HW1 (Due 09/21 In Class)

HW1 should be handed in on Thursday 21 during the class.

1 Problem 1

In class, we prove CTR is secure in the sense of IND$. Write a pseudo-code for CTR with arbitrary input length (messages not necessarily a multiple of blocksize). Prove the mode of operation is secure (meeting the IND$ security).

2 Problem 2

In Chapter 4 of Bellare and Rogaway's notes, they defined the traditional IND security. Is IND$ strictly stronger than IND? If yes, construct a scheme that is secure in the sense of IND but not in the sense of IND$? If no, are they equivalent? Or IND is stronger?

3 Problem 3

Let $F : K \times X \to Y$ be a secure PRF, where $K = X = Y = \{0, 1\}^n$. Prove that $F'(k, (m_1, m_2)) := F(k, m_1) \oplus F(k, m_2)$ is insecure.

4 Problem 4

Prove that if h_1 and h_2 are both collision resistant hashing then so is $H(x) := h_1(h_2(x))$.