# Problem Set 3

Due in class on Thursday, April 16, 2009.

## Problem 1 Computational indistinguishability preserved by efficient algorithms

[Textbook, Chapter 3, Exercise 2.]

## Problem 2 Smoothness of probability mass

[Textbook, Chapter 3, Exercise 12.]

## Problem 3 Modifications of a pseudorandom generator

[Textbook, Chapter 3, Exercise 15.]

## Problem 4 Role of error in interactive proofs

[Textbook, Chapter 4, Exercise 5.]

## Problem 5 Secrecy of commitment based on one-way permutations

A bit-commitment scheme based on a one-way permutation is presented in section 48.1 of lecture notes 19. A partial proof of secrecy is presented, but the task of showing that the constructed algorithm $A'$ has the desired advantage is left to the reader. Complete the proof by defining a suitable non-negligible function $\epsilon'(n)$ and showing that $A'(f(s))$ has the required advantage at guessing $b(s)$.