Introduction to Modern Cryptography (IMC)

Response to student feedback in 2022/23 course survey

I/We have taken note of the feedback from students in this course survey, and have the following comments in response.

- The students seem to struggle with the mathematical background needed for the course. The course only requires one to know how probability works (random variables, independence, Bayes' theorem), asymptotic computational complexity (e.g., big-O notation) and have a very high-level idea of what an algebraic group is. This is all the background needed, and in the course, I do refresh these topics. Next year, I plan to spend more time on the background and make it clear that students are welcome to ask me, or on Piazza, questions related to the background material. I want to add that what is needed in the course is not really a strong math background, but it is important to like problem-solving, and not be afraid of approaching problems that appear a bit abstract. I strongly think that if you enjoyed the courses on algorithm and complexity theory, you will like this course as well.
- About the notation used in the tutorials and the lectures. We will make sure to use consistent notation in the tutorials.
- About the tutorials' material. We will make this available on learn, and not on piazza.

Michele Ciampi, 12/07/2023