

Pseudo random function code explanation :

- For PRF we need two inputs k,x which are having same length
- First step is scanning these inputs and then we will pass these to PRF() function
- Based on bit in x ,if it is 0 then we calculate PRG on first half key otherwise second half of key and at the end we return the key

```
def PRF(k,x): #key and tree number Fk(x)

    for i in x: # for every bit in x make a tree
        g=PRG(k)
        n=len(g)
        if i==0: #g0
            k=g[:int(n/2)]
        else:    #g1
            k=g[int(n/2):]
    return k
```