SHA-512

$$\begin{aligned} Maj(x,y,z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \\ Ch(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \end{aligned}$$

$$\begin{aligned} RotR^n(x) &= \text{rotate (circular shift) bits } n \text{ positions to the right} \\ ShiftR^n(x) &= \text{shift bits } n \text{ positions to the right} \end{aligned}$$

$$\begin{aligned} \Sigma_0(x) &= RotR^{28}(x) \oplus RotR^{34}(x) \oplus RotR^{39}(x) \\ \Sigma_1(x) &= RotR^{14}(x) \oplus RotR^{18}(x) \oplus RotR^{41}(x) \\ \sigma_0(x) &= RotR^{1}(x) \;\; \oplus RotR^{8}(x) \;\; \oplus ShiftR^{7}(x) \\ \sigma_1(x) &= RotR^{19}(x) \oplus RotR^{61}(x) \oplus ShiftR^{6}(x) \end{aligned}$$

1 Words

The first 16 words are 64-bit sections of the message block. The rest of the words are derived from those original 16.

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

2 Compression function

$$\begin{aligned} tmp_1 &= h + \Sigma_1(e) + Ch(e,f,g) + K[i] + W[i] \\ tmp_2 &= \Sigma_0(a) + Maj(a,b,c) \\ h &= g \\ g &= f \\ f &= e \\ e &= d + tmp_1 \\ d &= c \\ c &= b \\ b &= a \\ a &= tmp_1 + tmp_2 \end{aligned}$$