Name: **Pers.nr.:** **E-mail:**

TIN092 — Algorithms

Exercise Set 6

Note: By submitting, you agree with the exercise set policy, which we enforce strictly:
`http://www.cse.chalmers.se/edu/course/TIN092/info.html#deliverables_exercisesets`

Exercise 1

As exercise [KT 8.4 a)] (only a)). Define the problem as a set of strings. To show that problem Y is NP-complete, you 1) show that $Y \in NP$ (give a polynomial-time verifier), 2) give a reduction A from some NP-complete problem X to Y, 3) prove that $s \in X \iff A(s) \in Y$. See [KT, p498-499] for an idea of which X to use. *Points: 4*

Exercise 2

As exercise [KT 8.15]. Define the problem as a set of strings. To show that problem Y is NP-complete, you 1) show that $Y \in NP$ (give a polynomial-time verifier), 2) give a reduction A from some NP-complete problem X to Y, 3) prove that $s \in X \iff A(s) \in Y$. See [KT, p498-499] for an idea of which X to use. *Points: 4*

Exercise 3

Prove that if $P = NP$, then the RSA cryptosystem can be broken in polynomial time. *Points: 2*
