ENEE/CMSC/MATH 456: Cryptography
PRF Class Exercise 2/20/19

Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

1. $F'_k(x) \coloneqq F_k(0||x)||F_k(x||1)$.

2. $F'_k(x) \coloneqq F_k(0||x)||F_k(1||x)$.