MODULE *sha*256

EXTENDS *Integers*, *Sequences*, *TLC*, *Reals*

VARIABLES A, B, C, D, E, F, G, H, *digest*, *Message*, $S0$, $S1$

$A0 \triangleq 13$
$B0 \triangleq 17$
$C0 \triangleq 19$
$D0 \triangleq 23$
$E0 \triangleq 29$
$F0 \triangleq 13$
$G0 \triangleq 17$
$H0 \triangleq 19$

$Divide(x,\ y) \triangleq x \div y$

$ModAdd(x,\ y) \triangleq ((x + y)\%(2^8))$ Updated to 32-bit for $SHA - 256$
$ModSub(x,\ y) \triangleq ((x - y)\%(2^8))$
$ModMul(x,\ y) \triangleq ((x * y)\%(2^8))$

$Xor(x,\ y) \triangleq ModSub(ModAdd(x,\ y),\ ModMul(2,\ ModMul(x,\ y)))$

$RightRotate(x,\ c) \triangleq ModAdd(((x \div (2^c))\%(2^8)),\ ((x * (2^{(32-c)}))\%(2^8)))$

$Ch(x,\ y,\ z) \triangleq (x \wedge y) \vee ((\neg x) \wedge z)$
$Maj(x,\ y,\ z) \triangleq (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$
$Sigma0(x) \triangleq Xor(Xor(RightRotate(x,\ 2),\ RightRotate(x,\ 13)),\ RightRotate(x,\ 22))$
$Sigma1(x) \triangleq Xor(Xor(RightRotate(x,\ 6),\ RightRotate(x,\ 11)),\ RightRotate(x,\ 25))$
$s0(x) \triangleq Xor(Xor(RightRotate(x,\ 7),\ RightRotate(x,\ 18)),\ (x \div (2^3)))$
$s1(x) \triangleq Xor(Xor(RightRotate(x,\ 17),\ RightRotate(x,\ 19)),\ (x \div (2^{10})))$

$K \triangleq \langle 11,\ 19,\ 29,\ 37,\ 13,\ 23,\ 31,\ 41,$
$17,\ 7,\ 47,\ 3,\ 43,\ 5,\ 2,\ 39,$
$28,\ 16,\ 12,\ 20,\ 45,\ 21,\ 34,\ 9,$
$38,\ 25,\ 14,\ 44,\ 33,\ 6,\ 24,\ 27,$
$30,\ 48,\ 35,\ 32,\ 49,\ 22,\ 36,\ 18,$
$26,\ 40,\ 15,\ 42,\ 8,\ 4,\ 46,\ 50,$
$1,\ 10,\ 13,\ 19,\ 7,\ 29,\ 23,\ 12,$
$17,\ 31,\ 22,\ 5,\ 6,\ 2,\ 37,\ 39\rangle$

RECURSIVE $GenerateWt(\_)$
$GenerateWt(chunk) \triangleq$
$[i \in 0\ldots 63 \mapsto$ IF $i < 16$ THEN
$SubSeq(Message,\ (chunk - 1) * 512 + i * 32 + 1,\ (chunk - 1) * 512 + (i + 1) * 32)$
ELSE
LET $W \triangleq GenerateWt(chunk)$
IN $ModAdd(ModAdd(ModAdd(s1(W[i-2]),\ W[i-7]),\ s0(W[i-15])),\ W[i-16])]$

$ProcessChunk(chunk) \triangleq$
LET
$Wt \triangleq GenerateWt(chunk)$
IN
$\land A' = A$
$\land B' = B$
$\land C' = C$
$\land D' = D$
$\land E' = E$
$\land F' = F$
$\land G' = G$
$\land H' = H$
$\land \forall i \in 0 \,..\, 63 :$
LET
$T1 \triangleq ModAdd(ModAdd(ModAdd(ModAdd(H,\ Sigma1(E)),\ Ch(E,\ F,\ G)),\ K[i]),\ Wt[i])$
$T2 \triangleq ModAdd(Sigma0(A),\ Maj(A,\ B,\ C))$
IN
$\land H' = G$
$\land G' = F$
$\land F' = E$
$\land E' = ModAdd(D,\ T1)$
$\land D' = C$
$\land C' = B$
$\land B' = A$
$\land A' = ModAdd(T1,\ T2)$
$\land$ UNCHANGED $\langle S0,\ S1,\ Message\rangle$

$Init \triangleq$
$\land A = 13$
$\land B = 17$
$\land C = 19$
$\land D = 23$
$\land E = 29$
$\land F = 13$
$\land G = 17$
$\land H = 19$
$\land S0 = 0$
$\land S1 = 0$
$\land digest = \langle\rangle$
$\land Message = \langle\rangle$

$Preprocess \triangleq$
LET $msg \triangleq Append(Message,\ 0)$
IN $\land Len(msg)\%512 = 448$
$\land Message' = Append(msg,\ Len(Message)\%(2^{64}))$

$$
\begin{array}{l}
\mathit{FinalCombine} \triangleq \\
\quad \land A' = \mathit{ModAdd}(A,\ A0) \\
\quad \land B' = \mathit{ModAdd}(B,\ B0) \\
\quad \land C' = \mathit{ModAdd}(C,\ C0) \\
\quad \land D' = \mathit{ModAdd}(D,\ D0) \\
\quad \land E' = \mathit{ModAdd}(E,\ E0) \\
\quad \land F' = \mathit{ModAdd}(F,\ F0) \\
\quad \land G' = \mathit{ModAdd}(G,\ G0) \\
\quad \land H' = \mathit{ModAdd}(H,\ H0) \\
\quad \land \mathit{digest}' = \langle A',\ B',\ C',\ D',\ E',\ F',\ G',\ H' \rangle \\
\quad \land \text{UNCHANGED } \langle S0,\ S1,\ \mathit{Message} \rangle
\end{array}
$$

$$
\begin{array}{l}
\mathit{Next} \triangleq \\
\quad \lor \mathit{Preprocess} \\
\quad \lor \exists\, \mathit{chunk} \in 1 \mathinner{..} \mathit{Divide}(\mathit{Len}(\mathit{Message}),\ 512) : \mathit{ProcessChunk}(\mathit{chunk}) \\
\quad \lor \mathit{FinalCombine}
\end{array}
$$

$$
\begin{array}{l}
\mathit{Spec} \triangleq \\
\quad \land \mathit{Init} \\
\quad \land \Box[\mathit{Next}]_{\langle A,\, B,\, C,\, D,\, E,\, F,\, G,\, H,\, S0,\, S1,\, \mathit{Message} \rangle}
\end{array}
$$