Aalto University
Department of Information and Computer Science
Pekka Orponen (tel. 25246)

T-79.4202 Principles of Algorithmic Techniques (5 cr)
Exam Thu 10 Mar 2011, 9–12 a.m.

Write down on each answer sheet:
- Your name, degree programme, and student number
- The text: "T-79.4202 Principles of Algorithmic Techniques 10.3.2011"
- The total number of answer sheets you are submitting for grading

Note: You can write down your answers in either Finnish, Swedish, or English.

1. Alice is using the RSA cryptosystem with key

$$K = (1003, 17, 59, e, d)$$

where e is an odd integer. The plaintext is $x = 237$. Show that then the ciphertext is $y = 237$.

2. How many lines (as a function of n) does the following program print? Derive a recurrence and solve it. You may assume that n is a power of 2.

```
function f(n)
  if n > 1:
    print_line(''foobity barbity'')
    f(n/2)
    f(n/2)
    f(n/2)
```

3. Suppose a Computer Science degree programme consists of n courses, all of them mandatory. The prerequisite graph G for the programme has a vertex for each course, and a directed edge from course u to course v if and only if u is a prerequisite of v. (We shall assume that the graph G contains no cycles.) Give a linear-time algorithm that takes as input the graph G and determines the minimum number of semesters necessary to complete the programme, assuming that a student can take any number of courses in one semester. Justify the correctness and complexity of your algorithm.

4. (a) Define what is meant by a search problem and by a reduction from one search problem to another.

   (b) Assume that there is a computationally challenging search problem A for which no polynomial time solution method is known. Show how you can argue using the notion of a reduction that another search problem B is at least as hard A, i.e., that a polynomial time solution method for B would imply a similar method for A.

Grading: Each problem 12p, total 48p.