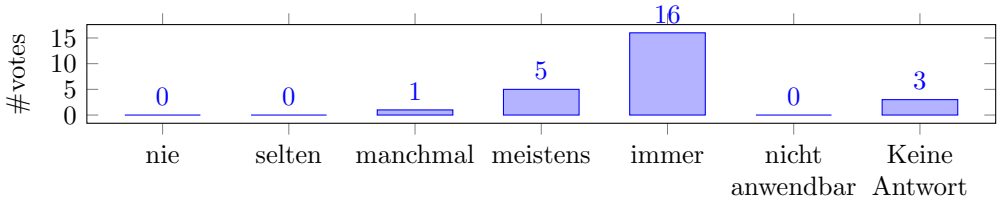
Modul:	**Semester:**
Cryptography	Wintersemester 20/21

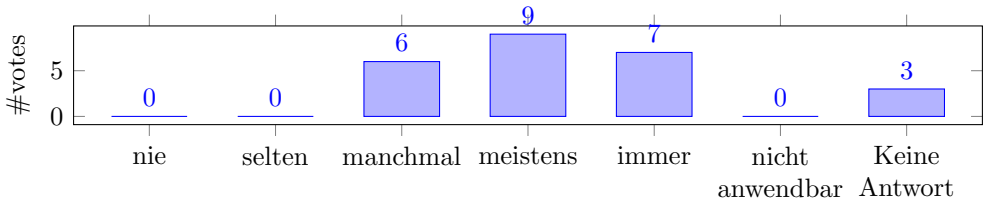
Ergebnis der Online-VLU. Die Umfrage fand in den letzten beiden Vorlesungswochen statt.

1 Bewertung der Vorlesung

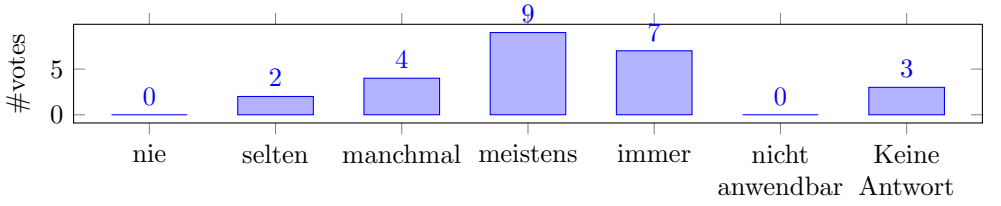
Wie oft hast du die Vorlesung besucht?



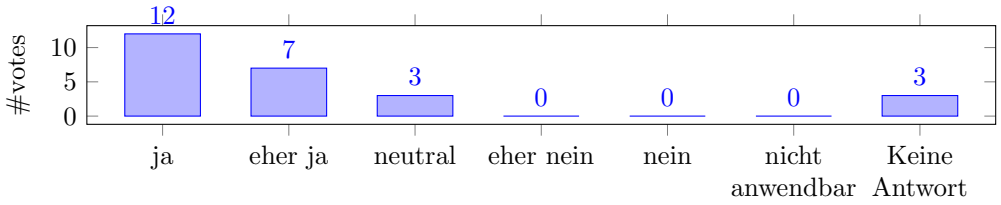
Wurden Themen durch Beispiele veranschaulicht?



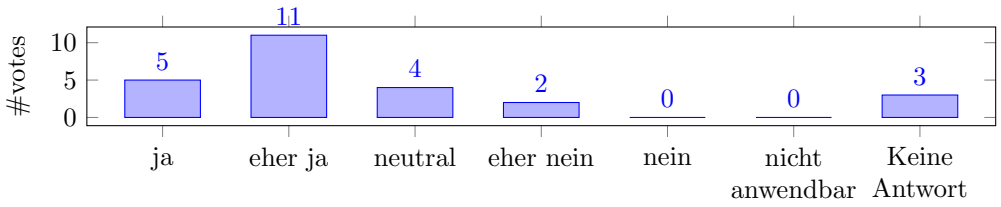
Wurden die Themen ausführlich genug erklärt?



War die Struktur der Vorlesung klar zu erkennen?

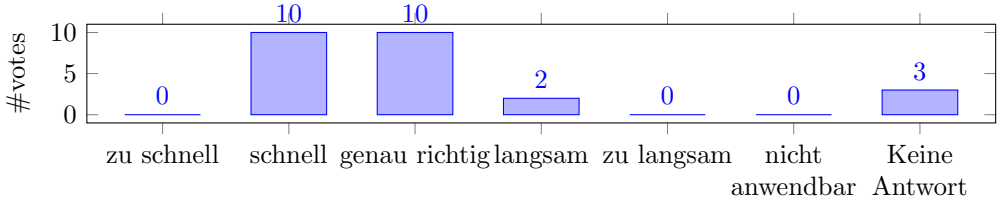


Waren die Folien/das Skript hilfreich?

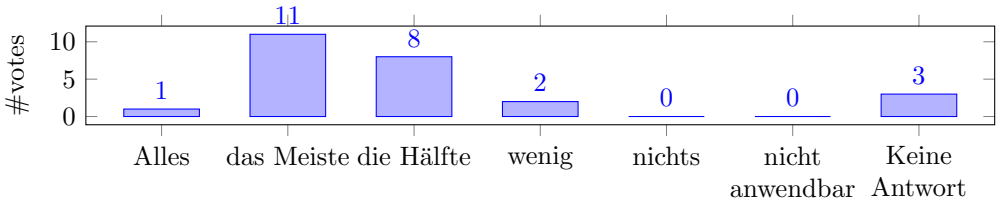


2 Bewertung der Dozierenden

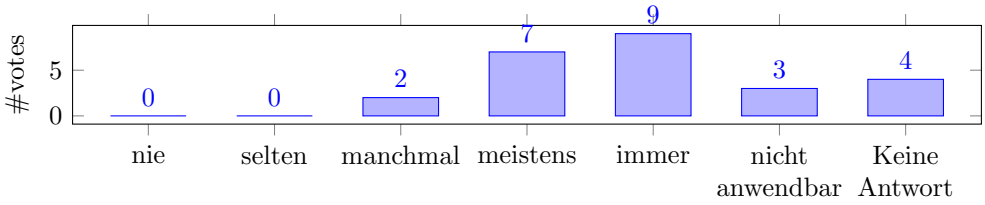
Die Geschwindigkeit der Vorlesung war...



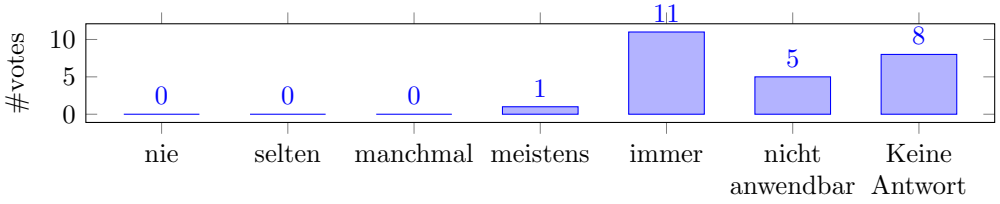
Wie viel verstehst du während der Vorlesung?



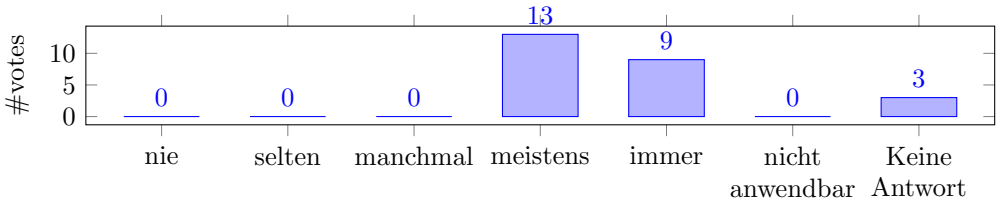
Ist der Dozent/die Dozentin gut auf Fragen eingegangen?



War der Dozent/die Dozentin außerhalb der Vorlesung für Fragen etc. erreichbar?

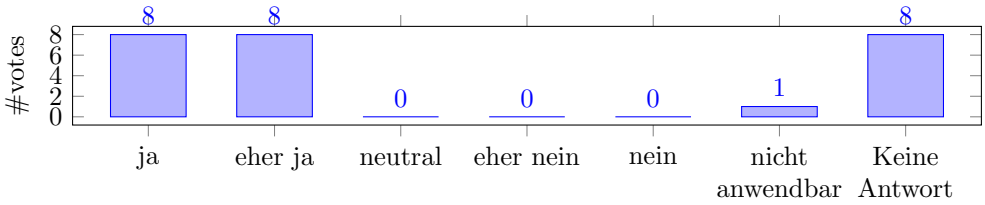


War die Dozentin / der Dozent akustisch gut zu verstehen?

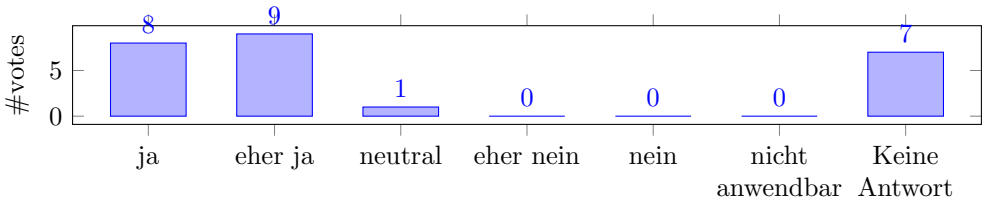


3 Bewertung des Moduls

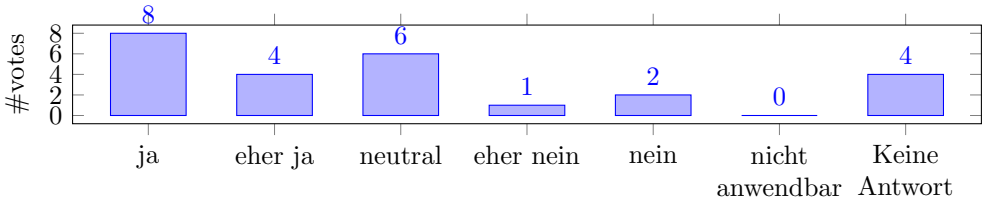
Helfen die verlangten Studienleistungen, das Modul erfolgreich abzuschließen?



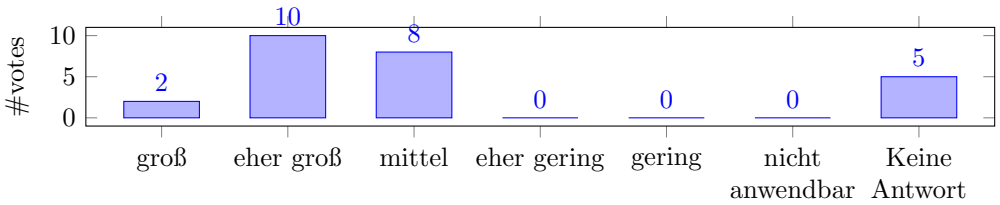
Findest du die verlangten Studienleistungen für dieses Modul angemessen?



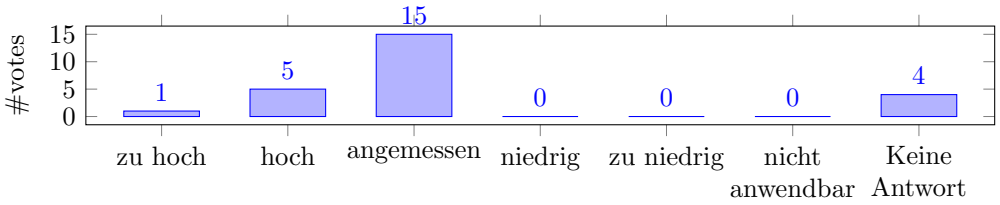
Würdest du das Modul weiterempfehlen?



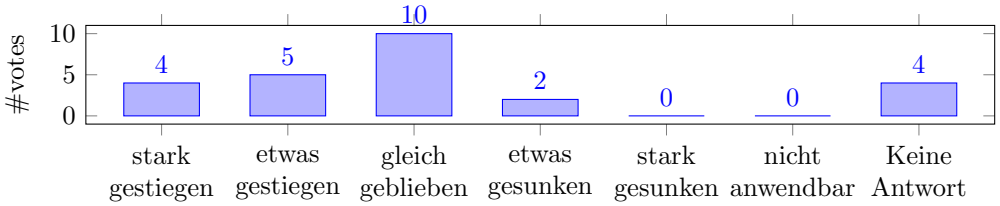
Der Praxisbezug war...



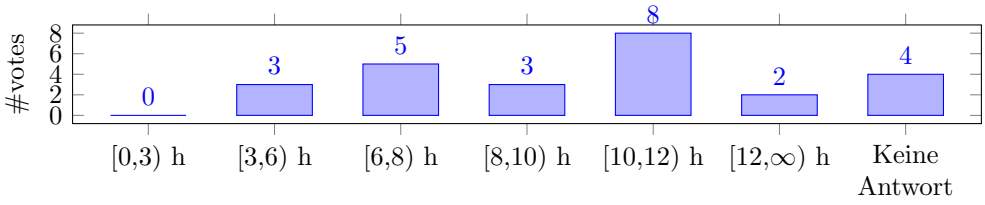
Ist der Arbeitsaufwand für dieses Modul im Hinblick auf die LP-Zahl angemessen?



Dein Interesse für dieses Thema ist...

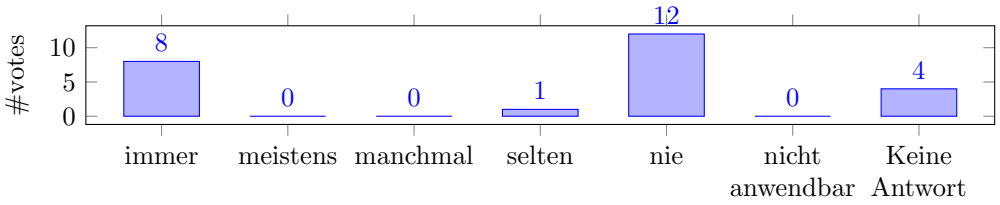


Wie viele Stunden hast du insgesamt, inkl. Vorlesung, Übung, Übungsaufgaben..., pro Woche für dieses Modul aufgewendet?

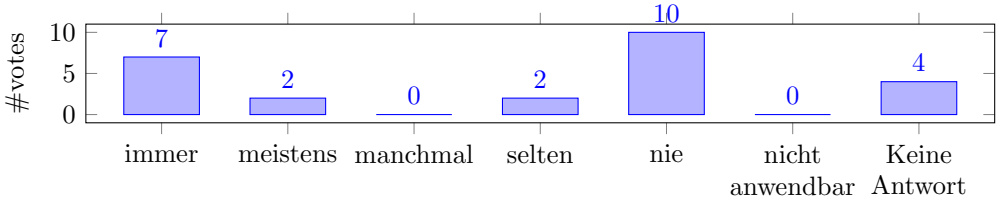


4 Bewertung der Übungsaufgaben

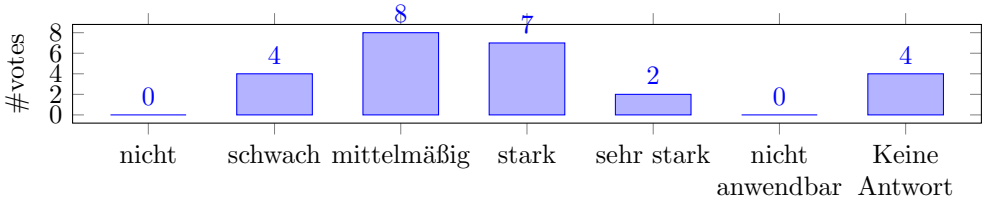
Wie oft hast du die Übungen besucht?



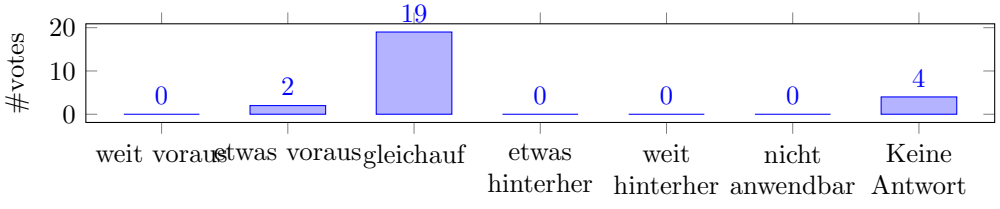
Wurden die Übungsaufgaben rechtzeitig zur Verfügung gestellt?



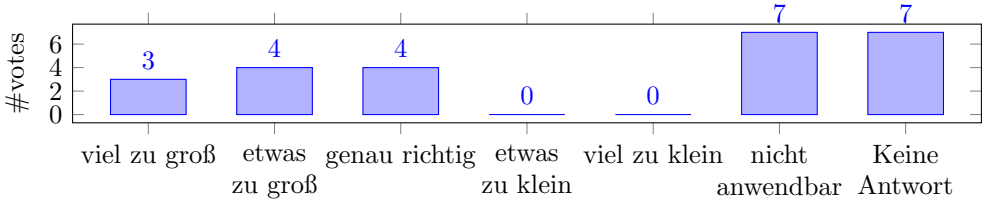
Die Schwierigkeit der Übungsblätter schwankte...



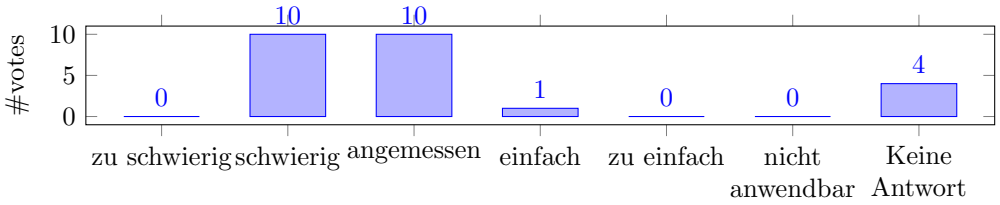
Die Vorlesung war...



Die Übungsgruppe war...

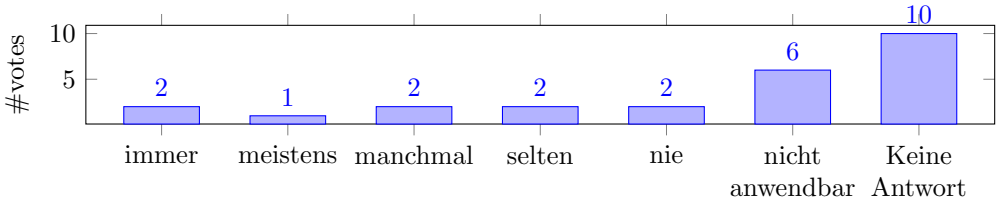


Die Übungsaufgaben waren meistens...

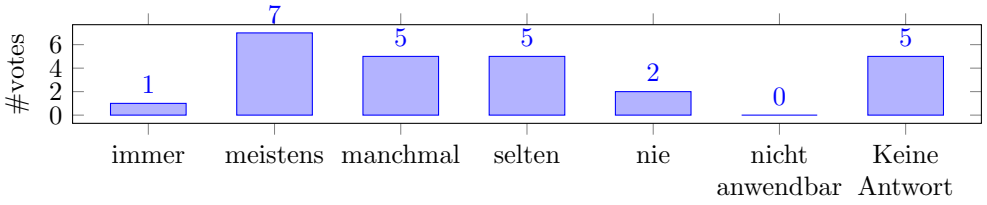


5 Bewertung des Tutoriums

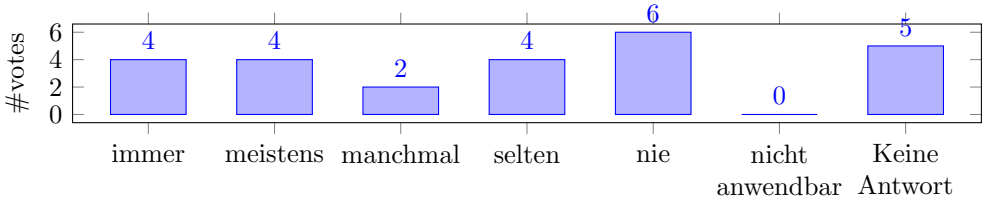
War der Tutor/die Tutorin außerhalb der Übung für Fragen etc. erreichbar?



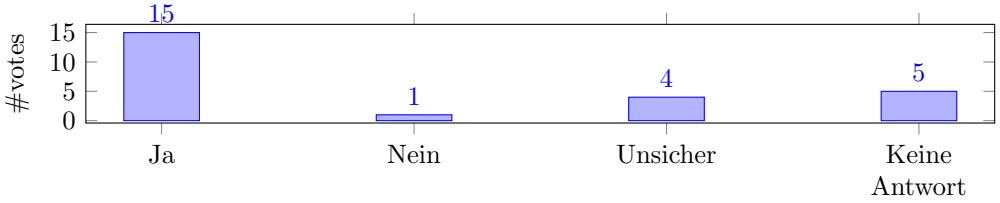
Waren die Korrekturen des Tutors/der Tutorin nachvollziehbar?



Wurde der Tutor/die Tutorin mit dem Stoff der Übung fertig?

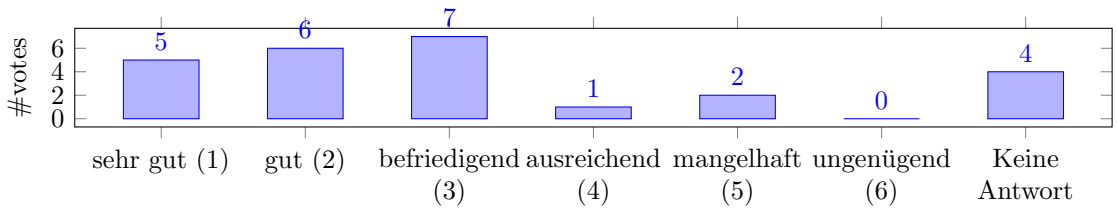


Lohnt sich der Besuch des Tutoriums?



6 Abschließende Bewertung des Moduls

Note:



7 Freitextkommentare

7.1 Was hat dir an dieser Lehrveranstaltung gefallen?

The content was interesting.

Das Thema war intressant und es wurden einleutend erklärt. Viele Defenitionen waren gut vormuliert in der VL.

Der Dozent hat mit viel Hintergrundwissen das sehr komplexe Thema gut verständlich gemacht

Die Begeisterung des Dozenten für sein Fach

- interactive parts of the lecture - lecturer's willingness to answer questions extensively - topics were broadly covered

The contents The lecturer made sure not to go that much into overtime anymore after he got the feedback from the first survey. The tutor also improved the formalism in the solutions presented.

- really good explanations with useful examples - in-depth repetitions (not just browsing through the slides) at the beginning of each class (really helpful, especially if one didn't understand something last class, listening closely on the repetition would usually do the trick) - bonus tasks that give an insight to applications and extensions that are beyond the scope of the course, but might be interesting

Der Dozent hat sich sehr viel Mühe gegeben praktische Anwendungsbeispiele aufzuführen und die Vorlesung damit sehr interessant gestaltet. Sehr gefreut hat mich, dass viel wert auf korrekt geführte Beweise gelegt wurde. Die Beweise in der Vorlesung hat der Dozent meiner Meinung nach sehr verständlich erklärt, auch wenn ich ab und an eine kurze Pause gebraucht hätte um einzelne Schritte nachvollziehen zu können. Aber dafür gab es ja auch die Vorlesungsaufzeichnung in der man einfach auf Pause drücken konnte um über das Gesagte nachzudenken. Die Aufzeichnung der Vorlesung war generell sehr hilfreich, wenn doch einmal beim nachbereiten eine Notation nicht mehr hunderprozentig klar war konnte man schnell nachhören was an der Stelle dazu gesagt wurde.

- The option to meet people in the first exercise session in the breakout rooms (" speedgrouping"). I am still meeting with people that I first met there to discuss the exercise sheets. I even met people that I had seen for years on the campus and in lectures, but never talked to, which is quite nice. - The free BBB room which is a nice meeting point for discussing (and sometimes ranting about ;)) the exercises. - Availability of lecture recordings! (Every course in the program should do that, it's extremely helpful to be able to rewind a bit or watch the lecture whenever you want) - The polls that make the lectures more interactive and motivate to think a bit more about the topics. Sometimes all of the answers are wrong, or multiple are " a bit" true, but this is fine, since the questions make you think about it. - Motivation of the lecturer to make the lectures and tutorials interactive, make topics accessible and generate a discussion. - Exercise Sheets that are generally tailored to make you think and discuss about the topics, a lot of " optional" exercises that go a little bit further than the actual contents. - Historical and other anecdotes / fun facts that make the lecture more vivid (like world war crypto machines, diplomatic bags, ...). - The moodle is the probably best working method of submitting exercises that I have seen in the CS courses in Bonn. - Of course, the beautiful paintings on the first slide each session ;)

Enthusiasmus des Dozenten und gute Aufbereitung der Themen. Außerdem hat mir gefallen, dass oft kleine einwürfe zur aktuellen Forschung von einzelnen Themen kamen!

When explaining new ideas, lecturer references related literature and papers. The contents taught in this lecture are highly related to the trend of/topics in academia/literature, which is very helpful for students who would like to do research afterwards.

7.2 Was könnte noch besser gemacht werden?

Some model answers to tutorials would of helped.

Manche Folien waren komisch geschrieben, Varibalen waren vlt unklar oder nicht vorher defeniert. so das der nachfolgende Algorithmus schwieriger versteh bar war.

Tutorium: Der Tutor kannte sich mit dem Thema selbst nicht gut genug aus. Dadurch konnte der Tutor nicht immer alle Fragen zufriedenstellend beantworten, sodass der Dozent zusätzlich erklärend eingreifen musste. Teilweise hat der Tutor selbst die Aufgaben zuerst nicht/falsch verstanden und fehlerhafte Lösungen präsentiert, die vom Dozenten während des Tutoriums korrigiert werden mussten. Daraus entstehende Diskussionen zwischen Tutor und Dozent waren manchmal mehr verwirrend als hilfreich. Vorlesung: Der Dozent hat oft während der Vorlesung auf seinen Folien Zeichnungen und zusätzliche Hinweise erstellt. Diese waren manchmal schlecht lesbar/erkennbar. Außerdem waren dort sehr wichtige/hilfreiche Inhalte, die im Nachhinein nur schwerer zugänglich in den Aufzeichnungen, aber nicht im PDF der Folien verfügbar waren. Es wäre hilfreicher, wenn die Folien von vornherein vollständiger wären, sodass diese zusätzlichen Inhalte gerade mit der Online Lehre außerhalb der Live-Vorlesung leichter zugänglich sind. Vorlesung/Aufgaben: Definitionen und Aussagen waren an einigen Stellen mathematisch/logisch ungenau formuliert. Das erhöht die Schwierigkeit beim Verständnis sehr stark. Es wäre hilfreich darauf zu achten, dass wichtige Definitionen und Aussagen auf den Folien und in Aufgabenstellungen eindeutiger formuliert werden, um eine unnötige Verständnishürde zu vermeiden.

Es wäre hilfreich, wenn der Dozent mit seinem Tutor eine Tutorenbesprechung machen würde. Dann wären die Übungsbesprechungen weniger konfus. Das Hin- und Herdiskutieren zwischen Tutor und Dozent während den Übungen hat bei mir oft zu großer Verwirrung geführt, und oft wusste ich am Ende nicht, was nun richtig und was falsch ist. Diese Diskussionen sollten meiner Meinung nach besser ausgelagert werden. Außerdem hatte ich den Eindruck, dass an manchen Stellen schon eine gewisse Intuition für Kryptographie vorausgesetzt wurde.

- slides: design and structure - proper tutor please (nothing against the student tutor, he was good. But I think I would have preferred if the lecturer who was present in the exercises anyways (!) did conduct the exercises) - exercise tasks: formulate a bit more clearly and extensively

The organization of the exercises did not improve much after the first feedback. Issues with the solutions presented by the tutor were not taken seriously by the lecturer and he understood it as criticism of the tutor, which I think it was not, but rather criticism of the organization and preparation of the exercise (on the side of the lecturer). We still did not really get 'correct' solutions as in: The tutor still had to come up with his own solutions without having one that was approved by the lecturer. This still leaves the uncertainty if the solution would be accepted like that in the exam. Communication was another issue. Ideas for the exam conduction were given late and upon request. (I understand the uncertainty of the information, but knowing what is planned is also worth a lot) Furthermore, it was never communicated clearly that there were no admission restrictions for the exam, we just got a vague " I just said who is admitted, not who is not admitted" , again upon request. If the communicated admission criteria for the exam would have acutally held, I think it's not a good idea to have just one tutor and make all students hand in their solutions by themselves and not in a group. Corrections were late, but most exercises were corrected.

- Formality: For an algorithmics course, the lecture and exercise tasks sometimes lack formality. Variables just pop up without stating where the come from. Adding a few lines like " n in mathbbN" would be helpful. - Comments on graded sheets: The comments on the graded sheets were scarce, for bonus tasks they were basically non-existent - Graded sheets available on time: Often, the tutor forgot to upload the graded sheets before the exercise meeting, said he would do it afterwards, and a week later, they were still not uploaded. - Using tutorials for exam preparation: It might sound nice to not present fully correct solutions in the tutorials and have all students engage in order to reach a good solution, but for one, the time frame is to small for that, and two, it does not help at all in preparing for a WRITTEN exam. Sure, for an oral exam discussions can be valuable, but a written exam doesn't give students a space for discussions. More than anything, those discussions and on-the-fly changes to the presented solutions were confusing as hell. Often, at the end of talking about a task for 40+ minutes, I would not know if what is on the screen is correct, if I noted down all the changes, why we had to do those changes and what was not correct about it and why... Please, PLEASE just start discussions from correct solutions. That is absolutely possible, there will always be a couple of students that did it differently or wonder why we can assume this or that. And it would be much more helpful for an exam what solution would give me full points. - The lecturer could stand up to their mistakes and straight on tell the students when there are no conditions for being admitted to the exam. Comments like " Well, you have to read my statements, I didn't say anything about not admitting anyone to the exam, is that clear enough?" in an exercise meeting four weeks prior to the exam are simply disrespectful, especially since the lecturer was asked multiple times to clarify the non-existence of admission conditions. On the slides and in the moodle it still reads " If you solved 50% of all corrected exercises, you are admitted to the exam" which, yes, mathematically doesn't imply that with less points, one would not be admitted, but linguistically, I think we can all agree that it does indeed imply just that.

Die hochgeladenen Vorlsungsfolien habe eine für mich cryptische Nummerierung, hier würde ich mir eine Erklärung der Nummerierung, oder eine " üblichere" Nummerierung wünschen.

- TUTORIAL SESSIONS: Unfortunately, the tutor himself has not done the course in an earlier semester, but is doing it for the first time. Thus, on a regular basis, the professor, who is present in the session as well, has to correct the tutor. Also, a lot of times the tutor does not know the answers to specific questions or how to explain things, since the topics are new to him as well. This damages the quality of the tutorial sessions a lot. Above that, due to the same reason, I have a feeling that a lot of minor or mayor errors in exercise corrections are not pointed out, instead the tutor awards full points without further comment. This is a critical problem since in the exam those errors maybe WILL count while in the exercises students are taught that they do not. It is unacceptable to hire a tutor with no previous experience in the lecture. This is obviously not the tutor's fault, but the fault of the person who decided to choose him as the tutor. Above that, since there was only one tutor, not all the exercises submitted could be corrected because the contracted working hours didn't allow that. That said, props and thanks to the tutor who surely works a lot and takes a lot of time to understand the topics and to be able to explain them. - SLIDES: Sometimes, the lecture slides lack the formality that is neccessary to be able to work on the exercises. Example: The (very central and important) " Game Hopping Lemma" was never stated formally, but only motivated with some drawings (neither you could really find it online or in the book under this name). Often times, proofs are only sketched, where the students would really benefit from reading the formal proof. I like that the lecturer tries to make the topics more accessible, but the formal part should not be forgotten about. - EXERCISES: Although it was explicitly asked multiple times, the professor never clarified that the exercise sheets are not mandatory for the admission to the exam. He only stated in the first lecture that, if we achieve 50% of the points, we get admitted to the exam, which is clearly - while formally correct - a misleading and incomplete statement. I appreciate that the lecturer obviously cares a lot about the fact that the students do exercises regularly. However, as Master students, I think that one can expect us to work in a responsible way without concealing facts about the admission rules.

In den Folien scheinen gleichbedeutende dinge teilweise verschieden Dargestellt zu werden, manchmal ändern sich " Konventionen" (z.b. eingabeparameter vom KeyGen) ohne Erklärung. Solche inkonsistenzen sind dann sehr verwirrend wenn man noch nicht 100% sicher mit dem stoff ist, und man sucht ggf. lange nach einer Begründung.

7.3 Hier hast du Platz für weitere Anmerkungen und Feedback zum Modul.

Das im Tutorial keine Musterlösungen vermittelt worden waren war schlimm.

Having a tutor for the tutorial is nice, but if the lecturer is there anyways in every tutorial and keeps asking the tutor questions and interrupts him, why does the lecturer not do the tutorial instead?

Next time when students criticise something about the tutorial, don't go into the next exercise meeting and make it seem like they all personally attacked the tutor. Of course he's doing a good job, especially in this difficult situation, i.e. not having completed the module beforehand, not getting sample solutions to work with and often not even a chance to talk his own solutions over with the lecturer. But all that doesn't make criticism on the overall procedure less valuable.

If you're interested in the " inner workings" and theory of cryptographic schemes and like number theory and some probability stuff, this module is for you. You'll need to dedicate a lot of time though; the 9 credit points are not free ;) Mind that it's more about the inner mathematical workings of the crypto schemes and analyzing possible attackers than about concrete implementations.

7.4 Hier hast du Platz für Anmerkungen und Feedback zur Umfrage.

Is there a time window in which I have to complete the questionnaire? I spent 20 minutes on this open comment page and then when I wanted to submit, I got an error message saying I had probably been inactive for too long and had to do it all again. Maybe typing isn't enough activity for the website? In that case, the open comments should maybe be split up again, even though it's useful to see all the questions at once...

Ob die Übungsaufgaben dazu beitragen das Modul erfolgreich abzuschließen ist zum Zeitpuntk der Umfrage nicht eindeutig zu beantworten, weil der (hoffentlich erfolgreiche) abschluss des Moduls ja noch aussteht.