

PseudoCode:

Break input into blocks of 16 bytes.

Start with $hash = 0$

For each block:

$temp = hash$

 if $hash$ is greater than 0:

$hash = (hash * block) \% 2^{128}$

 else:

$hash = block \% 2^{128}$

$hash = hash$ (shifted 10 bits left) AND $2^{128} - 1$

$hash = hash$ XOR $temp$

return $hash$