Let G be a PRG with,

$$G : \{0,1\}^n \to \{0,1\}^{2n}$$ now, define

G_0, G_1 as the left and right halves of G respectively. i.e,

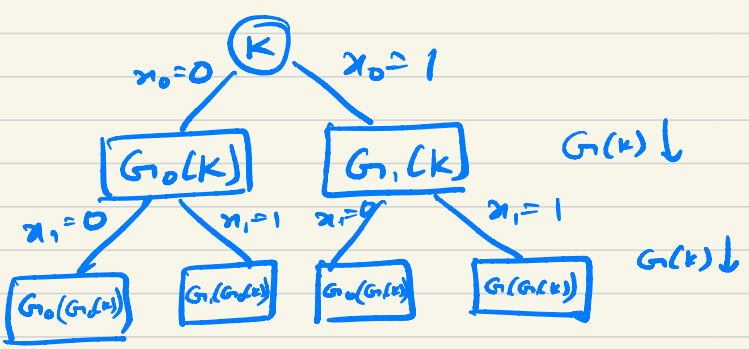
$$G(x) = G_0(x) \| G_1(x)$$

Now, for any key $k \in \{0,1\}^n$, any seed $x \in \{0,1\}^n$. $F_k : \{0,1\}^n \to \{0,1\}^n$ is the PRF such that,

$$F_k(x) = F_k(x_1, x_2, \cdots x_n)$$

$$= G_{x_n}(G_{x_{n-1}}(\cdots(G_{x_2}(G_{x_1}(k)))\cdots))$$

Visualisation



→ By applying the construction for the first time we get "$G_{n_0}(k)$". It is an output from PRG we can say that it cannot be distinguished from truly random function, due to the property of PRG's, which doesn't allow adversary to distinguish between a truly random sequence and pseudo random sequence.

→ let's again apply construction to get "$G_{n_1}(G_{n_0}(k))$" as the output. This is secure because it was generated by a PRG with $G_{n_0}(k)$ as input, hence it will indistinguishable from an output from a truly random function.

→ The n^{th} layer of the output cannot be distinguished from a truly random sequence because n^{th} layer output is generated by PRG G with output of $(n-1)^{th}$ layer as its input. Now due to this, output from this PRF cannot be distinguished from the output from a truly random function, ∴ it is secure.