CS 171: Problem Set 3

Due Date: February 13th, 2024 at 8:59pm via Gradescope

1. Pseudorandom Functions

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF). For the functions f' below, either prove that f' is a PRF (for all choices of f), or prove that f' is not a PRF.

(a) $f'_k(x) := f_k(0||x)||f_k(1||x)$.

(b) $f'_k(x) := f_k(0||x)||f_k(x||1)$.

Solution TODO ■

2. Weak CPA Security

Consider a weaker definition of CPA security where in the indistinguishability experiment the adversary $\mathcal{A}$ is not given oracle access to $\mathsf{Enc}_k(\cdot)$ after choosing m_0, m_1. That is, $\mathcal{A}$ can only query $\mathsf{Enc}_k(\cdot)$ in phase 1, but not in phase 2. We call this definition weak-CPA-security. Prove that weak-CPA-security is equivalent to CPA-security (i.e., Definition 3.22 in the textbook).

Hint: Begin by showing via a hybrid argument that any $\mathcal{A}$ interacting in the usual CPA game cannot distinguish whether its phase 2 queries are answered honestly (that is, if the response to the query m is $\mathsf{Enc}_k(m)$ or an encryption of 0; $\mathsf{Enc}_k(0)$ – something unrelated to m).

Solution TODO ■

3. Modes of operations are not CCA-Secure

Show that the CBC and CTR modes of encryption are not CCA-secure.

Solution TODO ■