Pseudo-Random Function

PRF is a function that maps from $\{0,1\}^n \to \{0,1\}^n$ parameterized by another input $\{0,1\}^n$. This function is randomly chosen from the 2^{n2^n} functions possible.

Thus effectively it maps from $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

For a function to be pseudo-random, there must exist no polynomial time distinguisher D st

$$\left| Pr\left(D^{F_k(\cdot)}(1^n) = 1\right) - Pr\left(D^{f(\cdot)}(1^n) = 1\right) \right| \le negl(n)$$

where k is the key & f is a uniformly randomly chosen function.

Construction -

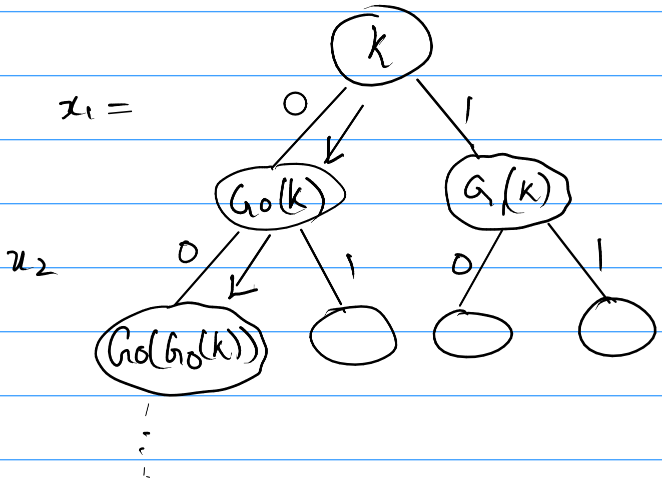
If G is PRG which takes n bits & outputs $2n$ bits. $G_0(k)$ is the left half of G's output & $G_1(k)$ is the right half.

Then the following definition of PRF is valid -

$F_k : \{0,1\}^n \to \{0,1\}^n$

$F(x_1 \ldots x_n) = G_{x_n}(\cdots G_{x_2}(G_{x_1}(k)))$

This construction can be visualized by -


k
$x_1 =$
0
1
$G_0(k)$
$G_1(k)$
x_2
0
1
0
1
$G_0(G_0(k))$