



KTH Computer Science
and Communication

Rules for Solving Problems and Reporting Solutions

Foundations of Cryptography 2014

The CSC Code of Honor¹ applies to this course. Make sure you read it carefully. This document only details 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 Deadlines

In this course, **deadline really means deadline**. Zero points are awarded late solution sets.

There are of course extreme exceptions where the deadline rule does not apply, e.g., severe illness or the death of a family member. Please contact the lecturer by email at dog@csc.kth.se in such a case. Lack of time due to work or leisure outside the university or enlisting on many parallel courses are not considered extreme exceptions.

2 Formatting Solutions

1. The solutions must be written down using \LaTeX and the template file for the given homework found at the handouts homepage². (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 student's name must be visible without opening the folder.

The first requirement ensures that I 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 Krypto14-compartment at the Student office at CSC³ before the deadline given on the course home page. No other way to submit solutions is allowed. In particular, emailed solutions or solutions put in my postal compartment will not be awarded zero points.

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 time. The rule avoids these problems.

¹http://www.kth.se/csc/student/hederskodex?l=en_UK

²<http://www.csc.kth.se/DD2448/krypto14/handouts>

³<http://www.kth.se/en/csc/student/studentexpeditionen-1.17048>

3 Solving Problems and Reporting the Results

1. You should write down your own solution in your own words. This also apply to programs you write as part of an assignment, i.e., each student is expected to write his or her own program. 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 writes 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 of a homework by email is considered cheating.
3. You cannot be a member of several study groups for the same homework set, but you may choose a new study group for each homework and/or your research presentation.
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.
5. The level of detail in your solutions and proofs should be such that even the weakest student following the course can understand the solution after reading the problem statement.

4 Is something still not clear?

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