Boaz was able to use an iPad, so that was perfect in that sense.
Everything
Lectures were generally smooth.
Lectures worked well over Zoom (at least comparatively). They were clear, and having notes prepared for students before class was incredibly helpful so we could "look back" at previous frames like we would be able to with a real whiteboard. We had few technical difficulties due to Boaz handling Zoom with ipad very well.
Ipad for remote lecture.
Recorded section + office hours. I really appreciated going to digital section too.
Lectures and office hours both translated quite straightforwardly into the remote setting.
All things worked well.
Very flexible OH times, lecture/OH recordings.
Thanks for recording everything.
Lectures went fairly well, although slides sometimes made it harder to follow as the material is presented more quickly, even with live annotations
Lectures worked pretty well, and the problem sets continued as usual.
GoodNotes, Prof. Barak’s enthusiasm, Lecture Recordings.
The zoom lectures were lively and zoom chat allowed for Boaz to more effectively answer questions in real–time.
Professors and teaching staff made themselves available to help
Didn't feel like that much changed.
I think it was all pretty good.
There was no real changes in the course, so I had no difficulty adjusting.
Lectures.
Lecture style format translated smoothly to Zoom.

In this course, what aspects of remote learning didn't work well?

Comments
Working with other students on problem sets became much harder because of remote learning.
hard to collaborate
I definitely think that the loss of peer–to–peer interaction in class (at least most of it) was detrimental, since that was probably the most important part of my learning in the first half of the semester. I also think it was harder to work with peers outside of class, but I think that is a common thread for most students.
I'm satisfied. No issue.
Office hours becomes less casual and so serendipitous conversation is more difficult.
It was hard to collaborate with others in this course, but this issue is not specific to this course.
Glitches in lecture.
N/A
I do not think there was anything that did not work well.
No comments.
It carried over pretty well
The board isn't as big, so we can't look at multiple definitions at the same time. Board space was compromised, but I really don't think that's anybody's fault.
It was harder to complete problem sets remotely without my friends in the course physically present; without the serendipity that comes with a shared physical space we were less inclined to collaborate on problem sets.
Classroom atmosphere suffered, no "talking to your table–mates"
It was harder to focus in lecture, which is understandable and probably universal to some extent
Technological issues with zoom.
It was hard to collaborate with fellow students.
Collaboration died

I was able to participate fully in the course during remote learning.

I was able to participate fully in the course during remote learning.



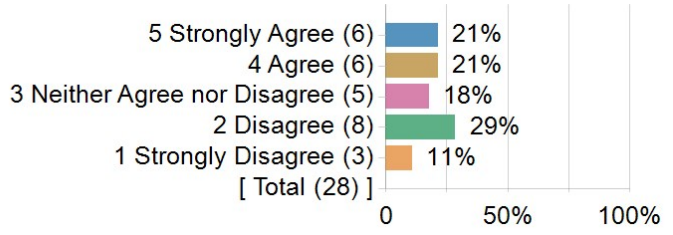
Options	Count	Percentage
Yes	23	82%
No	5	18%

Please Explain:

Comments
I was able to maintain the same level of engagement, attending lectures and asking the TFs questions about homework problems.
(This is my fault), with the lectures recorded, I decided to watch them later, but ended up not doing so...
The inability to work with others, for the most part, is what made this course most challenging this second half of the semester, since it was such an important part of my learning.
Generally my attendance was unaffected but the general stress of times definitely made focusing more difficult.
I had access to a computer and stable internet connection.
Not much changed.
I had access to the recordings of lectures and office hours. This was extremely helpful.
I couldn't go to lecture due to time difference.
There were plenty of opportunities for participation in the zoom lectures.
Could not participate in class as fully

I was able to interact and collaborate effectively with my classmates during remote learning.

I was able to interact and collaborate effectively with my classmates during remote learning.

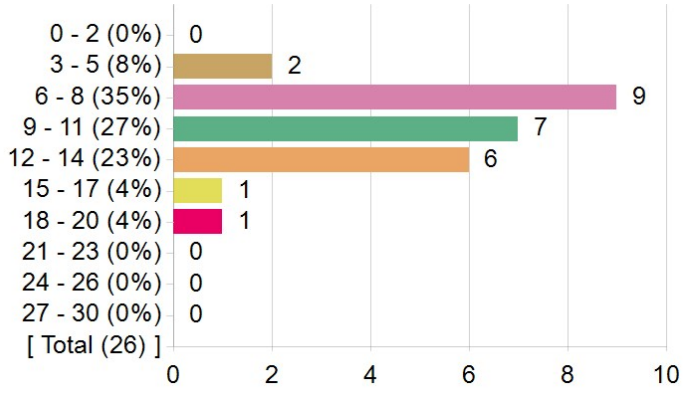


Options	Score	Count	Percentage
Strongly Agree	5	6	21%
Agree	4	6	21%
Neither Agree nor Disagree	3	5	18%
Disagree	2	8	29%
Strongly Disagree	1	3	11%
Statistics			**Value**
Response Count			28
Mean			3.14
Median			3.00
Standard Deviation			1.35

How many hours per week did you spend on this course during the second part of the semester (during the Harvard Closure)? Enter a whole number between 0 and 168.

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

How many hours per week did you spend on this course during the second part of the semester (during the Harvard Closure)? Enter a whole number between 0 and 168.



Statistics	Value
Response Count	26
Response Ratio	72%
Mean	9.85
Median	9.00
Mode	8
Standard Deviation	3.51

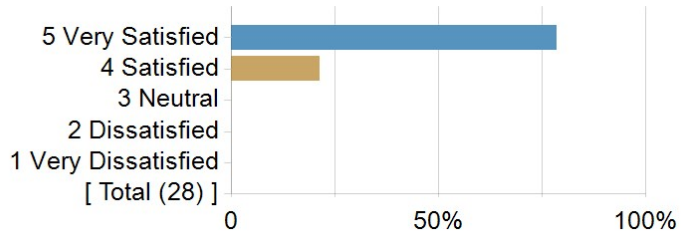
What did you have to do differently as a learner to adapt to remote instruction?

Comments
a lot more self–studying for problem sets.
I had to be more vigilant about actually making sure to attend class, and pay full attention during class. I also had to be more on top of doing homework, since it was much harder to work with my peers.
Ensure no distractions when viewing lectures.
I needed to work through concepts much more individually than before, because asking friends for help understanding material —– whether in class or not —– became much harder. Though lectures were done well, it was much easier to get lost, disengage, and decide to watch the recording instead. Watching recorded lectures helped me a lot, though of course it took more time.
The transition to the remote study was smooth. I was fine with that.
I had to interact with my pset partners virtually and therefore did more work on my own.
Not much changed, other than identifying which of the material was important to do at each moment
Keep myself motivated, set up a desk at home similar to the one I had in lab, try to be productive in a very closed, isolated and stale environment – But, it became better and easier with time.
I had to be proactive in reaching out to friends to collaborate with; I also had to set myself more of a schedule for completing my coursework without the structure provided by an education in a physical space.
Rely more on notes than lecture
Learn how to focus at home by creating a productive work environment
I had to spend more time on problem sets since collaboration was more challenging
N/A
Get used to going to lecture much earlier in the day.

Custom Questions

Your overall satisfaction with the course?

Your overall satisfaction with the course?



Options	Score	Count	Percentage
Very Satisfied	5	22	79%
Satisfied	4	6	21%
Neutral	3	0	0%
Dissatisfied	2	0	0%
Very Dissatisfied	1	0	0%

What would you like to tell future students about this course? (taking into account that their experiences will be different from the special circumstances of Spring 2020)

Comments
cryptography is really cool, and the course definitely teaches you a lot about the mathematics behind the subject!
Really rigorous course that delves into cryptography — definitely pay attention to the key concepts + definitions introduced at the beginning of the semester! problem sets are definitely doable with office hours / collaborating with others
This course is a lot of work, and keeping up with the readings and fast pace is difficult, but the key concepts and methods which you will learn to think about security will be fascinating and useful, no matter the future discipline.
The course is *awesome*. You will learn how to actually do crypto! It is not an easy course. Compared to C121, the reductions are subtler and the pace is faster. However, the efforts you put in will payoff big time.
It's a very fast moving course with challenging homework assignments. Lectures are important, and find a supplementary textbook you like to follow along with.
Interesting material, though stay on top of the lectures as they can move fast. The material from the first 6 or 7 lessons is also used over and over again during the rest of the course. Homeworks can be pretty heavy, be sure to set aside enough time.
Cryptography is a fascinating subject, and this course will both teach you the fundamentals very well (the concepts are reinforced throughout the semester) and expose you to exciting and very modern areas of cryptography. The workload is standard for a comparable math course, but is much more rigorous and time–expecting than CS121. Grading (even before sat/unsat) is very fair. Boaz was very accomodating for his students in the transition to remote learning, and this is only one aspect of how dedicated he is to his students. Don't fall behind on readinds and enjoy this course!
Challenging yet rewarding – Crypto was one of my favorite classes at Harvard. The material is really cool and is accessible even without a crazy strong math background. 121 helps significantly. The one obstacle I encountered was group theory, which took a week to get used to but was OK thereafter.
I loved this course, it was definitely one of my favorite classes at Harvard and would so strongly recommend it to anyone interested in theoretical CS. I would strongly encourage anyone who enjoyed CS 121 and is excited about dedicating around at least 10+ hours per week to learning cryptography to take the course. During the first two weeks of the course, I found myself intimidated by the steep learning curve to crypto and was a bit nervous because I don't have a strong math background, but found that 121/124 was sufficient with a bit of extra review. Boaz is fantastic and his enthusiasm for this subject makes every lecture enjoyable.
Take it!!! Even if you think you’re not “math–y” enough to be a cryptographer!
One of my favorite courses at Harvard! Boaz's enthusiasm for the subject really shone through in each lecture, and I feel like I've learned enough about cryptography to read and comprehend (some) current research in the field. Be warned: the difficulty of the readings picks up quite a bit in the latter half of the course (not that they're particularly easy to begin with). Be sure to give yourself plenty of time to study them, possibly consulting the other sources that Boaz posts on the website.
This is a fabulous course. Keep in mind that it is almost entirely focused on theoretical cryptography —– classes like CS 263 complement this by focusing much more on security in practice. It is a math class, sort of like a more sophisticated version of a class like CS 121. Boaz is extremely kind and accessible. Fully understanding concepts and proofs will often require either talking to him/TFs outside of class or doing extra reading in the books. Some homework problems were also rather tricky, but there was plenty of support. I loved this class.
This course is very good.
The course was rough at first, but there was a lot to learn. I think it took me 3–4 psets to get used to the proof style and just the basic general concepts of cryptography. The virtual version of the course was great as well, and the teaching team was very understanding and supportive given the unprecedented circumstances.
If you're interested in cryptography, this course is incredible. It gives great coverage of the important topics in cryptography, and I am walking away with both an understanding of not only the mathematics behind cryptography, but also it's spirit (ie common themes and a higher level understanding of the subject). While the class is a good amount of work, this is the good type of work where it leads to really in–depth learning. Also, the class has all the hallmarks of an excellent Boaz class (bonus points on the HW that reduce stress about grades while also challenging you to think about hard problems, a knowledgable and flexible instructor, and emphasis on learning and the beauty of theory). I strongly recommend taking this course if you have an interest in cryptography and/or have an interest in math.
Cryptography is really cool and fun! It will definitely help to have the mindset that you should make this class one of your priorities, as the psets can take awhile and it also takes a good amount of time to do the readings thoroughly. If you enjoy the content of 121 and are willing to put a fair amount of time then it's a good class to take.
Overall a great course if you like to solve puzzles! Sure, the course could be more polished in some areas (we were regularly assigned problems with major typos/the teaching staff did not know the answer to the problems), but the major themes of using math to formalize different notions of security is great!
Have some grounding in basic discrete probability, and reductions/combinatorics at the level of CS–121. Given the fast pace, it is

Comments
unlikely that you will develop the familiarity to parse terse but subtle and meaningful definitions and write clear proofs if your mathematical grounding in logic/probability/reductions is shaky.
I could not recommend this course more highly. I found it to be pretty difficult, and the content is most likely going to be completely useless in your day–to–day life unless you become a cryptographer, but it's so interesting and beautiful, and Boaz is such a wonderful teacher that you'll find yourself looking forward to going to lecture (if in–person lectures are a thing again) each week.
Covers interesting material, introduces you to effective ways of thinking
It’s hard (especially if you don’t have a super strong math/theory background) but definitely doable! There are lots of opportunities for extra credit and the course staff cares a ton about helping you learn. If you interested in security, this is a great class to take in combination with 263
If you're willing to put your head down and grind away, you'll gain a lot from this class. Material is fascinating and challenging.
I really enjoyed this course. It is definitely challenging, but you will learn a lot, and the course staff is very supportive.
Very fun course but quite difficult if you don't have experience with probability.
Great class. Quite technical and mathematical but Boaz loves teaching and that makes this class fun to take! Make sure to understand the concepts in depth over just getting the problem sets done because the class definitely moves at a fast pace and builds up fundamentals needed throughout the course.
This course is really challenging but also really rewarding – Boaz delivers on his promise to give an intensive and complete intro to crypto. there was no difference between 127 and 227 this year other than 227 had to do a final project and some lecture notes. Strongly recommend for anyone trying to get into theoretical cs
Boaz isn't kidding when he says this is a "fast–paced introduction" —– the course starts at pretty much the beginning of crypto and gets pretty far. It is a really well designed course overall and has great lecture notes (even if they are buggy) to rely on. The course staff is super supportive. It's easy to get lost but they help you get back on track. Would highly recommend this course, it's both theory–intensive and applicable.
This class takes a decent amount of time for the readings and psets, and can be technical at times. However, I ultimately felt that the difficulty was quite balanced.

Any suggestions for improving this course in the future?

Comments
a lot of reading —- may be nice to do something more interactive than a reading quiz
If at all possible, it would be great to have a course (perhaps separate from this one) which covers similar topics (maybe just the core of public and private key crypto) at a slower, more manageable pace. I understand that the course is designed specifically to be an advanced intro, but I often found myself falling behind and such a slower course would be great.
I personally would have liked to spend more time on constructions, but there was really no time to do so.
The pre–lecture quizzes were very helpful for my learning. I think it would have helped to discuss the quizzes very quickly at the start of lecture to emphasize what you wanted us to get from the reading.
More lecture notes.
I didn't realize how helpful it was for office hour notes to be published until the course went online. Perhaps a more organized and accessible way of giving hints or receiving problem set help would be great. Some weeks I felt super anxious about the assignments and found myself prioritizing my life and schedule around making it to in–person office hours. This shouldn't have to happen / office hours shouldn't have to be attended physically in–person to receive help.
It would be nice if the lecture notes were edited and streamlined.
I do not have suggestions. The course is already very good.
Sometimes it is hard to jump between texts (for example when moving to Boneh–Shoup for AKE) because the notation is different and the paradigm is a bit different. I understand that this is a graduate course, so students are able to do that, but I think it would make the course even better if all the course material was incorporated into Boaz's textbook.
I think that slowing down a little bit at the very beginning could be helpful. There was still a lot of room to cover "advanced" topics at the end, so by cutting out a week of that content there could be room to focus on the fundamentals of private–key cryptography, which felt a little rushed (esp. around the PRG, PRF, block cipher, OWF area)
Add more polish to the course – in particular, be more careful about the problems that are posted each week, whether there are major typos in them, etc.
Just maybe slightly slower in the first week?
Update the textbook and possibly hold more office hours.
Lighter required reading, more targeted recommended reading
I mentioned this earlier, and it's not a big deal, but the first few three or so problem sets were really quite difficult in a much less fun way than the remaining problem sets. This may have been intentional to try to weed people out, but I much preferred the problem sets after those first three, and I don't feel I learned less. I suppose it's possible that I just adjusted to the style of thinking in the course and that's why it became easier, in which case there's no need for a change. Also, the lecture notes could be made slightly more clear in some parts. The amount of material covered per lecture is good/reasonable, but sometimes I felt there were some important concepts that required a logical leap for me to make to understand the key point of the concepts, and not just in a "it's good to be thinking hard about the material" way.
N/A
Some of the review sessions you gave at the end (I'm imagining your diagram of the "globe" of crypto) were great and I think could provide a useful roadmap if you referred to them throughout the course. One topic I remained confused on was the actual instantiation of some cryptographic objects. For example, modes of operation for block ciphers was always a bit confusing for some reason. Another example is hash functions, like why is SHA 256 believed to be secure?

Any specific feedback for either the lecturer or the teaching fellows?

Comments
I really really appreciate the teaching staff being so understanding in the second half of the course!
I really appreciate the work they did to adapt to the online format and their flexibility, especially in the initial transition phase. It made everything much more manageable.
Alec is incredibly patient and explains things well in his office hours and sections (which I watched virtually — really, Nari deserves a shoutout here too for asking great questions). All the TFs made themselves very accessible during the transition to remote learning, which I really appreciate. Boaz is a great lecturer, though it took some time to get used to his style. The lectures were ambitious in their scope, but I would always leave with enough new understanding to go back to the reading with more confidence. I also appreciate that Boaz encouraged discussions about concepts during class.
No. Thank you very much <3
To Boaz: I really appreciated how accommodating you were throughout the course, especially during our transition home / online. Your commitment to giving the highest quality lectures you could while online was also much appreciated. To Kai: You are one of the best CS TFs I've ever had; thank you for being so kind and always making me feel so excited to learn crypto!
The lectures were somewhat hard to follow. Maybe make them less dense and only serve to reinforce the text.
Thanks so much for all your work in making this an enjoyable class in light of the circumstances.
The lecturer and TFs are very good. They helped me a lot with this course.
Boaz, I really appreciate your work on this course. You did an excellent job handling all of the COVID uncertainty; you added flexibility for students who needed it while also maintaining a rigorous course that delivered material well. Thanks for being such an awesome instructor and human being! Alec, I really appreciate your hard work in this course. Thanks for recording your OH, being so available, and doing a really rigorous job of answering Ed questions. Leor and Kai, I interacted with y'all less, but thanks for helping make the course solid even given the circumstances.
They did a great job in the strange circumstances, and they were very helpful and accommodating!
Thank you for all the help, everybody! Every single feedback and/or clarification was super helpful!
You guys did a really great job adjusting to the online format. I ran into some difficulties this semester and you were proactive and made sure that I stayed on track while being nothing but accommodating.
Overall good
The office hours were helpful (but not in a "too much help" way), and sections helped to clarify material from lecture. I definitely appreciated both of them. I also appreciated the increased flexibility in the second half, both because sometimes things were harder, and because it was more challenging to collaborate with other students and bounce ideas off of people to solve problems, making the problem set completion process more time–consuming, at least for me.
N/A, Boaz, Alec, Leor, and Kai were great.

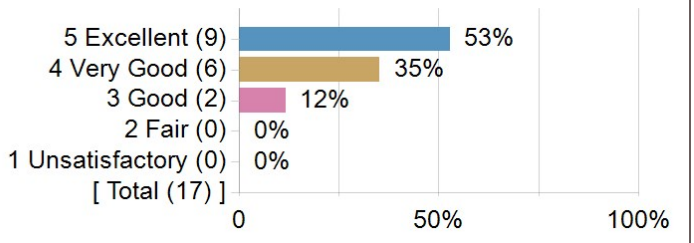
The Embedded EthiCS module aimed to introduce ethical content that is closely tied to the course and to help you reason about ethical concerns in CS. What feature of the module was most successful in this? What suggestions do you have for how best to integrate ethics content into CS courses?

Comments
I think cryptography especially concerns a lot of ethical content, and the embedded ethics module for this course was both interesting and informative. I liked the small group discussions and the enthusiastic presentation of the material!
I thought being able to break off into groups to discuss in the Zoom setting was an excellent way to engage with the material, especially given the difficult and unengaging nature of online learning.
I enjoyed our discussion!
The assigned reading was very good.
This embedded EthiCS module was the best one I have participated in so far (three other modules in my other cs classes). I think this was largely due to the interest of students in the class in the material and that we had involved group discussions. That this was a more rigorous CS class helped as well, as the philosophical argumentation needed to make Embedded EthiCS deal with rigorous ethics was easy for students to get on board with or challenge productively. This embedded ethics module was also especially relevant to our lives, which helped students engage and bring their own beliefs into the discussion. Again, this module was fantastic (even when held over zoom!).
This was a really good EthiCS module. More like this one.
The lecturer did a great job! Maybe she would have given a more organized lecture if she was given more context on exactly what we did and did not cover in the course, as it seemed she wasn't aware.
Idk
I think all features of that worked well. I think ethics content would be helpful for many courses.
I really liked the reading for the lecture. While I didn't agree with everything the article said, it led to some important questions. I think two things made this ethics module effective. First, it was tied in with the material (ie having studied fully homomorphic encryption and other topics allowed you to have a more in–depth discussion than if you hadn't studied it, so it felt like the ethics was really about cryptography). Second, the connection to ethics was authentic and not contrived. These are important questions to ask about cryptography, and discussing them is useful. For example, in 124 last year, the ethics lecture used "flow" to analyze an ethics problem, but it felt that the ethics problem was so unrelated to the real world that it had been specifically constructed so that we could use flow (and was not really an important ethical question to discuss). The ethics module in crypto felt the opposite way; extremely important to discuss.
The reading was really interesting and I think the whole document should be required reading, maybe as part of an assignment. Compared to other embedded ethics modules, this one felt particularly relevant because cryptography has a big political and moral dimension to it.
The ethics lecture was a nice diversion, I liked the case studies and thinking about different sides of an issue
I think in general it is helpful to have an ethiCS module, specially in TCS courses, because we math aficionados forget that somewhere down the pipeline our math has real consequences in the “real world”.
Embedded EthiCS was a good addition to the course. I loved hearing from my peers, who were very thoughtful in their contributions to the class.
The discussion was interesting, but seemed more about sharing opinions than actual ethical dialogue. Setting up some framework for ethical questions to begin with may have been helpful.
The best part of the ethics lecture was tying it all into the current state of the world (specifically re: coronavirus); put the ethicality of cryptography in perspective. Honestly, I would have loved having some more articles/references to read up on following the discussion. Would have piqued my interest more.
The Embedded EthiCS module for this course was great. It connected cryptography to current events and to ethics in general, in ways that I don't think I had fully realized. I'm not quite sure what made this Embedded EthiCS module so good, but whatever it was should be imitated for other courses!
The most effective part of the EthiCS module was the focus on specific current issues that really made me think.
I think embedded ethics is really good as it is and I appreciate the commitment to getting feedback and improving.
I think the embedded ethics module was done very well, and chose a relatable topic for discussion. Perhaps the ideas could be spread throughout the course – ethics is critical to crypto and crypto brings up very interesting ethics discussions.

GSAS Module Questions

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

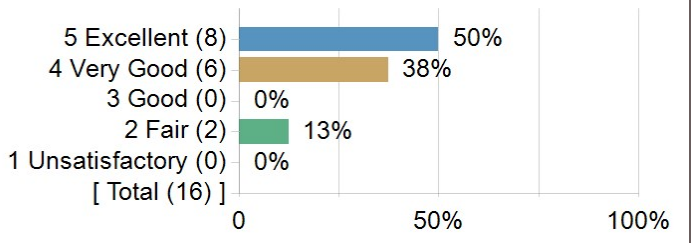
Included discussion or assignments that pointed to a potential dissertation topic, or, in the sciences, a potential research lab



Options	Score	Count	Percentage
Excellent	5	9	53%
Very Good	4	6	35%
Good	3	2	12%
Fair	2	0	0%
Unsatisfactory	1	0	0%
Statistics			**Value**
Response Ratio			47%
Mean			4.41
Median			5.00
Standard Deviation			0.71

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

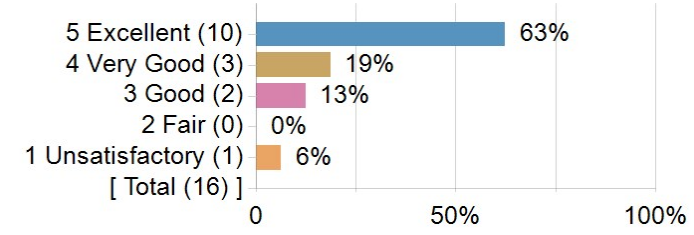
Included assignments that helped to develop necessary research skills for a potential dissertation topic



Options	Score	Count	Percentage
Excellent	5	8	50%
Very Good	4	6	38%
Good	3	0	0%
Fair	2	2	13%
Unsatisfactory	1	0	0%
Statistics			**Value**
Response Ratio			44%
Mean			4.25
Median			4.50
Standard Deviation			1.00

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

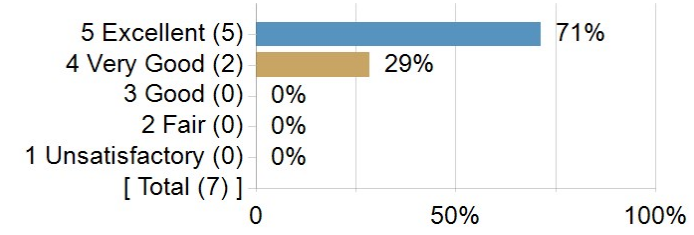
Included assignments that could be developed into professional talks or potential publications



Options	Score	Count	Percentage
Excellent	5	10	63%
Very Good	4	3	19%
Good	3	2	13%
Fair	2	0	0%
Unsatisfactory	1	1	6%
Statistics			**Value**
Response Ratio			44%
Mean			4.31
Median			5.00
Standard Deviation			1.14

Helped directly or indirectly in preparation for generals/qualifying exam

Helped directly or indirectly in preparation for generals/qualifying exam



Options	Score	Count	Percentage
Excellent	5	5	71%
Very Good	4	2	29%
Good	3	0	0%
Fair	2	0	0%
Unsatisfactory	1	0	0%
Statistics			**Value**
Response Ratio			19%
Mean			4.71
Median			5.00
Standard Deviation			0.49

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

Comments
learned a lot about the research field of cryptography!
The Psets, the scribe notes, and the project were very helpful.
Not a GSAS student.
The research project was an obvious example of this, and the lecture notes scribe task was also a good way to explore a topic more completely
I have been thinking about a seed length lower bound for entropy flattening, and in general, the course covered topics very closely related and had proof techniques that seemed related to the ones I am experimenting with.
I felt like this course gave me helpful insight into what cryptography and cryptographic research actually look like