512-bits → $\boxed{\text{SHA-256}}$ → 256 bits in Hex

Steps

1) Convert msg into binary

Hello world → 01100 1 ... 01

2) Pre processing

→ After msg append 1 & all other zero till whole data become ~~512-bits~~ 448 bits

Hello world one append

↓

1101011001111 1000000 ... 0

~~512-bit~~ 448-bits

message + 1 + zeros message length

448 bits 64-bits

3) In message length ~~count~~ put length of original msg

Ex Hello world = 10 character * 8 bits = 80 bits

so in Append zeros 80

0 00001010000

64-bits

YASH SIDDHAPURA

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

5) Pre-processing

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

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

right rotate

right shift

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

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

$a = H_0$
$b = H_1$
$\vdots$
$h = H_7$

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

$$\Sigma_0(x) = (x >> 2) \oplus (x >> 13) \oplus (x >> 22)$$
$$\Sigma_1(x) = (x >> 6) \oplus (x >> 11) \oplus (x >> 25)$$

>> means rotate

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

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

8) Add with initial value

$$H[0] = (H[0] + a)$$
$$H[1] = (H[1] + b)$$
$$\vdots$$
$$H[7] = H[7] + h)$$