CS 171: Discussion Section 4 (2/12)

1 Pseudorandom Functions

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. For each of the candidates below prove whether it is pseudorandom or not.

1. $f'_k(x) = f_k(x) \parallel f_k(\overline{x})$ where $\overline{x}$ flips all the bits of x.
2. $f'_{(k_1,k_2)}(x) = f_{k_1}(x) \parallel f_{k_2}(x)$.

2 Psuedorandom Permutations

Assume that pseudorandom permutations exist. Show that there exists a function that is a pseudorandom permutation but not a *strong* pseudorandom permutation.