

Pseudocode:

Break input into blocks of 16 bytes.

Start with $hash = 0$

For each block:

$a = hash$

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

$hash = hash XOR a$

return $hash$