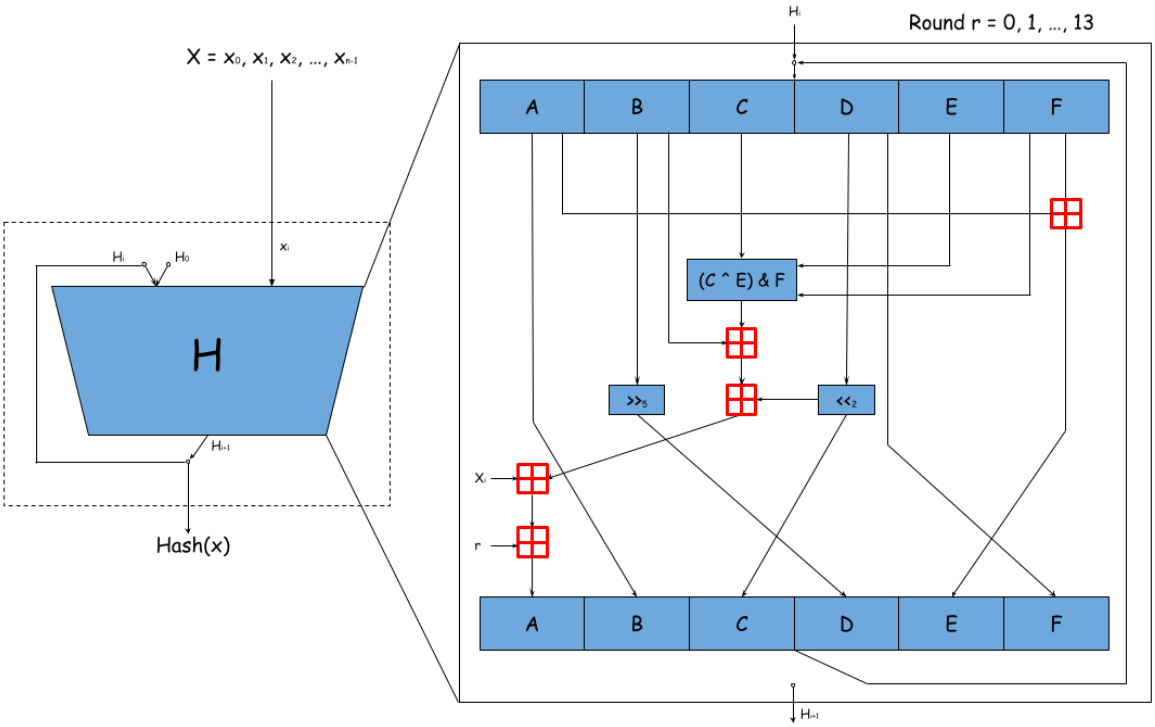
RITSEC HASH



- RITSEC HASH processes an arbitrary length message and produces a 48-bit output.
- x denotes a sequence of bytes (unsigned characters) x_0, x_1, …, x_n. These characters are are processed sequentially by the H function which
  - consists of 13 rounds, each which perform identical operations
  - takes a byte (an unsigned character) in x_i and the output of the previous round and generates a sequence of 6 bytes denoted as A, B, C, D, E, and F

- The hash digest is then defined as an out of the last iteration of the H function
  - H_0 is the initial seed value. Let H_o = {‘R’, ‘I’, ‘T’, ‘S’, ‘E’, ‘C’}
  - $H_{i+1} = H(H_i, x_i)$ for i = 0, 1, …, n-1

- Internal Structure of the H function:
  - Each of A, B, C, D, E, and F represent a single byte (unsigned char)
  - << 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

Hash check:

“RITSEC_CTF_2021” → 3ba50807aa02