Problem Set 5

Due: Wednesday March 4, 2009, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

Problem 1. [40 points] Consider the following computational problem:

INPUT: N, a, b, x, y where $N \geq 1$ is an integer, $a, b \in \mathbf{Z}_N^*$ and x, y are integers with $0 \leq x, y < N$

OUTPUT: $a^x b^y \bmod N$

Let $k = |N|$. The naive algorithm for this first computes $a^x \bmod N$, then computes $b^y \bmod N$, and multiplies them modulo N. This has a worst case cost of $4k + 1$ multiplications modulo N. Design an alternative, faster algorithm for this problem that uses at most $2k + 1$ multiplications modulo N.
