

## Homework 5

Lecturer: Sasha Boldyreva

Due: October 29, 2009

**Problem 5.1** Carefully read and understand Chapter Computational Number Theory from the lecture notes.

**Problem 5.2, 15 points.**

Consider the batch-exponentiation problem that on inputs a  $k$ -bit integer  $N$ ,  $a_1, a_2, \dots, a_l \in \mathbb{Z}_N^*$  and  $b_1, b_2, \dots, b_l \in \mathbb{Z}_{N-1}$  returns  $a_1^{b_1} \cdot a_2^{b_2} \cdot \dots \cdot a_l^{b_l} \bmod N$ .

The naive algorithm for this problem uses  $2lk + l - 1$  multiplications modulo  $N$ . design a new algorithm that uses  $2k + 2^l - l - 1$  multiplications modulo  $N$ . This would often be more efficient, when  $l \geq 2$  but not too large, but  $k$  is large, that is typically the case in cryptography.

**Problem 5.3, 10 points.**

Let  $p, q$  be relatively prime. Prove that  $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$ .

**Problem 5.3, 15 points.**

Let  $N$  be a product of two distinct primes, i.e.  $N = p \cdot q$ . Show that if  $N$  and  $\phi(N)$  are known then, it is possible to compute  $p$  and  $q$  in polynomial time (in the length of  $N$ ).