MD5

$$RotL^n(x) = \text{rotate (circular shift) bits } n \text{ positions to the left}$$

1 Words

The 16 words are 32-bit sections of the message block.

$$0 \leq i \leq 15 \quad \begin{cases} W[i] = M[i] \end{cases}$$

2 Compression function

$$\begin{aligned} tmp &= b + RotL^{s[i \mod 4]}(a + F(b,c,d) + K[i] + W[g]) \\ a &= d \\ d &= c \\ c &= b \\ b &= tmp \end{aligned}$$

2.1 Rounds

$$0 \leq i \leq 15 \quad \begin{cases} F(b,c,d) = (b \wedge c) \vee (\neg b \wedge d) \\ g = i \\ s = \{7, 12, 17, 22\} \end{cases}$$

$$16 \leq i \leq 31 \quad \begin{cases} F(b,c,d) = (b \wedge d) \vee (c \wedge \neg d) \\ g = (5 \times i + 1) \mod 16 \\ s = \{5, 9, 14, 20\} \end{cases}$$

$$32 \leq i \leq 47 \quad \begin{cases} F(b,c,d) = b \oplus c \oplus d \\ g = (3 \times i + 5) \mod 16 \\ s = \{4, 11, 16, 23\} \end{cases}$$

$$48 \leq i \leq 63 \quad \begin{cases} F(b,c,d) = c \oplus (b \vee \neg d) \\ g = (7 \times i) \mod 16 \\ s = \{6, 10, 15, 21\} \end{cases}$$