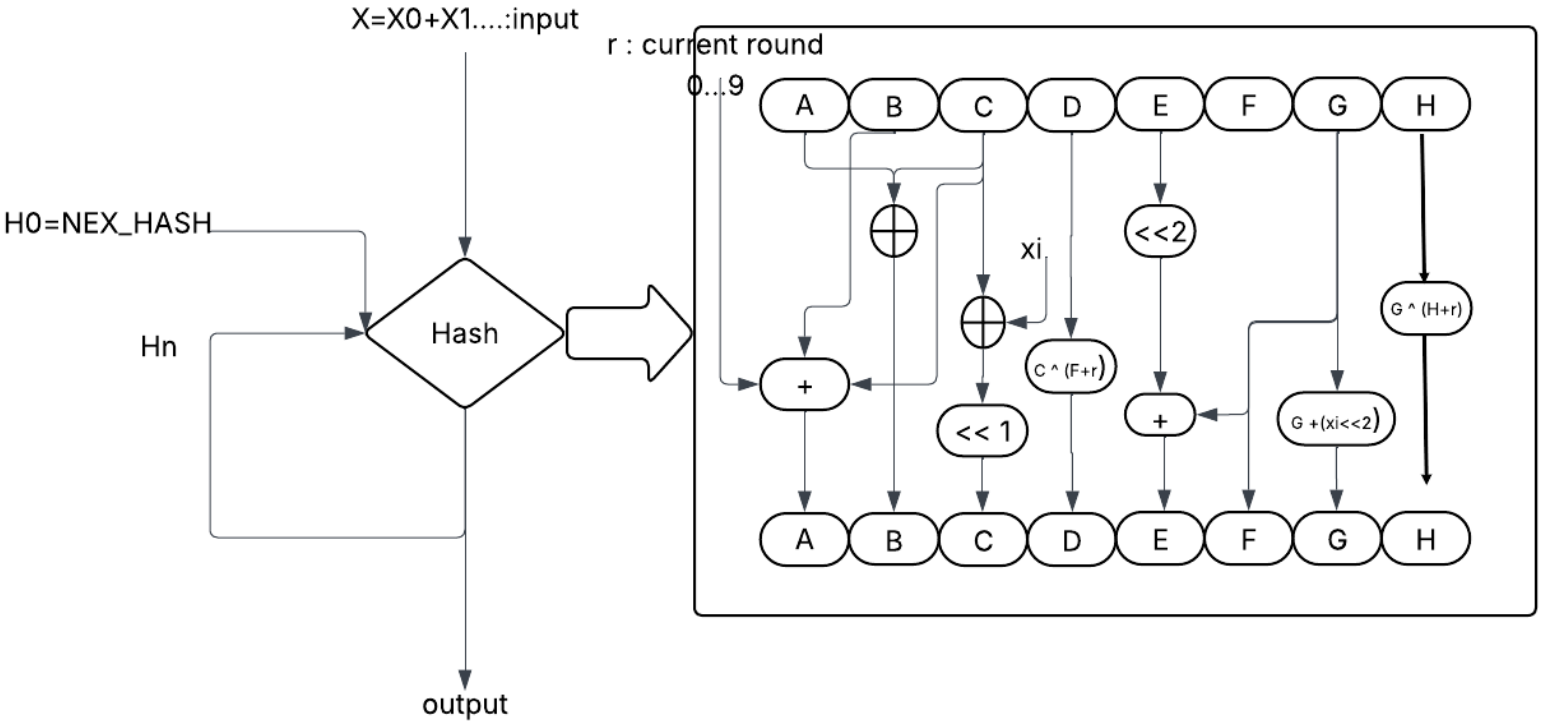
NEX_HASH Hash Function

- NEX_HASH processes an arbitrary length message and produces a (8 bytes) 64bit output.
- x denotes a sequence of bytes (unsigned characters means from 0x00 to 0xff) x0, x1, …, xn. These characters are are processed sequentially by the H function which
  - consists of 10 rounds, each which perform identical operations from 0 to 9
  - takes a byte (an unsigned character) in xi and the output of the previous round and generates a sequence of 8 bytes denoted as A, B, C, D, E, F ,G ,H
- The hash digest is then defined as an out of the last iteration of the H function
  - H0 is the initial seed value. Let Ho = {'N','E','X','_','H','A','S','H'}
  - Hi+1 = H(Hi, xi) for i = 0, 1, …, n-1 , n the is the length of the string

- Internal Structure of the H function:
  - << and >> are the bitwise shift left and right operations respectively
  - & is a bitwise AND operator
  - ^ is a bitwise XOR operator Final Hash is then converted to hex for each byte in the digest



● The Password hash we need to crack is : f903467a43c75b9f

Flagformat : nexus{password}