Johan Håstad, CSC
January 14, 2008

Foundations of Cryptography
Rules for homework, Spring 2008

As always, the CSC Code of Honor (available electronically separately from the course home page) applies to this course. Make sure you read it carefully. This document only details the rules specific to this course.

Problem sets

There will be two traditional sets of problems. For each set you should hand in a written solution which you later discuss with one of the instructors. You will be able to reserve a time for the oral presentation via the course web page. Your solutions will be graded by the person with whom you have booked a time, *so, until you have reserved a time, your solution will not be graded at all.*

Writing programs and solutions should be done individually

You should write down your own solution *in your own words*. The same rules apply to programs you write as part of an assignment. Each student is expected to write his or her own program. Any exceptions to these rules will be explicitly stated on your homework sets. Unless explicitly stated the rules for code is as follows. Code should *not* be handed in with the solutions but made available electronically to the appropriate instructor. Instructions how to view the code should be included with the solution.

Collaboration in study groups

You are, however, 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). On your written solution you should clearly state the members of your study group. You cannot be a member of several study groups on the same homework set.

Deadlines and late solutions

Problem sets have a deadline which is a certain time on a certain day. For each homework set you may hand in some problems on time and some problems late. However, for each problem set, only one set of late solutions is accepted. After your oral presentation you may not hand in late solutions. *Late solutions must be put in Johan Håstad's mailbox at the department, level 4, Lindstedsvägen 3.*

Late solutions are graded as follows. Your score is multiplied by 0.9^d, where d is the number of *working* days that the solution is late. Solutions handed in late but on the correct day will be considered as being one day late. That is, if the deadline is on a Friday at 10:15 and one student hands in a solution on Friday at 16:00 and another student hands in a solution the following Monday before 10:15, both these solutions are one day late. A solution handed on on Monday afternoon is defined to be two days late. If you hand in some solutions on time and some late, only those that where handed in late are subject to the 0.9^d multiplier. Remember that you may only hand in one set of late solutions.

Presentation

As a part of the course you will present a research paper that appeared at a recent conference in cryptography. You should yourself choose which paper to present. As we limit the number of students that can present the same paper to two, please inform Johan Håstad as soon as you have made your choice.

Any paper that appeared in the three most recent years of any of the below listed conferences is automatically accepted. To present a paper from a different conference or year, submit name and year of conference and an electronic version of the paper to Johan Håstad. In particular, older papers can be presented if they are considered as "classical".

Accepted conferences: Crypto, Eurocrypt, Asiacrypt, Indocrypt, Fast software encryption, Cryptography Track of ICALP, Theory of Cryptography Conference, Financial Cryptography. Papers in cryptography appearing at the general theory conferences such as Foundations of Computer Science (FOCS) or Symposium on Theory of Computation (STOC).

Some remarks/rules in connection with the presentation

There are a number of rules and recommendations.

- The presentation is given a grade which is either "fail" or a multiple of 10 in the range $[30, 80]$. The grade is awarded based on the overall impression of the presentation. Giving a practice presentation with or without audience is usually helpful but will not be organized by the intructors.
- The time allowed for the presentation is 12 minutes and should contain a high level description of the result and some words about the techniques used in the paper. Timing is important and normally a warning is given when 3 minutes of the time remains and when the time is up[1]. Presentations lasting longer than 15 minutes are automatically given the grade "fail".
- The presentation should be done and prepared individually.
- The presentations will be given in blocks of up to 6 presentations in a 2 hour session. The student is required to attend the other presentations in the session in which he/she gives his/her own presentation. These presentation will be scheduled once the students have chosen the papers to present.
- Presentations can be given on the blackboard, using an OH-projector or by slides projected from a computer. It is usually considered that making a presentation as short as 12 minutes on the board is a difficult task and requires very careful planning and hence this must be considered to be the most difficult method.
- The intended audience for the presentations is at the level of a member of our course, i.e. people that know the basics of cryptography but are not experts.
- Background and overview are essential parts of the presentation. The audience should be told what problem is addressed, what the results are and something about its context. It is often useful and interesting to say something about the techniques used but in such a short presentation it is usually difficult to give a large amount of detail.

[1] These warnings can be changed for any speaker that wishes.