ENEE 457: Computer Systems Security
PRF Class Exercise

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

1. a) How many functions are there from $\{0,1\}^n \rightarrow \{0,1\}^n$?

   b) How many *permutations* are there from $\{0,1\}^n \rightarrow \{0,1\}^n$?

   c) What is the expected number of bits needed to describe a random function f?

   d) What is the expected number of bits needed to describe a random permutation f?

   e) Let F be a length-preserving pseudorandom function, $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$. Assuming the description of F is public, how many bits are needed to represent a function F_k?

2. Consider a keyed function $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$.

   a) If F has the property that for all k, x, y: $F_k(x \oplus y) = F_k(x) \oplus F_k(y)$, can F be a pseudorandom function? Justify your answer.

   b) If F has the property that for k, ℓ, x: $F_{k \oplus \ell}(x) = F_k(x) \oplus F_\ell(x)$, can F be a pseudorandom function? Assume the above relation holds for any k and x and some particular value of ℓ. Justify your answer.