Computer Science and Engineering, UCSD
CSE 207: Modern Cryptography
Problem Set 6

Fall 09
Instructor: Mihir Bellare
November 2, 2009

Problem Set 6

Due: Monday November 9, 2009, in class.

Collaboration is allowed on this problem set. See the course information sheet for more information and details about rules.

Problem 1. [25 points] Let $G = \langle g \rangle$ be a cyclic group of order m, and let $k = \lceil \log_2(m) \rceil$. The group G as well as g, m, k are public and known quantities. Suppose you are given a (possibly randomized) algorithm B such that $\mathbf{Adv}^{\mathrm{dl}}_{G,g}(B) \geq 1/2$. You are also given a positive integer s. Design an algorithm A that uses B as a subroutine to achieve $\mathbf{Adv}^{\mathrm{dl}}_{G,g}(A) \geq 1 - 2^{-s}$. The running time T_A of A should be $sT_B + \mathcal{O}(skT_G)$ where T_B is the running time of B and T_G is the time to do a group operation. The big-oh hides a small constant.

Problem 2. [25 points] Let $G = \langle g \rangle$ be a cyclic group of order m. Let $k = \lceil \log_2(m) \rceil$ and let w be a positive integer dividing k. The group G as well as g, m, k, w are public and known quantities. An *exponentiation with pre-processing scheme* is a pair (P, E) of algorithms. The first takes no inputs and outputs a table T. The second takes input T and any $x \in \mathbf{Z}_m$ and outputs g^x. Design such a scheme so that T consists of at most $(k/w)2^w$ group elements and E uses at most k/w group operations.