Pseudorandom functions:

A pseudorandom function is a deterministic function of a key and an input that is indistinguishable from a truly random function of the input. More precisely, let s be a security parameter, let k be a key of length s bits, and let $f(k,x)$ be a function on keys k and inputs x. Then f is a pseudorandom function if:

- f can be computed in polynomial time in s; and
- if k is random, then f cannot be distinguished from a random function in polynomial time.

In this context, "distinguishability" refers to the ability of an algorithm to tell whether a function is not truly random.

PRF from PRG:

Let G be a pseudorandom generator with expansion factor $l(n) = 2n$ .Denote the first half of the output of G as $G_0(k)$,and the other half output as $G_1(k)$. For every k∈ $\{0,1\}^n$ define the function $F_k: \{0,1\}^n \to \{0,1\}^n$ as

$$F_k(x_1x_2x_3 \dots \dots x_n) = G_{x_n}\left(\dots G_{x_2}\left(G_{x_1}(k)\right)\right)$$