Pseudo Random Function

Input: A key k of length seed_size, message m of arbitrary length.

Output: A random bit sequence of size equal to input seed length.

Algorithm:

For each bit i in input seed:

Compute the Pseudo Random Generation of key

If i is 0: consider the first the half of the above output as new key

Else : consider the first the half of the above output as new key

End-For

Return key