

HOTP values:

Example 1:

K = 0x123456789abcdef0123456789abcdef0

C = 2023

HS = 3564b2c92bc61706c1c552aefd0596ff04f75581

String[19] = 81 = (1000 0001) (hexadecimal)

Low-order 4 bits is: 0001 (1) (decimal)

Offset = 1

P = String[1]String[2]String[3]String[4]

P = 64b2c92b

Return the last 31 bits:

leading term: 6 = (0110), return 6

Return: result = 64b2c92b (This is base 16)

Convert to base 10:

result = 1689438507 (base 10)

final_result = result (mod 10⁶)

final_result = 438507

Example 2:

K = 0x123456789abcdef0123456789abcdef0

C = 2024

HS = 613fb3e414c5ec96516a61435059721049d6b229

String[19] = 29 = (0010 1001) (hexadecimal)

Low-order 4 bits is: 1001 (9) (decimal)

Offset = 9

P = String[9]String[10]String[11]String[12]

P = 6a614350 (this is base 16)

Return the last 31 bits:

leading term: $6 = (0110)$, return 6

Return: $\text{result} = 6a614350$ (this is base 16)

Convert to base 10:

$\text{result} = 1784759120$ (base 10)

$\text{final_result} = \text{result} \pmod{10^6}$

$\text{final_result} = 759120$