*Function* PRF

This is the pseudo random function implemented using pseudo-random generator (PRG)

*Input Arguments*

K – key, a binary string

X – a binary string

*Output*

Binary string

*Logic*

For each bit in the X

If the bit is 0, first half of the output of prg is taken as input for next iteration

Else if bit is 1, next half is considered and flows the above logic

*Usage*

PRF is more random than PRG, hence it is used in all further implementations