

Homework 2

Lecturer: Sasha Boldyreva

Due: September 10, 2009

Recommended reading is relevant parts from the symmetric encryption chapter from the lecture notes of Bellare and Rogaway.

Problem 2.1, 20 points. Assume you have an encryption scheme $SE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. Using this scheme construct a new encryption scheme SE' such that

- (a) SE' is IND-CPA if SE is IND-CPA;
- (b) SE' is not IND-CCA even if SE is IND-CCA.

Specify the algorithms of your scheme. Make sure that your scheme is correct (you don't have to write the justification for that). You have to prove each claim.