

Homework 4

Lecturer: Sasha Boldyreva

Due: October 1, 2009

Problem 4.1, 10 points.

Prove that the matrix construction we studied in class is a universal function family.

Problem 4.2, 10 points.

Problem 6.1 from the lecture notes of Bellare and Rogaway (for those who downloaded the older version of the notes). In the updated version posted now it's Problem 1 in Section 7.9. The problem asks you to break a modification to CBC-MAC we discussed in class, where the message length is appended to the message before the MAC is applied.

Problem 4.3, 7 points.

Prove Theorem 2 from the slides on Authenticated Encryption. It states that MtE is not always IND-CCA.

Problem 4.3, 5 points.

Find blockcipher-based constructions of secure MACs for messages of variable length (of length mn , where n is the block size and n is arbitrary integer greater than 1. Just give the names and references where the descriptions can be found.