Pseudo Random Functions

It does not make much sense to say that any fixed function is pseudorandom. We refer to pseudorandomness of a distribution on functions. An easy way to do this is to consider keyed functions.

A keyed function F is a two-input function **F : {0, 1}* x {0, 1}* → {0, 1}***, where the first input is called the key and denoted k, and the second input is just called the input. In general, the key k will be chosen and then fixed, and we will then be interested in the (single-input) function **F_k : {0, 1}* → {0, 1}***. For simplicity, we will assume that F is length preserving so that the key, input, and output lengths of F are all the same; i.e., we assume that the function F is only defined when the key k and the input x have the same length, in which case $|F_k(x)| = |x| = |k|$. By fixing key k, we obtain a function F mapping n-bit strings to n-bit strings. We say F is efficient if there is a deterministic polynomial-time algorithm that computes F(k, x) given k and x as input.

A keyed function F induces a natural distribution on functions given by choosing a random key $k \leftarrow \{0, 1\}^n$ and then considering the resulting single-input function F_k. Intuitively, we call F_k pseudorandom if the function (for randomly-chosen key k) is indistinguishable from a function chosen uniformly at random from the set of all functions having the same domain and range; that is, if no polynomial-time adversary can distinguish whether it is interacting with F_k (for randomly-chosen key k) or f (where f is chosen at random from the set of all functions mapping n-bit strings to n-bit strings). We wish to construct a keyed function F such that F_k (for $k \leftarrow \{0, 1\}^n$ chosen uniformly at random is indistinguishable from f_n (for $f_n \leftarrow Func_n$ chosen uniformly at random).