Plir 256 Hashing Algorithm

Prima Agus Setiawan a.k.a joeheartless

January 31, 2025

1 Bitwise Rotation

Bitwise left rotation of a value x by n bits within a b-bit word:

$$\text{rotate\_left}(x, n, b) = (x \ll n) \mod 2^b \mid (x \gg (b - n)) \tag{1}$$

2 Modular Mixing Function

A modular arithmetic-based mixing function for diffusion enhancement:

$$\text{modular\_mix}(x, y) = ((x \times 31) + (y \times 17) + \text{rotate\_left}(x, 7) + \text{rotate\_left}(y, 11)) \mod 2^{32} \tag{2}$$

3 Deterministic Message Expansion

Given an input string T of length L, the expansion function generates blocks:

$$B_i = \text{unpack}_{\text{LE}}(T[i : i + 4]) \oplus (S \gg (i \mod 16)) \tag{3}$$

where the seed S is initialized as:

$$S = \sum_{i=1}^{L} \text{ord}(T_i) \times 137 \tag{4}$$

and updated iteratively as:

$$S = \text{rotate\_left}(S, 5) \oplus (S \times 71) \tag{5}$$

4 Hash Function Iterations

For N rounds and M stages, the hashing function is defined as:

$$h_i = h_{i-1} \oplus (K \oplus \text{modular\_mix}(h_{i-1}, M_i)) \mod 2^{32} \tag{6}$$

where:

$$K = C_G \oplus (i \times 73) \oplus \big(h_{(i \mod 8)} \ll (i \mod 6)\big) \oplus \big(h_{(i+3) \mod 8} \gg (i \mod 4)\big) \oplus \big(h_{(i+5) \mod 8} \ll (i \mod 8 \tag{7}$$

and C_G is the golden ratio constant:

$$C_G = 0x9E3779B9 \tag{8}$$

5 Final Hash Output

After M stages, the final hash output is:

$$H = \sum_{i=0}^{7} h_i \mod 2^{256} \tag{9}$$