



Summer 2023 Individual Report for MATH P-12170 Cryptography (35527) Stephen McKean

Project Title: **2023 Harvard Summer School Course Evaluations**

Courses Audience: **17**
Responses Received: **15**
Response Ratio: **88%**

Instructors Audience: **17**
Responses Received: **14**
Response Ratio: **82%**

Report Comments

Information about this report:

- Questions are not necessarily in the order asked on the questionnaire
- Instructors of team-taught courses see their individual results only
- Some questions are shown in both data table and graphical chart formats

Questions about 7-week and 3-week course reports can be addressed to:

Karen Flood
Associate Dean for Academic Affairs
evals@summer.harvard.edu

Questions about Pre-College Program course reports can be addressed to:

Jacqueline Newcomb
Director of Pre-College Program
precollegestaff@fas.harvard.edu

Creation Date: **Tuesday, July 18, 2023**

Course Questions

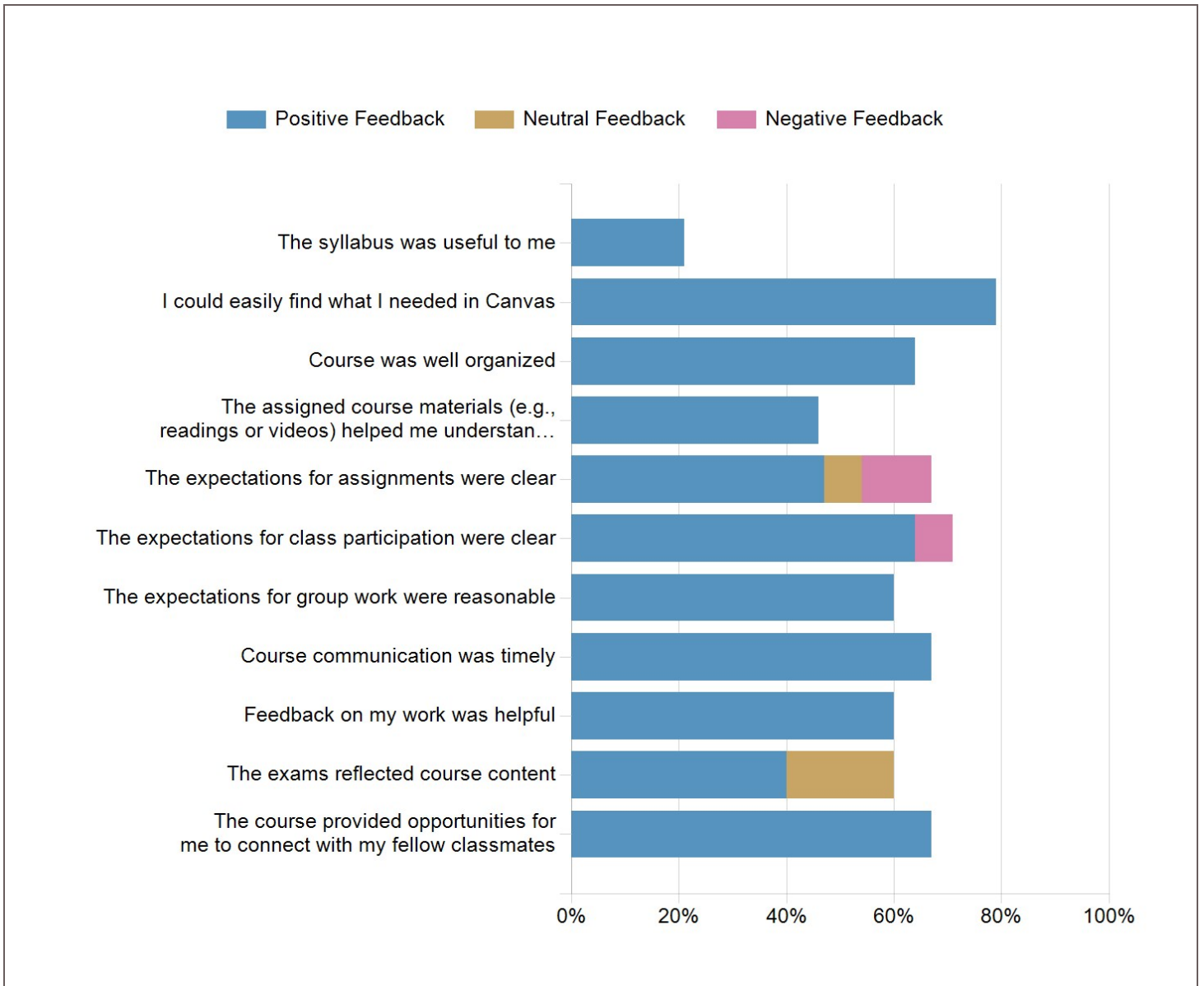
Course Overall

Question	Instructor Average	School (Summer)
	Mean	Mean
How would you rate your overall experience with MATH P-12170 Cryptography (35527)?	4.7	4.7

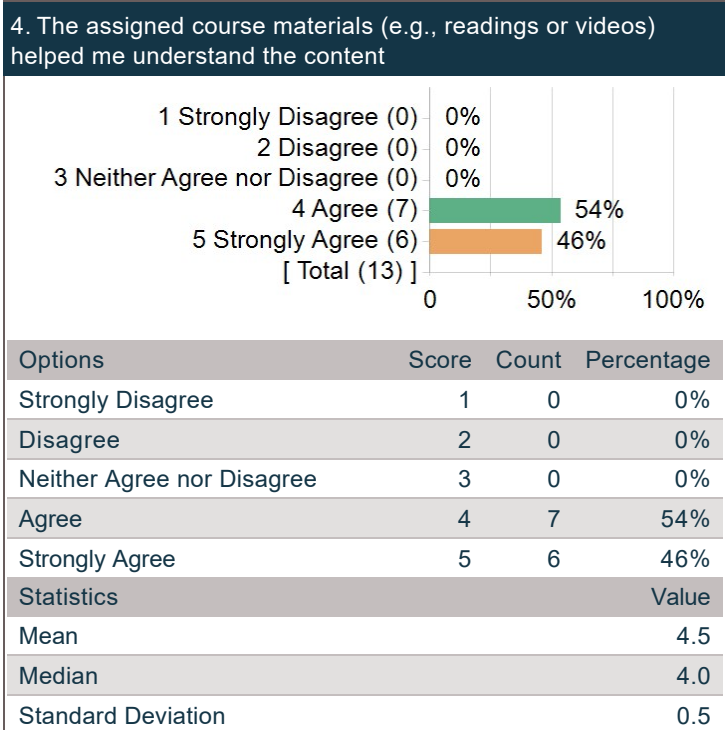
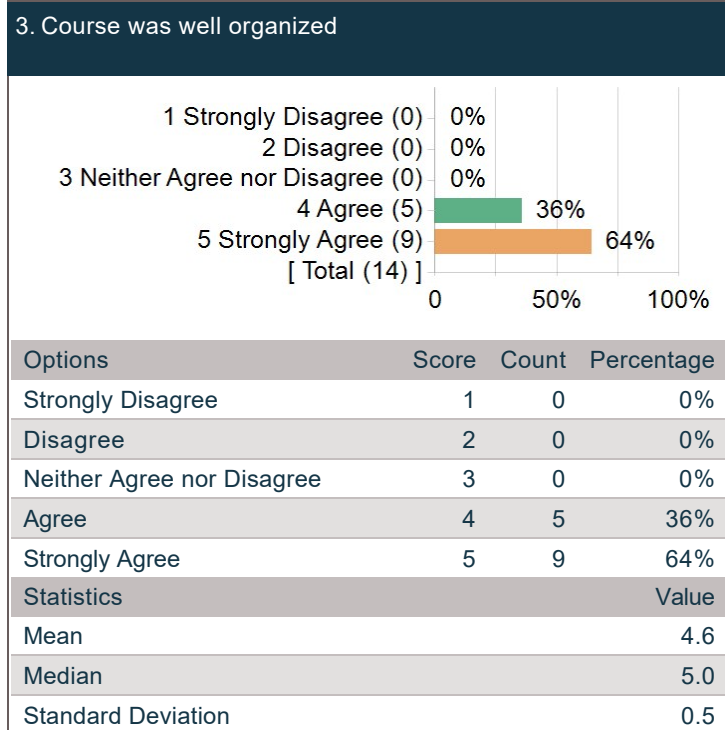
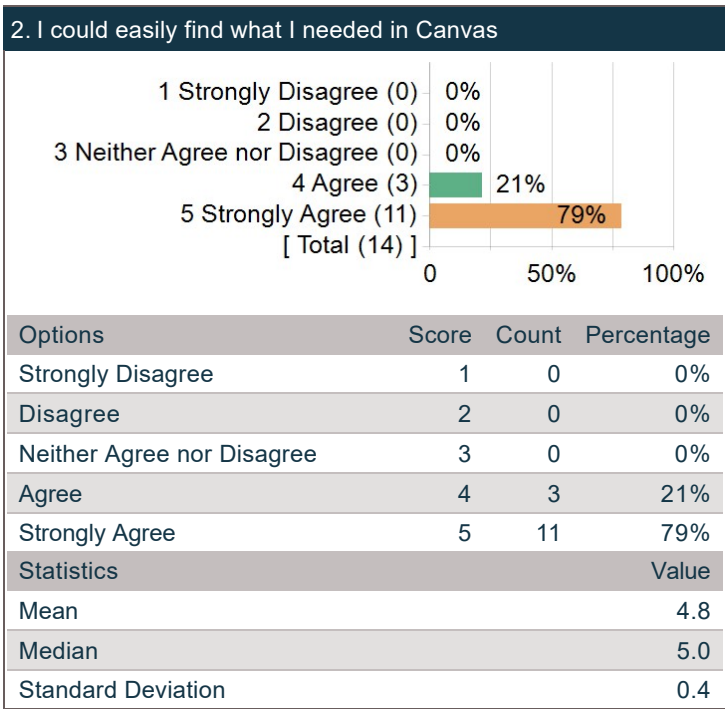
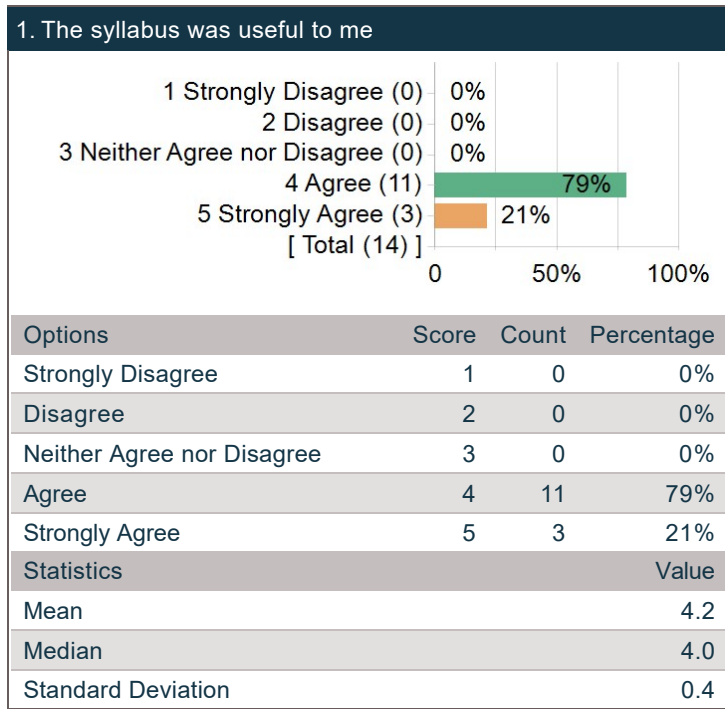
Course Questions - Summary Table

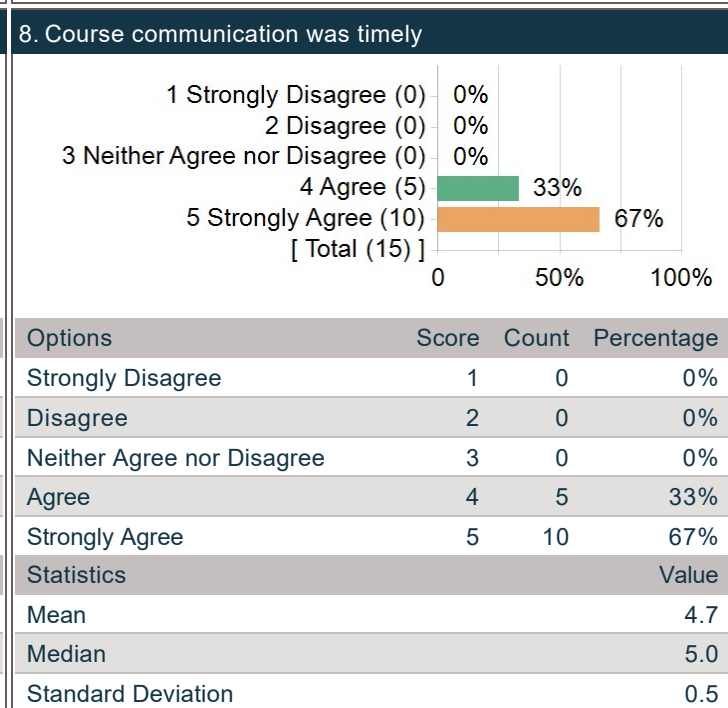
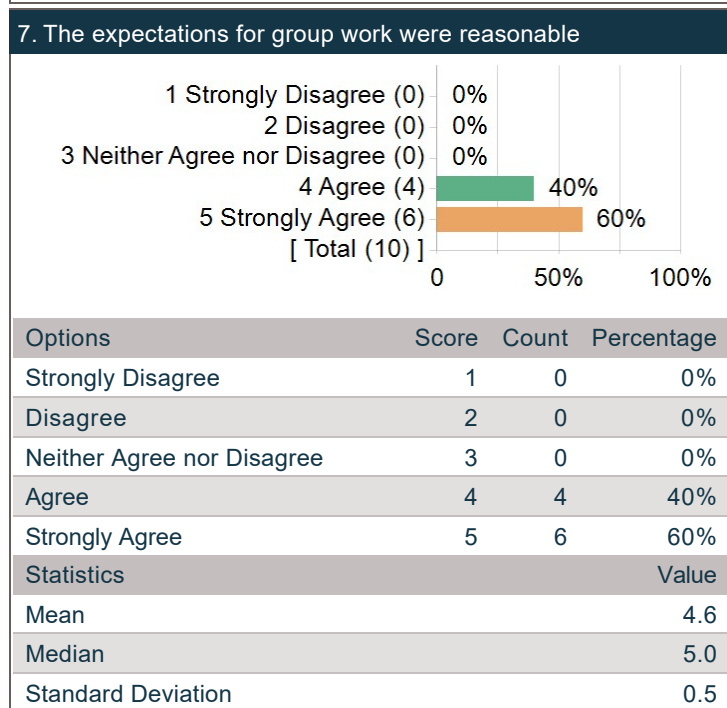
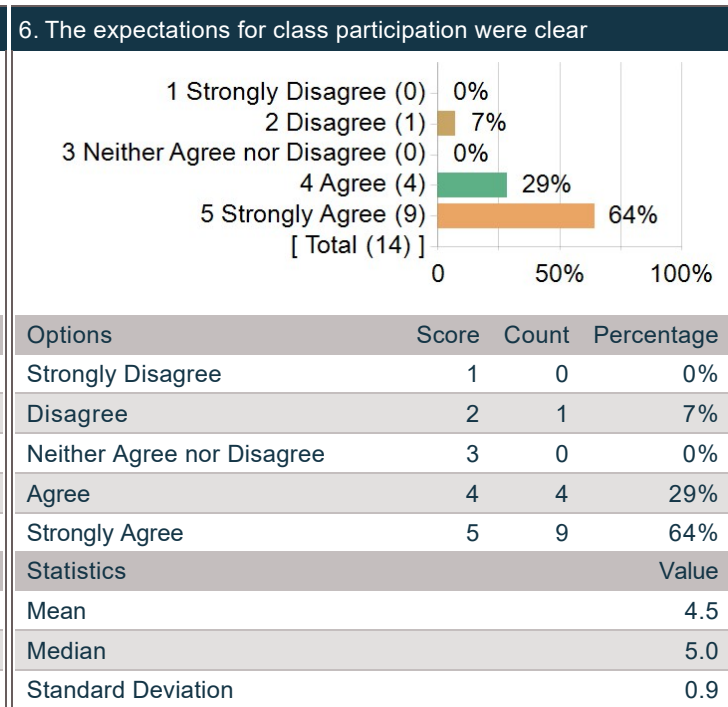
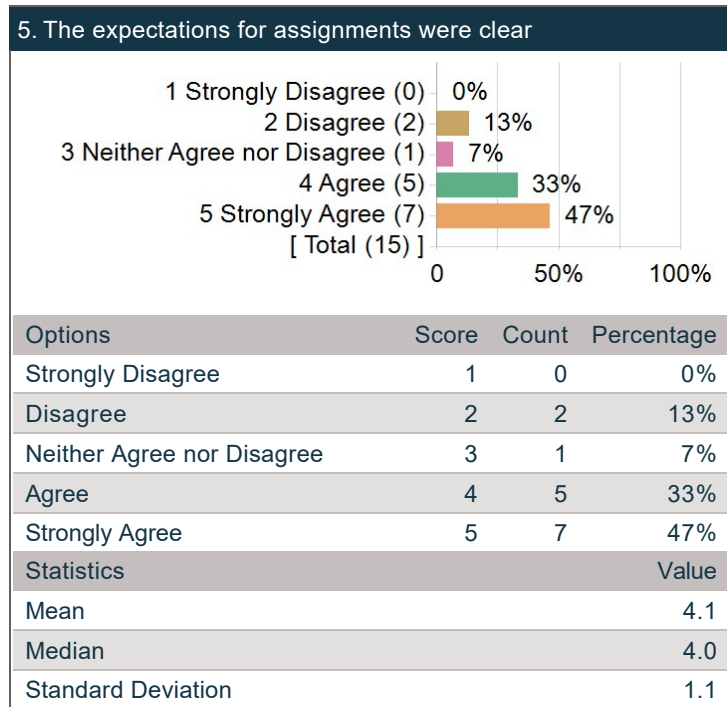
	Count	RespRate%	Agreement	Neutral	Disagreement	Instructor Mean	School Mean
The syllabus was useful to me	14	82%	14	0	0	4.2	4.5
I could easily find what I needed in Canvas	14	82%	14	0	0	4.8	4.6
Course was well organized	14	82%	14	0	0	4.6	4.6
The assigned course materials (e.g., readings or videos) helped me understand the content	13	76%	13	0	0	4.5	4.5
The expectations for assignments were clear	15	88%	12	1	2	4.1	4.5
The expectations for class participation were clear	14	82%	13	0	1	4.5	4.5
The expectations for group work were reasonable	10	59%	10	0	0	4.6	4.6
Course communication was timely	15	88%	15	0	0	4.7	4.6
Feedback on my work was helpful	15	88%	15	0	0	4.6	4.4
The exams reflected course content	5	29%	4	1	0	4.2	4.6
The course provided opportunities for me to connect with my fellow classmates	15	88%	15	0	0	4.7	4.7

Course Questions - Scale Distribution Chart

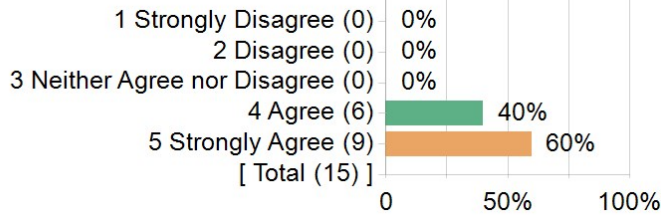


Course Questions - Frequency Charts



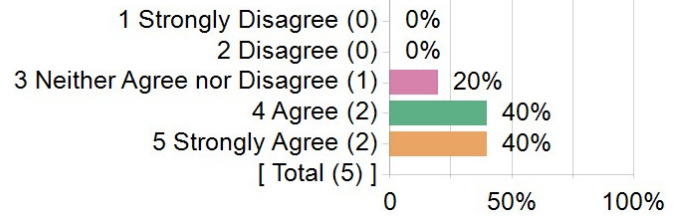


9. Feedback on my work was helpful



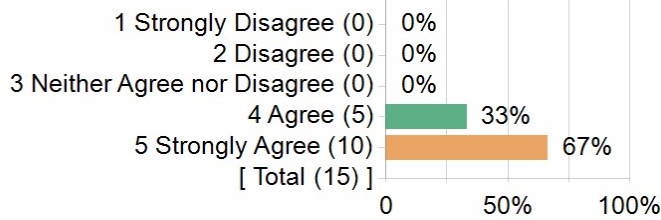
Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Neither Agree nor Disagree	3	0	0%
Agree	4	6	40%
Strongly Agree	5	9	60%
Statistics			Value
Mean			4.6
Median			5.0
Standard Deviation			0.5

10. The exams reflected course content



Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Neither Agree nor Disagree	3	1	20%
Agree	4	2	40%
Strongly Agree	5	2	40%
Statistics			Value
Mean			4.2
Median			4.0
Standard Deviation			0.8

11. The course provided opportunities for me to connect with my fellow classmates



Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Neither Agree nor Disagree	3	0	0%
Agree	4	5	33%
Strongly Agree	5	10	67%
Statistics			Value
Mean			4.7
Median			5.0
Standard Deviation			0.5

Instructor Questions

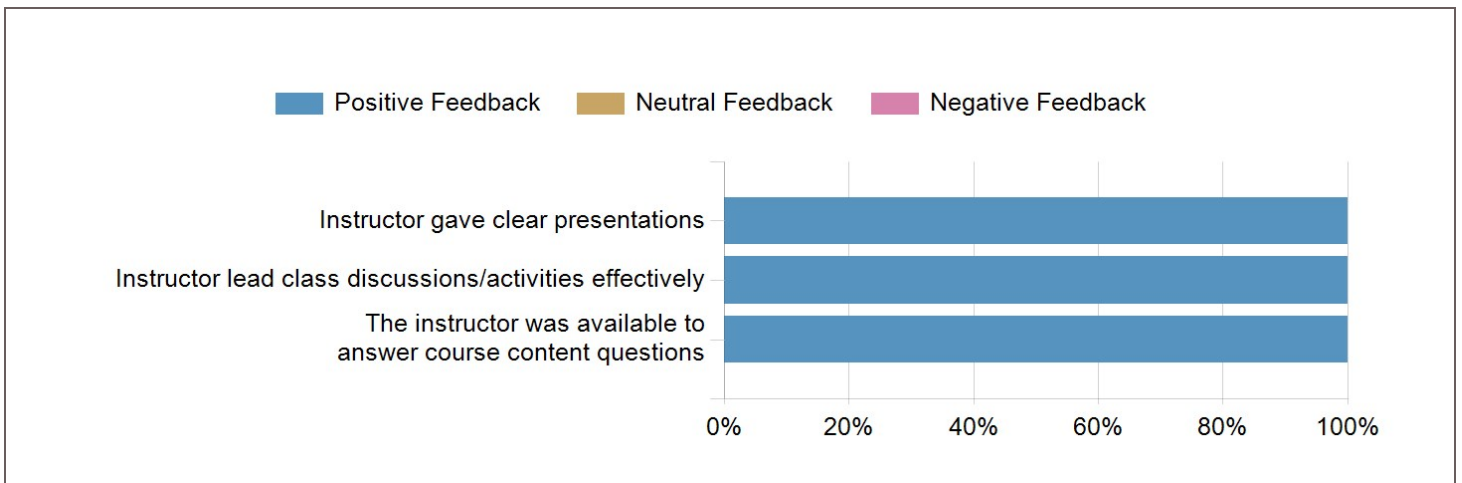
Instructor Overall

Question	Instructor Average	School (Summer)
	Mean	Mean
How would you rate your experience with Stephen McKean?	4.9	4.8

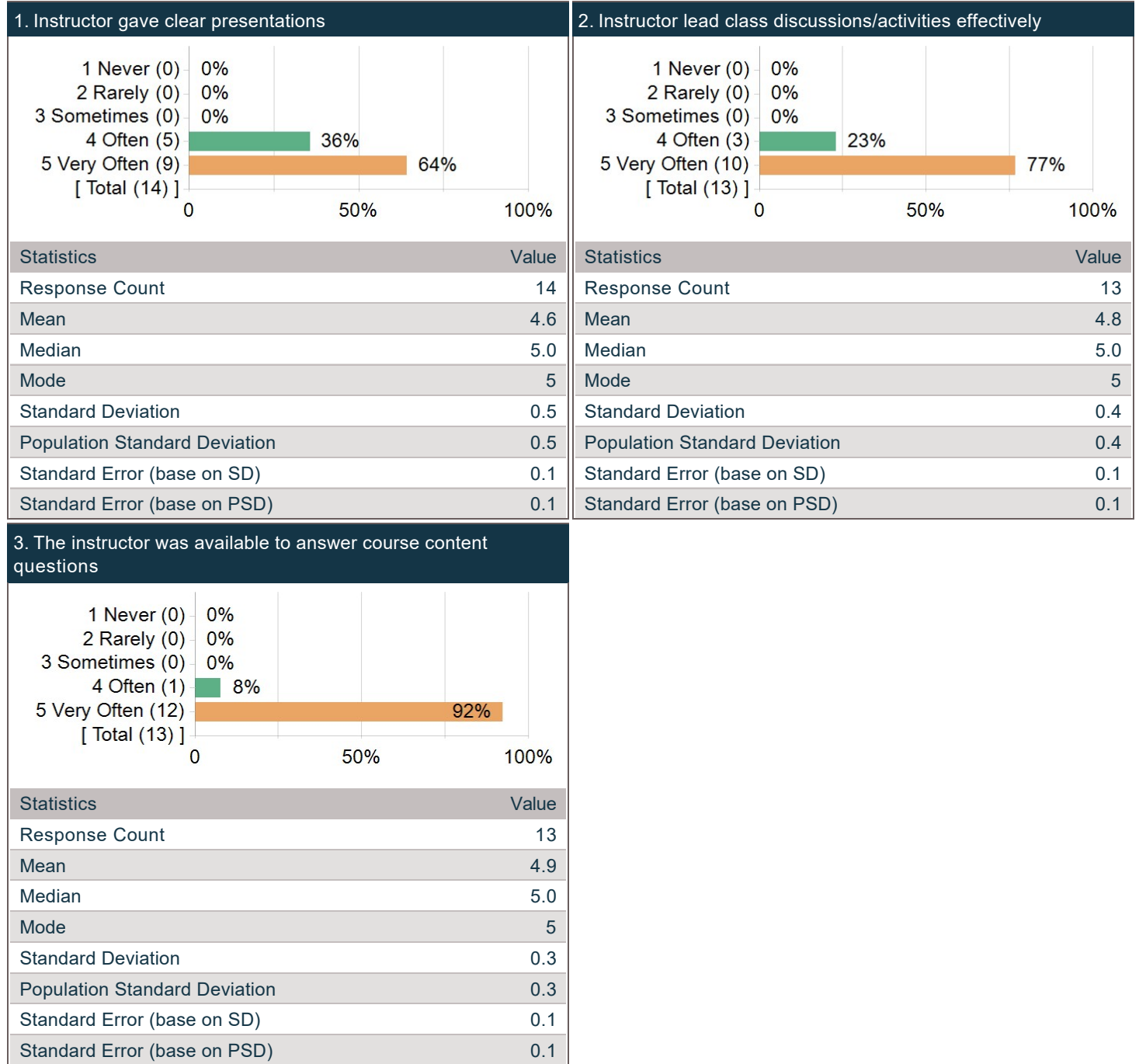
Instructor Questions - Summary Table

	Count	RespRate%	Freq(4,5)	Freq(3)	Freq(1,2)	Instructor Mean	Mean School
Instructor gave clear presentations	14	82%	14	0	0	4.6	4.8
Instructor lead class discussions/activities effectively	13	76%	13	0	0	4.8	4.8
The instructor was available to answer course content questions	13	76%	13	0	0	4.9	4.9

Instructor Questions - Scale Distribution Chart



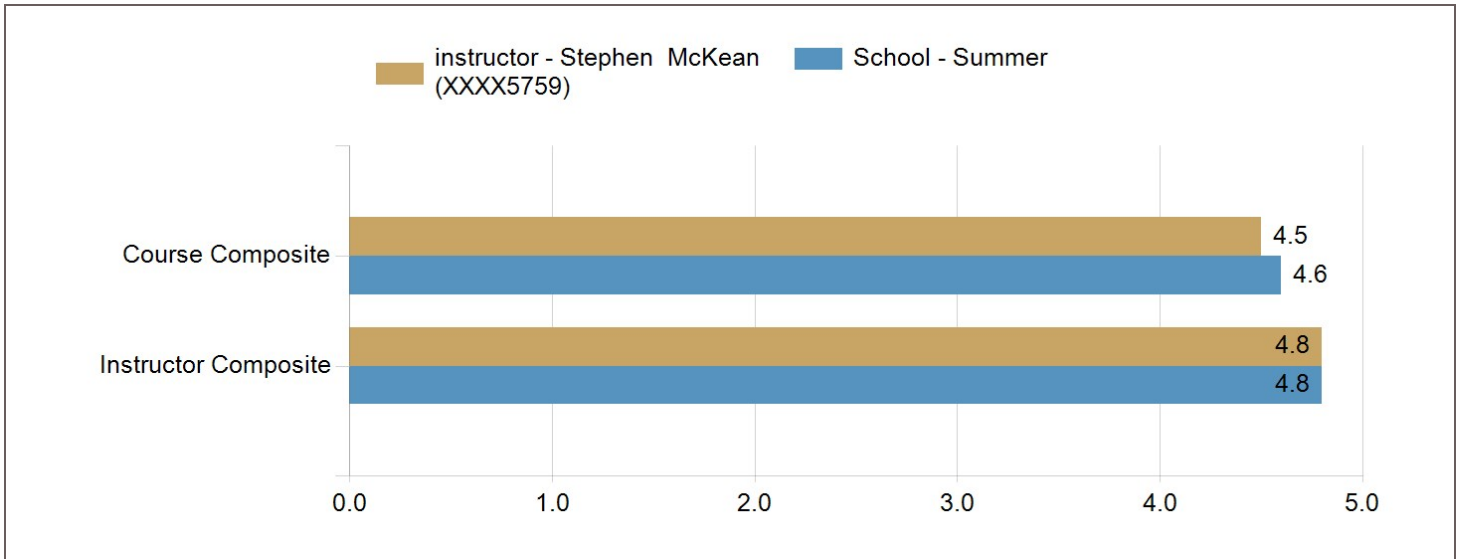
Instructor Questions - Frequency Charts



Instructor Questions - Gap Analysis

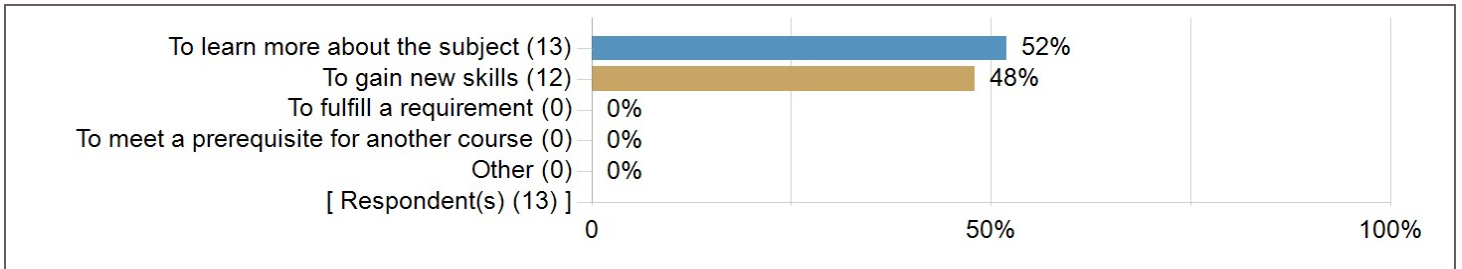
Gap Analysis

The gap analysis is calculated as the difference between the instructor norm and the school norm for both the instructor composite questions and course composite elements.

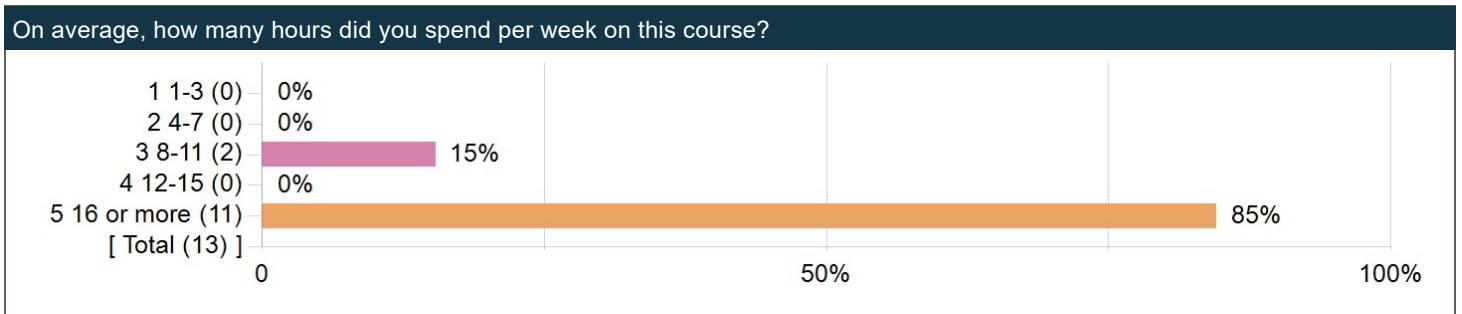


Course Questions

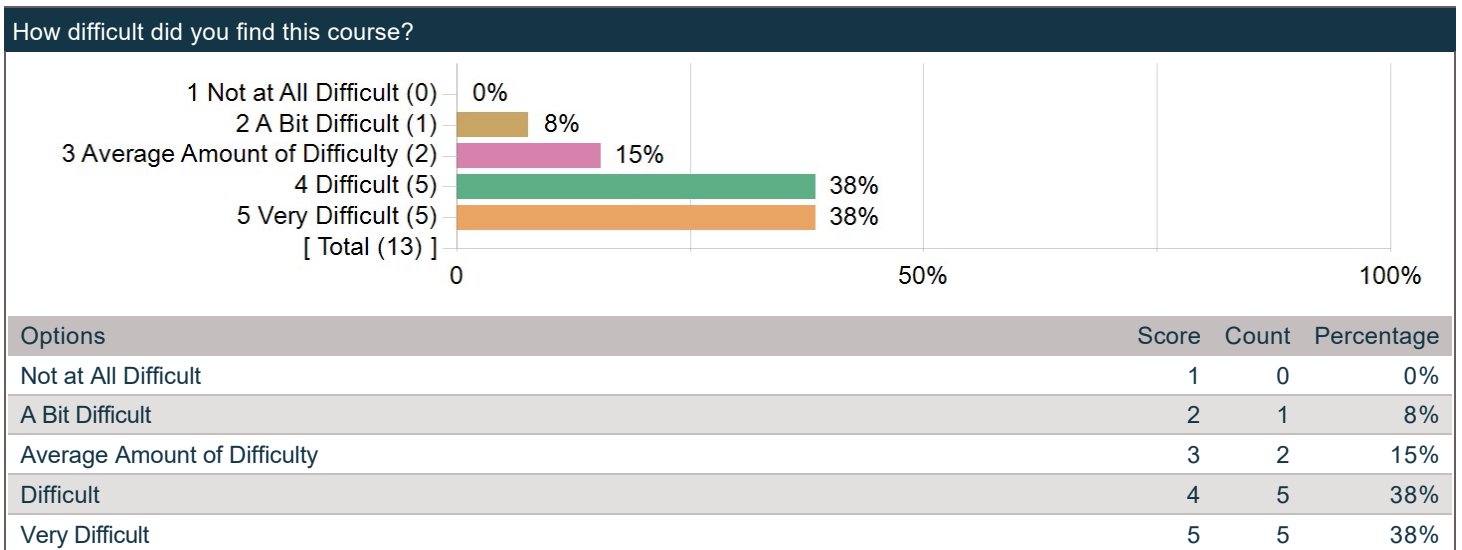
What were your reasons for enrolling in the course?



On average, how many hours did you spend per week on this course?



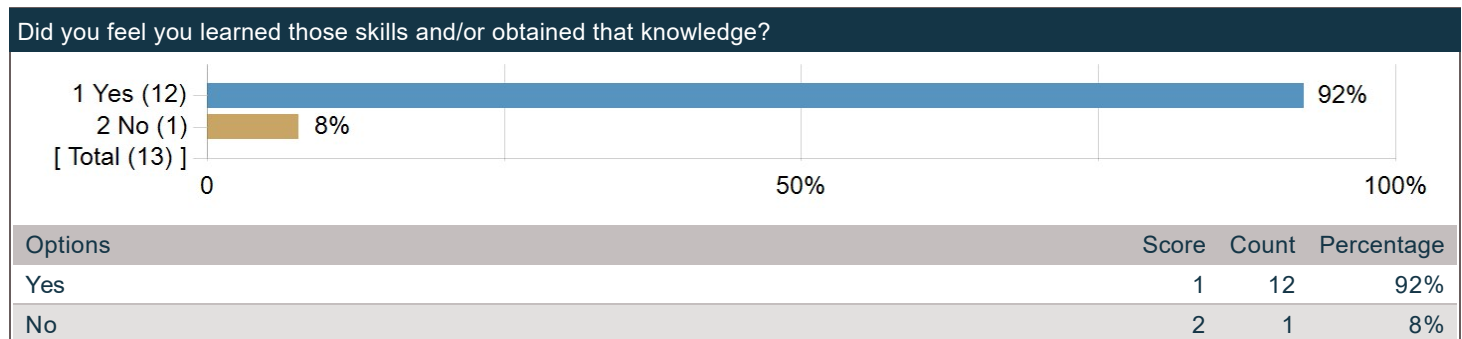
How difficult did you find this course?



What skills/knowledge did you hope you would learn from the course?

Comments
I hoped to improve my coding skills.
<ul style="list-style-type: none"> - encryption and decryption methods - how does math link to cryptography - python coding
Critical thinking, independent thinking skills, problem solving abilities, mathematics beyond the high school curriculum
Problem solving and mathematical thinking
Cybersecurity
math and more cs knowledge
I wanted to learn more about various mathematical topics and hopefully their applications. I also was interested in encryption and decryption methods and how they worked.
<ul style="list-style-type: none"> - improved understanding of more advanced math concepts that I would learn in college - improve my logical and rational thinking when solving math problems
I wanted to learn about the math involved in cryptography, and become acquainted with the subject on a deeper level. I was also excited to see some of the math that I might learn in college, as well as a bit of how a college math class might be structured.
programming and knowledge of whether I should pursue cybersecurity in the future
Expand my knowledge of the subject and to better clarify if it could be an interesting opportunity for my future studies.
I came into it wanting to get a better understanding of modern cryptographic systems. Especially elliptic curves, because that was something I had heard about but never really understood.

Did you feel you learned those skills and/or obtained that knowledge?



Comments about the Course

Which aspects of this course were most helpful for your learning?

Comments
Introductions and applications of abstract algebra and group theory.
The way the material was explained made it easy to grasp and the homework was set up in a way that challenged us just the right amount.
the teaching, the interactive discussions, the fact that the homework assignments challenged me to think beyond the surface level and analyse everything
The homework questions were just difficult enough that they prompted us to think instead of following predetermined solutions in a textbook. It challenged us to utilize what we learned in the classroom to tackle many types of problems and strengthen our understanding of the concepts. I really enjoyed this novel way of learning
The office hours with Stephen were great because he was able to explain anything I was confused about in depth during those office hours.
Independent problem-solving that stimulated my thinking
The groupwork, because it helps to use more than one brain on an assignment in such a course.
Learning about groups, rings, and fields prior to using them in cryptography systems. It really helped make sense of what we were doing with RSA and ElGamal. The addition of lecture notes with the homework proved to be very helpful in reviewing materials and providing tips on coding with Sage/Python.
The interactive parts of the class were the most helpful. Office hours were beneficial as well, and having the ability to work with classmates was absolutely necessary, especially for the first week. I appreciated that we were explicitly given instructions to do so.
The part of the class where we try and tackle problems in the lab and have time to ask the teacher & student assistant questions
I really benefited from going to office hours. I felt like they helped me maintain a balance between struggling independently and receiving support where I absolutely needed it.
The professor was wonderful! I liked the interactive nature of the math course by using cryptography to teach these higher levels of materials.
The lessons have been extremely clear and well organized, sometimes rather tough and challenging, always well explained and interesting. Materials uploaded on Canvas were also extremely precise and helpful.
The lectures and office hours were very helpful. Most of the content was covered during the lectures and then further questions were clarified during office hours. Both Stephen and Jonathan were very helpful and answered all questions. I liked how there was a lot of engagement and interaction throughout the lectures. 3 hours is a long time to just listen to someone speak, so it was great to work through questions on our own/in groups.

Which aspects of the course were least helpful for your learning?

Comments
Towards the end of the course it was getting difficult to come up with new methods of encryption.
–
The first few days were rough because we kind of just had to be immersed into all the math, which was difficult for me to grasp at first. I wished that Stephen would have given us a little reassurance that things will get easier after those first few days just for my own sake.
Office hour times that sometimes conflicted with other events
Although this is a cryptography course, I felt like the brute force homework questions, although fun were not helpful. I really enjoyed learning mathematical processes and group theory and I actually love CS (but when the intention is useful like building a web app to serve a desired functionality). Writing python scripts for brute force is good to SHOW why algorithms are secure, but emphasizing it is not good.
Too much info in one class
Sometimes, we would go on a tangent to the point that what's being discussed is completely unrelated to the material. Although very fun and interesting, I think the learning process would go a lot smoother if it had stayed more focused.
The first few days' homework was rough. I wish we had been told earlier that we didn't need to get every single problem right; everyone was very stressed over not being able to get the substitution ciphers and worried about not passing the class because they hadn't been able to complete the sets. I also think that some light background reading on sets, groups, rings, and fields before starting the class would have been helpful (though not having any was not the least helpful aspect, per se).
Nothing was really unhelpful, but maybe we could've done more class activities like we did on the first day instead of just lecturing theorems, but even those were quite interactive and stephen answered our queries whenever
I can't think of anything (except for substitution ciphers)!
I think there should be more regular breaks or maybe a morning lecture and an afternoon lab (this is just something with precollege administration). Math classes in high school are usually an hour and a half max so after that, I was fading a bit. The breaks were excellent for future awakens and learning though!
Nothing could be defined as not helpful, all elements of the course worked together in an excellent way.
Overall, I have mainly great things to say about the class. The lectures were very packed with content and were covered/explained very well. The one thing I struggled with was the large amount of homework, it was often daunting to have multiple problems which each looked like they could require a large amount of time/thought working on. I know the intent was to have a challenge, but I would find myself trying to complete a little bit of each question as to not waste all of my time on one problem, instead of fully devoting myself to each problem I attempted. Maybe this was just me, but I think it would have been more helpful if you explicitly told us that it was alright to not finish every problem.

What advice would you give to students who are considering taking this course about its level, the amount of work required, any prior training needed, and ways to get the most out of the course?

Comments
Programming experience is more helpful than implied by the syllabus.
I think the most important thing is to stay on top of your homework and go to the office hours if you need to.
To students who are considering taking up this course, I would definitely encourage them to go ahead with this for it is a challenging yet enlightening experience. Yes, there is a lot of work and effort that is required to be put in but I feel that the outcome is for sure worth it. Personally, it took me 2–3 days to adapt to the kind of work and expectations that were required by this course, like the hours it takes to complete the work and the syllabus. I would advice students to go through the syllabus before hand and tell them to expect at least 2–3 hours of work everyday, if not more. However, I don't think that should be taken in a negative sense. Since there are no knowledge pre-requisites, everything is taught within class and it is a free space where any questions can be asked. Students need to keep in mind that the homework assignments for this course are designed in a way that goes beyond what is taught and challenges them to see math from different perspectives. Another thing I would advice is to try your best. The main goal of this course is not to get every answer right, however it is to put forth your thinking process and understanding, even if you cannot reach the answer. Some ways to get the most out of this course would be – going to office hours, paying attention and participating in class, collaborating with peers on homework assignments and not being afraid to ask questions.
To someone who was already a math nerd, this course somehow made me fall even deeper in love with the subject. The topics covered in this course qwev challenging and required many hours of work outside of class. However, I enjoyed every second of it despite the occasional frustration and late nighters that came with not being able to solve a hard problem. I don't believe a lot of background in math or computer science is necessary to succeed in this course; instead, I think a passion for cryptography and being willing to spend time on the problems are the most important things to consider choosing this course.
I would recommend doing a little bit of research about python during the course to make it easier for yourself to code programs to

Comments
break ciphers, especially because the programs make such a difference. Additionally, I would take full advantage of office hours, emailing Stephen, and utilizing the textbook with the course. I struggled with the “modulus for Z/n ” aspect of the math, which was the foundation for all the math we ended up doing. Through the command+F function with my online copy of the textbook, I was able to ask more specific questions during office hours and narrow down exactly what confused me about the topic.
Be patient and ask questions
No prior training. Someone who is interested in math would love it.
you should defo have some programming experience before and have a higher experience and level of knowledge in math to really fully understand the concepts in this class, because they are very different than some average math or cs class.
A strong understanding in algebraic properties is recommended, and some familiarity with matrices is also nice. No prior coding experience is needed as all coding will be explained from the simplest level. Several aspects of the course can be very difficult to understand at first, but note that the main focus of this course is to explore and introduce you to an area of math that you've probably never seen before. There is no need to worry about grades as the course is not grade-oriented. The homework is given daily and all will be given feedback by the instructor/TA, and certain difficult questions may also be reviewed in class. If you are struggling with homework, you can just ask for help from the instructor during office hours. In fact, make the most out of office hours to ask anything from your instructor, not just regarding homework. The most important thing is to keep an open mind and have the willingness to learn something new and exciting. Have fun learning cryptography!
I would tell them to become a little bit familiar with basic Python programming before the class and to take all the opportunities for help and collaboration available. Go to office hours if you don't understand something and work with your classmates. Don't be afraid to ask questions.
It gets easier and you start to understand better after a while even if the class/homework seems impossible
The course is quite hard, but it is equally rewarding. I spent much of my day working on the homework problems, and often still didn't come to a complete answer before the next class. Because of the high level and fast pace of the class, your time and care in attacking problems is almost always more important than your ability to solve them perfectly. There were students in the class of all different math levels, and the instructors were able to work around that and explain concepts in a way accessible to all. To get the most out of the class I would say to use all available resources (teachers, classmates, code, your own thinking) before simply searching up an answer. Even though the work is challenging, the experience of that struggle will teach you so much more than a perfect copied-down answer.
This is a difficult yet rewarding class. You are not expected to have a basis in higher-level math or in computer science, but a dabble in some of these fields would be very helpful. The work is much more fun with groups, but make sure you can a lot time to process on your own so you can all think creatively.
A prior basic-medium knowledge of coding (even if not mandatory) is extremely suggested: I really suffered from never having done coding before. On the other hand, any math preparation would be fine since the topics discussed and analyse in the course differ widely from the subjects taken in high school. Definitely not a light course, in terms of work required and homework: you will find yourself facing extremely hard questions alone, and will definitely fell frustrated several times. Nonetheless, overall a great course for math and coding lovers, gives you the chance to explore math in ways you never experience in high school. I would encourage anyone that is willing to focus for a long time in class (and outside) to take this course. P.S. The teacher is really able to make you appreciate the beauty of the subject in its different forms.
If you are on the edge about taking this class, I would absolutely encourage it. The course goes over several cryptographic systems and all of the math behind them. There is not much prerequisite, some previous python is helpful, but really not needed. That being said, the class is very rigorous, you will have many hours of homework, and will be learning some complicated math/cryptography concepts. If you want a challenge, and an eyeopener into the realm of cryptography and some deeper math, I would totally recommend this course. If you don't have passion for math and a drive for work, I would probably advise picking a different course, because this class is a lot of work (fun work, but still work!).

Comments about the Instructor

What did Stephen McKean do that was most helpful for your learning?

Comments
Engaging classes, fun activities
He explained and taught the material very well.
One thing professor Stephen did which I thoroughly enjoyed was the amount of times he went out of syllabus to talk about topics brought up in class. I really liked going on those tangents and exploring the depths of math, even if they weren't part of our syllabus. I feel like doing this really helped my learning as it taught me that there are so many areas of math where beauty lies which I just haven't discovered.
I liked the tangents on homomorphisms, the different types of infinity, and transcendental numbers during the lecture — I felt they enriched my learning of math and introduced me to even more fascinating topics. Also, I feel the lecture was structured with a great combination of definitions and examples for me to understand the concepts.
Responding to questions and giving useful advice
Made the class engaging. The course was just fun, he was very knowledgeable.
Help us in office hours
The lecture notes that he made were very helpful in reviewing materials and doing homework. Giving easy-to-understand examples after explaining a certain topic really helped me wrap my head around that material better. I also liked how he would sometimes allocate time at the end of the class for 'lab', where we could explore a certain topic ourselves, try writing our own code, play around with elliptic curves, etc. He and Jonathan (the TA) always walked around the class to see how we were doing. If we had any problems, they would always be ready to help us out.
Office hours were extremely helpful.
<ul style="list-style-type: none"> – set interesting assignments which challenged us – gave useful class notes so that we could recheck if we forgot – answered all our questions & knew what he was talking about – office hours were a great time to get help with work
Like I said in a previous question, his consistent availability inside and outside of class for questions/ extra support with a concept really helped me. He was also careful never to give too much away about a problem which, while occasionally frustrating in the moment, is so important in facilitating actual learning.
He radiates a passion for mathematics, teaching, knowledge, and curiosity. This made his lectures so enjoyable. Even when topics seemed boring, he made them fun.
Explanations extremely clear and always willing to help even outside of class and of office hours. Makes you love the subject and as a consequence he encourages you automatically to engage in the course.
I have only good things to say about Stephen. In his lectures he explained complicated topics in ways that we could understand. Stephen is very knowledgeable with the mathematical content of the class, and was able to answer pretty much any question we asked, or at least pointed us to where we should look.

What might the instructor have done differently to help you learn more?

Comments
I thought the class was taught as well as it could be.
To further increase my learning, I would have liked to have more group interactions and just teamwork assignments in class which I wish we could have done. Especially since this is a content-heavy course, I feel like communicating with other people and having that understanding develop through either group work/class assignments would have been more helpful. Even though I did enjoy the sessions in that they were very interactive, I would have liked working with others in my class as well.
Nothing that I can think of.
Explaining the concepts more clearly (may be because of time constraints) Otherwise, I understood the concepts well.
I dont know
Perhaps reducing the amount of time spent on tangents could help us stay more focused and make sure we could review everything in time.
Have us read a little bit about sets, groups, rings, and fields before the class or right at the beginning to make everything else easier to understand.
More class and group activities
I can't think of anything!
An alternating lecture and application system throughout class might be better for students to internalize the information they are learning.
I might not share the vision of giving homework without explaining the subject before: it can sometimes be extremely interesting and rewarding, but in my experience, and in the one of many other classmates in this course, it has been rather frustrating and time consuming. Maybe changing slightly the structure of homework could help future students understand better the requirements for the homework.
One thing that would have been cool to learn would be more introduction behind each cryptographic system. It would be interesting to learn the context behind each one, and the thought process that led to their creation. It felt like they were introduced in kind of a mystical way, where we only learned how they worked, not so much how it was invented.

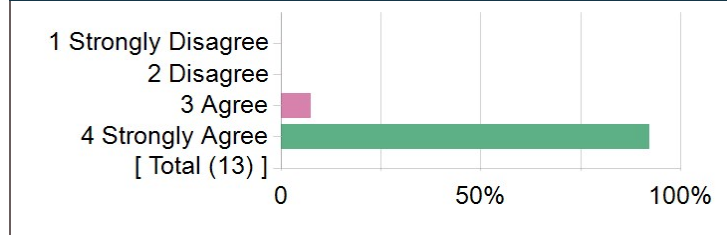
What was the most interesting thing you learned in this class?

Comments
Group theory, different ways to look at math.
The most interesting thing was the fact that you could use math to analyze how often certain encrypted letters were used in order to decode a text.
elliptical curves
Using sage to encipher and decipher secret messages
Group theory and isomorphisms
i dont know, everything
Graphing in $Z \text{ mod } p$
I loved doing ElGamal. It made a lot of sense to me, and it was especially fun to try to extend it to elliptic curves. I also enjoyed the bizarre brain-bending that came with learning about how different groups/rings/fields worked. (For example, in $Z/5$, $4+2=1$. That was a weird day.) All of the material was interesting, though.
Elliptic curve & projective geometry and how that can be used in cryptography
There are so so many things, but one that I think I will always remember (and tell people) is that in a slightly different ring, 228 has the exact same function as $1/8$.
The plethora of encryption methods in the world. I especially enjoyed learning about el gamal
Algebraic Geometry
Either the quaternions or the ideas behind RSA

Rate this course based on three of its primary learning objectives.

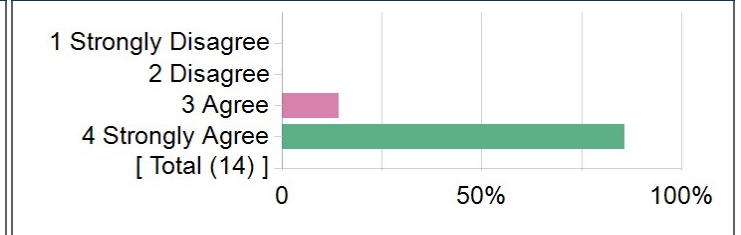
Competency Statistics	Value
Mean	3.8
Median	4.0
Mode	4
Standard Deviation	0.4
Standard Error (base on SD)	0.1
Population Standard Deviation	0.4
Standard Error (base on PSD)	0.1

1. This course introduced me to new ideas in abstract algebra



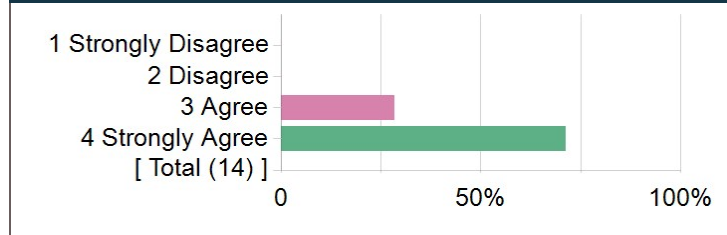
Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Agree	3	1	8%
Strongly Agree	4	12	92%

2. This course improved my understanding of cryptography theory.



Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Agree	3	2	14%
Strongly Agree	4	12	86%

3. This course showed me how to use Python to simplify some computations used in cryptography.



Options	Score	Count	Percentage
Strongly Disagree	1	0	0%
Disagree	2	0	0%
Agree	3	4	29%
Strongly Agree	4	10	71%