CSE 208: Advanced Cryptography Fall 2002

Problem Set 0

Instructor: Daniele Micciancio Sep. 26, 2002

Due: Thu. Oct. 3, 2002

This is a calibration homework. The grade you receive on this homework does not count toward your final grade. The purpose of this assignment is to test your background knowledge in complexity theory and basic cryptography, and give you some feedback. The homework is supposed to test both your knowledge of the basic definitions, as well as the techniques used in cryptography. I expect your solutions to be much more detailed and precise than the way the problems are stated here. (E.g., even if problem 1 refers to distribution ensambles without giving a precise definition, you are expected to use the right definition of distribution ensamble in your solution.)

Computational indistinguishability

Let A and B be two distribution ensambles. Give a formal proof that if A and B are statistically close, then they are computational indistinguishable.

Cryptographic definition and provable security

In class we formally defined a bit commitment scheme. Give a formal definition of string commitment scheme, and associated security properties. Then, show how to build a string commitment scheme out of a bit commitment scheme, and prove that your construction is secure.

Hardness amplification

Let f be a function that is moderately hard to invert, i.e., any probabilitic polynomial (in n) time adversary succeeds in inverting f on a random input (of length n) with probability at most 1/2. (You may assume f is a length preserving permutation.) Prove that the function

$$g(x_1; \ldots; x_n) = f(x_1); f(x_2); \ldots; f(x_n)$$

(i.e., the function that takes an input of length n^2, breaks it into n pieces of length n, and apply f to each piece) is very hard to invert. How hard?

Number theory

Let p be a prime congruent to 3 modulo 4. Given an efficien (polynomial time) algorithm that on input an integer x, computes another integer y such that $y^2 = x \pmod{p}$, or reports that no solution exists.