SHA-1

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

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

1 Words

The first 16 words are 32-bit sections of the message block. The rest of the words are derived from those original 16.

$$
W[i] = \begin{cases} 0 \leq i \leq 15 & M[i] \\ 16 \leq i \leq 79 & RotL^1(W[i-3] \oplus W[i-8] \oplus W[i-14] \oplus W[i-16]) \end{cases}
$$

2 Compression function

$$
\begin{aligned}
tmp &= RotL^5(a) + F(b, c, d) + W[i] + K + e \\
e &= d \\
d &= c \\
c &= RotL^{30}(b) \\
b &= a \\
a &= tmp
\end{aligned}
$$

2.1 Rounds

$$
\begin{aligned}
0 \leq i \leq 19 \quad & \begin{cases} F(b,c,d) = Ch(b,c,d) \\ K = \text{0x5A827999} \end{cases} \\
20 \leq i \leq 39 \quad & \begin{cases} F(b,c,d) = Par(b,c,d) \\ K = \text{0x6ED9EBA1} \end{cases} \\
40 \leq i \leq 59 \quad & \begin{cases} F(b,c,d) = Maj(b,c,d) \\ K = \text{0x8F1BBCDC} \end{cases} \\
60 \leq i \leq 79 \quad & \begin{cases} F(b,c,d) = Par(b,c,d) \\ K = \text{0xCA62C1D6} \end{cases}
\end{aligned}
$$