PRF-Documentation

This class implements the PRF

init:

Params:
p: prime number
n: bit length of this prime number

generate:

Params:
x: the variable denoting the key in the PRF
y: the variable denoting the random initialisation vector

Returns:
Randomised n bit long vector

Iteratively passes the first half or the second half of the previous iteration to the pseudo-random generator according to the corresponding bit being 0 or 1 respectively.