Institut for Matematik og Datalogi
Syddansk Universitet

Assignment 6 — Introduction to Computer Science 2015

This is your fifth assignment in DM534/DM558. The assignment is due at **8:15 on Thursday, December 17**. You may write this either in Danish or English. It must be made in LaTeX. Write your full name, your section number (D1, D2, or D3), and your "instruktor"s name (Kristine Vitting Klinkby Knudsen, Mathias W. Svendsen, or Jesper With Mikkelsen) clearly on the first page of your assignment (on the top, if it's not a cover page). You should turn it in as a PDF file via Blackboard through your DM534/DM558 course. The assignment hand-in is in the menu for the course and is called "SDU Assignment". Choose the correct one for your section number, D1, D2 or D3. 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/DM558.

Please note that you must have this assignment approved in order to pass DM534/DM558. 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 in the course, and you must have it approved on your single allowed retry for this assignment. Note that you have only two retries in total for the assignments in DM534.

Assignment 6

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.

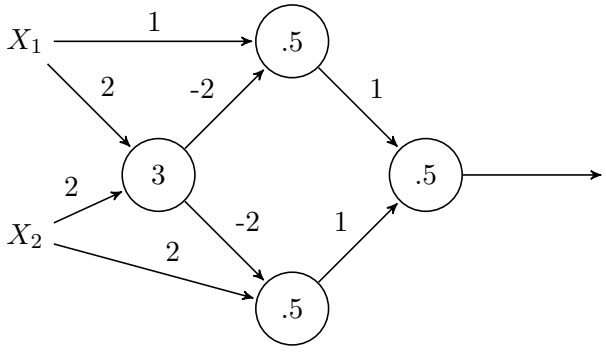
1. In these two problems, consider the RSA system. Use the notation and algorithms from the slides presented in lectures on November 10 and November 19; they are available through the course's homepage. (You may use Maple to check your work, but show all steps of your

calculations, using the algorithms in the slides.) Let $N_A = 1517$ and $e_A = 13$.

- Encrypt the message $m = 43$. 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 $p = 37$ and $q = 41$. 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.

2. Do problem 29 on page 533 of the textbook. It is OK to draw this by hand, scan the result, and include that in your LaTeXdocument.

3. For each of the four possible pairs of inputs (X_1, X_2), indicate what the output (on the arrow furthest to the right) from the neural network below will be. Use a table, and place the inputs in the order $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$.



4. Include your LaTeX code for this assignment at the end.