Rules for Solving and Submitting Take-home Exam
Foundations of Cryptography 2019

Douglas Wikström, dog@kth.se

May 10, 2019

The Code of Honor[1] applies to this course. Make sure that you read it carefully. Below we detail the rules specific to this course. The goal of these rules is to improve learning and avoid wasting precious teaching time on administrative tasks.

1 Deadline

A take-home exam is an exam, so zero points are awarded late solutions. There are extreme circumstances where the deadline rule does not apply, e.g., severe medical problems or the death of a family member.

Please contact the lecturer as soon as possible in such a case by phone or by email at dog@kth.se with subject `DD2448 Emergency`. Lack of time due to work or leisure outside the university or enlisting on many parallel courses are not considered extreme circumstances.

2 Formatting and submitting solutions

1. The solutions must be typeset using LaTeX and the designated template file. (A brief introduction to LaTeX is available at `http://tobi.oetiker.ch/lshort/lshort.pdf`. This suffices for this course.)

   This forces students to write organized solutions that are easy to follow. Furthermore, learning LaTeX is important to present mathematically oriented content in reports and presentations, which is one of the goals of the course.

2. The printed sheets of paper must not be stapled together, collected with a paper clip or similar. Instead they must be collected into a *transparent* folder with easy access. The students' names must be visible without opening the folder.

   The first requirement ensures that we can easily copy your solutions after marking them, which is needed since we walk through your solutions during the oral exam. The second requirement simplifies administration.

3. The folder must be placed in the Krypto-compartment at Student service on level 4 in the E-building. Make sure to check when it is open!

   Documents in the PDF format are not completely portable and sometimes print incorrectly. Students also forget to attach files, or attach the wrong files, or put them in the wrong postal box. Dealing with such problems is a waste of both your and our time. The rule avoids these problems.

[1] `https://www.kth.se/en/eecs/utbildning/hederskodex`

3 Solving problems

1. You must write down your own solution individually in your own words. This also applies to programs you write. Any exceptions to these rules will be explicitly stated.

2. You are allowed to discuss the problems in study groups of up to three students, but still, each group member must write down and hands in his or her own solution. (Not one solution per group and not several copies of the same solution.) Only *informal discussions* between the group members are allowed. In particular, you may not read the solutions of the members of your study group, e.g., sending or receiving somebody elses draft by email, or reading hand written solutions of other students, is considered cheating.

3. You cannot be a member of several study groups for the take-home exam, but you may choose a new study group different from the one used for the group project or for studying the exercises.

4. You must motivate all your answers, even to those problems where the final answer is simply yes/no or a number. Partial or flawed motivations give only partial credit, even if the final answer is correct.

4 Level of detail in solutions, proofs, and programs

In general, every student following the course must be able to follow all your solutions after reading the problem statements.

Reading problems. For problems where you summarize material you are asked to read you must strive to form a story line that the reader can follow. Choosing a suitable level of detail for different parts of your presentation to emphasize the most interesting ideas is considered part of the problem.

Programming problems. All programs submitted as solutions to Kattis must follow best practice in software engineering. Any reasonable code standard is acceptable, but you must be consistent, organize your code, and comment your code.

Mathematical problems. A solution to a mathematical problem should be a proof. What an acceptable level of detail is in a proof depends on the context and the target audience. Research papers you encounter may leave out arguments that are considered standard, but this does not mean that you can leave out such details, since your target audience is your fellow students.

You may, however, leave out details that are covered in prerequisite courses, e.g., you do not need to prove basic properties from group theory, or probability theory, but make sure that you state which properties you use.

5 Is something still not clear?

If some part of the above rules is not clear, then please send an email to `dog@kth.se` with the subject `DD2448 Solution Rules`, and we will update this document.