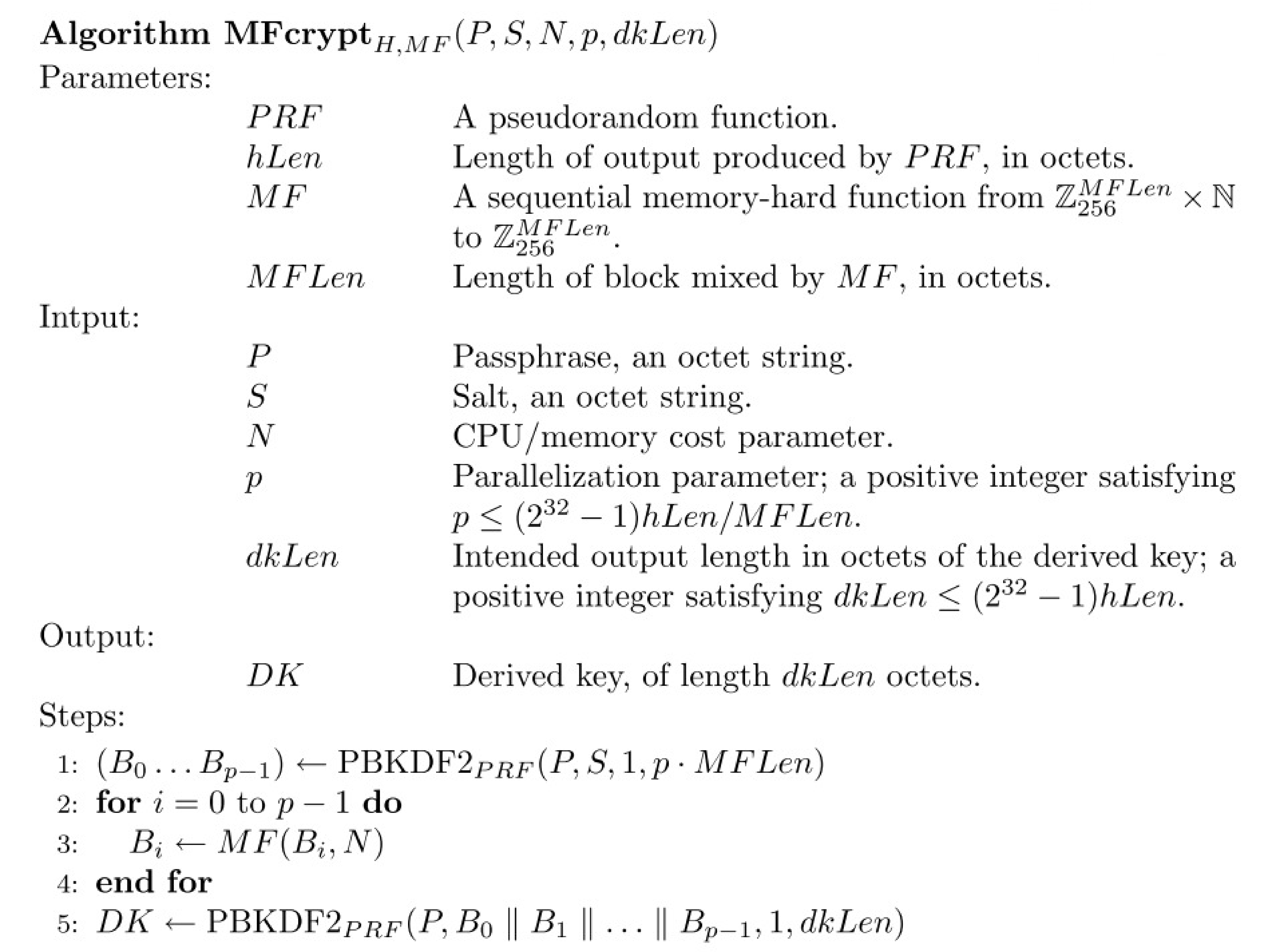

Algorithm MFcrypt$_{H,MF}(P, S, N, p, dkLen)$

Parameters:

PRF	A pseudorandom function.
$hLen$	Length of output produced by PRF, in octets.
MF	A sequential memory-hard function from $\mathbb{Z}_{256}^{MFLen} \times \mathbb{N}$ to $\mathbb{Z}_{256}^{MFLen}$.
$MFLen$	Length of block mixed by MF, in octets.

Intput:

P	Passphrase, an octet string.
S	Salt, an octet string.
N	CPU/memory cost parameter.
p	Parallelization parameter; a positive integer satisfying $p \leq (2^{32} - 1)hLen/MFLen$.
$dkLen$	Intended output length in octets of the derived key; a positive integer satisfying $dkLen \leq (2^{32} - 1)hLen$.

Output:

DK	Derived key, of length $dkLen$ octets.

Steps:

```
$(B_0 \ldots B_{p-1}) \leftarrow \mathrm{PBKDF2}_{PRF}(P, S, 1, p \cdot MFLen)$
**for** $i = 0$ to $p - 1$ **do**
    $B_i \leftarrow MF(B_i, N)$
**end for**
$DK \leftarrow \mathrm{PBKDF2}_{PRF}(P, B_0 \parallel B_1 \parallel \ldots \parallel B_{p-1}, 1, dkLen)$
```