2021201041
NVSS Maneesh Gupta

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, later half is considered and is taken as input for next iteration

Usage

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