

Homework 1

Lecturer: Sasha Boldyreva

Due: August 27, 2009

Recommended reading is Chapter 1 from the lecture notes of Bellare and Rogaway and the first set of slides.

Assignment 1.0 To be done individually. Read all the information and rules on the course's web page.

Problem 1.1, 20 points. Prove that an encryption scheme is perfectly secure if and only if it is Shannon-secure. Your proof has to be formal and consist of two parts, each proving one direction ("if" and "only if" directions).

Below I recall some basic clarifications to the notation in the slides and facts you can use in your solution.

For every M , $PD(M)$ stands for the probability that a message is M taken over the the random choice of a message. I.e.

$$PD(M) = \Pr_m [m = M] .$$

For every M, C

$\Pr_K [\text{message is } M \mid \text{ciphertext is } C]$ stands for $\Pr_{K,m} [m = M \mid \mathcal{E}_K(m) = C]$.

$$\Pr_{K,m} [\mathcal{E}(K, m) = C] = \sum_M \Pr_m [m = M] \cdot \Pr_K [\mathcal{E}(K, M) = C] .$$

Problem 1.2, 10 points. Problem 1.3 from the lecture notes of Bellare and Rogaway..