Build a provably secure PRF from PRG

To construct PRF from PRG :
Let G be a pseudorandom generator with expansion factor l(n) = 2n. Denote by $G_0(k)$ the first half of G's output, and by $G_1(k)$ the second half of G's output. For every k belonging to $\{0,1)^n$, define the function $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$ as :

$$F_k(x_1,x_2,...x_n) = G_{x\_n}(...(G_{x\_2}(G_{x\_1}(k)))...)$$

If G is a pseudorandom generator with expansion factor l(n) = 2n, then the above method gives a pseudorandom function.

The PRF function uses a PRG to create a PRF. 'r' is an integer whose binary representation decides which half of the random number acts as the new seed. The seed is an integer which is the initial seed to the PRG.
It returns an integer whose binary representation corresponds to a PRF.

The code has been explained in the comments present in the script wherever necessary.