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 $\{0,1\}^n \rightarrow \{0,1\}^n$?
   
   Truth table has $2^n$ number of rows. For each row there are $2^n$ number of choices. So the total number is $(2^n)^{2^n} = 2^{n*2^n}$.

b) How many permutations are there from $\{0,1\}^n \rightarrow \{0,1\}^n$?
   
   Truth table has $2^n$ rows. For row i there are $(2^n - i + 1)$ choices.
   
   So the total number of choices is $2^n * (2^n-1) * (2^n-2)... = (2^n)!$

c) What is the expected number of bits needed to describe a random function $f$?
   
   $\log_2(2^{n*2^n}) = n*2^n$.

d) What is the expected number of bits needed to describe a random permutation $f$?
   
   $\log_2 ((2^n)!)$.

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.

   No. Because given $x, y \neq 0$ and $F_k(x)$ and $F_k(y)$, we can predict the value of $F_k(x \oplus y) = F_k(x) \oplus F_k(y)$. Whereas for a (pseudo) random function, knowing the value of the function on 2 points should give no information about its value at a third distinct point.

   b) If $F$ has the property that for all $k, \ell, x$:
   
   $F_{k \oplus \ell}(x) = F_k(x) \oplus F_\ell(x)$,

   can $F$ be a pseudorandom function? Justify your answer.

   Yes, this is possible. In the security game the attacker *only* gets access to $F$ with a particular secret key $k$. Therefore, the attacker would not be able to obtain the values $F_k(x)$ and $F_{\ell}(x)$ in a security game with secret key $k \oplus \ell$. (It would only be able to obtain the values $F_{(k \oplus \ell)}(x)$ and $F_{(k')} (x)$ for known $k'$.)