Institut for Matematik og Datalogi
Syddansk Universitet

Assignment 5 — Introduction to Computer Science 2013–14

This is your fifth (and last) assignment in DM534. The assignment is due at 8:15 on Monday, March 31. You may write this either in Danish or English. It must be made in LaTeX. (though you do not need to include your LaTeX code). Write your full name, your section number, and your "instruktor"s name (Magnus Gausdal Find for S7 or Christian Kudahl for S17) clearly on the first page of your assignment (on the top, if it's not a cover page). Turn in an electronic version as a PDF file via Blackboard through your DM534 course (choose the correct one, S7 or S17). The assignment hand-in is in the menu for the course and is called "SDU Assignment". Keep the receipt it gives you proving that you turned your assignment in on time. Blackboard will not allow you to turn in an assignment late.

Cheating on this assignment is viewed as cheating on an exam. You are allowed to talk about course material with your fellow students, but working together on this assignment is cheating. If you have questions about the assignment, come to Joan Boyar or your "instruktor" for DM534.

Please note that you must have this assignment approved in order to pass DM534. If it is not turned in on time, or if you do not get it approved, it will count as one of your two retries (assuming you still have at least one retry remaining) in the course, and you must have it approved on your only allowed retry for this assignment.

Assignment 5

Do the following problems and write your solutions in LaTeX. Write clear, complete answers, but not longer than necessary. Do not include the statements of the problems or other information not asked for in the problems.

1. In these three problems, consider the RSA system. Use the notation and algorithms from the slides presented in lectures on February 12

and February 19; they are available through the course's homepage. (You may use Maple to check your work, but show all steps of the calculations, using the algorithms in the slides.) Let $N_A = 1333$ and $e_A = 13$.

- Encrypt the message $m = 283$. For the modular exponentiation, use the algorithm from the slides, page 30. Show all steps in your computation.
- If you had created the keys, you would know that $p = 31$ and $q = 43$. From this information and $e_A = 13$, find the secret key d_A. Use the Extended Euclidean Algorithm from the slides, page 48. Show all steps in your computation.
- Decrypt the result you got when encrypting. Use the same modular exponentiation algorithm and show all steps in your computation. Check, of course, that you get the expected result!

2. Do problem 25 on page 518 of the textbook.

3. Do problem 44 on page 519 of the textbook.