

512-bits  $\rightarrow$  SHA-256  $\rightarrow$  256 bits in Hex

## Steps

1) Convert msg into binary

Hello world  $\rightarrow$  01100111111101

2) Pre processing

$\rightarrow$  After msg append 1 & all other zero till whole data become ~~512-bit~~ 448 bits

    Hello world      one append  
    ↓  
11010110011111110000000 - - - 0  
    ← 448-bits

message + 1 + zeros      message length  
    ← 448 bits      ← 64-bits

3) In message length ~~can't~~<sup>put</sup> length of original msg

ex Hello world = 10 character \* 8 bits = 80 bits

so in

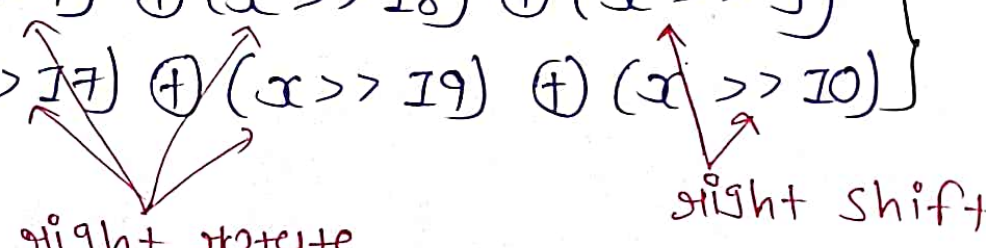
    Append zeros      80  
    ←      ←  
0 .... 00001010000  
    ← 64-bits

4) slice 512-bits into 32-bit length block  
 means there will be 16 blocks  
 having 32-bits length.

5) Pre-processing

$$W_t = \begin{cases} m_z & 0 \leq t \leq 15 \\ \sigma_1(W[t-2]) + W[t-7] + \sigma_0(W[t-15]) + W[t-16] & 16 \leq t \leq 63 \end{cases}$$

$$\left. \begin{aligned} \sigma_0(x) &= (x \gg 7) \oplus (x \gg 18) \oplus (x \gg 3) \\ \sigma_1(x) &= (x \gg 17) \oplus (x \gg 19) \oplus (x \gg 10) \end{aligned} \right\} 16 \leq x \leq 63$$


  
 right rotate                      right shift

$$W_t = \sigma_1(W_t - 2) + W_t - 7 + \sigma_0(W_t - 15) + W_t - 16 \quad \text{for } 16 \leq t \leq 63$$

6) initialize hash value  $H_0 - H_7$  & give name like

$$\begin{aligned} a &= H_0 \\ b &= H_1 \\ &\vdots \\ h &= H_7 \end{aligned}$$

7) For each round  $t = 0$  to  $63$

$$T_1 = h + \Sigma_1(e) + ch(e, f, g) + K_t + W_t$$

$$T_2 = \Sigma_0(a) + maj(a, b, c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + T_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = T_1 + T_2$$

where

$$\begin{aligned} \Sigma_0(x) &= (x \gg 2) \oplus (x \gg 13) \oplus (x \gg 22) \\ \Sigma_1(x) &= (x \gg 6) \oplus (x \gg 11) \oplus (x \gg 25) \end{aligned} \quad \left. \begin{array}{l} \gg \\ \text{means} \\ \text{rotate} \end{array} \right\}$$

$$Ch(x, y, z) = (x \wedge y) \oplus (\sim x \wedge z)$$

$$maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

8) Add with initial value

$$H[0] = (H[0] + a)$$

$$H[1] = (H[1] + b)$$

$\vdots$

$$H[7] = (H[7] + h)$$