

## Homework 6

Lecturer: Sasha Boldyreva

Due: November 5, 2009

**Problem 6.1, 20 points.**

Let  $G$  be a cyclic group of known order with a generator  $g$  such that the DDH problem is hard for  $G, g$ . Prove that for the associated ElGamal encryption scheme is IND-CPA secure against adversaries that make only *one* query to the LR encryption oracle. (The standard IND-CPA security will follow from the theorem we state in class.)

**Problem 6.2, 20 points.** Assume there exists a polynomial-time algorithm  $A$  that given an RSA public key  $(N, e)$  can invert 1% of all ciphertexts  $C \in \mathbb{Z}_N^*$ . That is, given  $(N, e)$  and  $C = M^e \bmod N$  it can efficiently compute  $M$  if  $C$  happens to be in a “weak” 1% fraction of all ciphertexts.

Show that then there exists an algorithm that given  $(N, e)$  inverts *every* ciphertext  $C \in \mathbb{Z}_N^*$  with probability more than  $1/2$ , and is *usually* efficient (runs in expected polynomial time).

**Hint.** Use the multiplicative property of RSA: for every public key  $(N, e)$  and  $M_1, M_2 \in \mathbb{Z}_N^*$ ,  $M_1^e \cdot M_2^e = (M_1 \cdot M_2)^e \pmod{N}$ .