MODULE *sha*256

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

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

$A0 \triangleq 1779033703$
$B0 \triangleq 3144134277$
$C0 \triangleq 1013904242$
$D0 \triangleq 2773480762$
$E0 \triangleq 1359893119$
$F0 \triangleq 2600822924$
$G0 \triangleq 528734635$
$H0 \triangleq 1541459225$

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

$ModAdd(x,\ y) \triangleq ((x + y)\%(2^{32}))$
$ModSub(x,\ y) \triangleq ((x - y)\%(2^{32}))$
$ModMul(x,\ y) \triangleq ((x * y)\%(2\ ^{32}))$

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

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

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

$K \triangleq \langle 1116352408,\ 1899447441,\ 3049323471,\ 3921009573,$
$961987163,\ 1508970993,\ 2453635748,\ 2870763221,$
$3624381080,\ 310598401,\ 607225278,\ 1426881987,$
$1925078388,\ 2162078206,\ 2614888103,\ 3248222580,$
$3835390401,\ 4022224774,\ 264347078,\ 604807628,$
$770255983,\ 1249150122,\ 1555081692,\ 1996064986,$
$2554220882,\ 2821834349,\ 2952996808,\ 3210313671,$
$3336571891,\ 3584528711,\ 113926993,\ 338241895,$
$666307205,\ 773529912,\ 1294757372,\ 1396182291,$
$1695183700,\ 1986661051,\ 2177026350,\ 2456956037,$
$2730485921,\ 2820302411,\ 3259730800,\ 3345764771,$
$3516065817,\ 3600352804,\ 4094571909,\ 275423344,$
$430227734,\ 506948616,\ 659060556,\ 883997877,$
$958139571,\ 1322822218,\ 1537002063,\ 1747873779,$
$1955562222,\ 2024104815,\ 2227730452,\ 2361852424,$
$2428436474,\ 2756734187,\ 3204031479,\ 3329325298\rangle$

```
RECURSIVE GenerateWt(_)
GenerateWt(chunk) ≜
  [i ∈ 0 .. 63 ↦ IF i < 16 THEN
                   SubSeq(Message, (chunk − 1) ∗ 512 + i ∗ 32 + 1, (chunk − 1) ∗ 512 + (i + 1) ∗ 32)
                 ELSE
                   LET W ≜ GenerateWt(chunk)
                   IN  ModAdd(ModAdd(ModAdd(s1(W[i − 2]), W[i − 7]), s0(W[i − 15])), W[i − 16])]

ProcessChunk(chunk) ≜
  LET
    Wt ≜ GenerateWt(chunk)
  IN
    ∧ A′ = A
    ∧ B′ = B
    ∧ C′ = C
    ∧ D′ = D
    ∧ E′ = E
    ∧ F′ = F
    ∧ G′ = G
    ∧ H′ = H
    ∧ ∀ i ∈ 0 .. 63 :
        LET
          T1 ≜ ModAdd(ModAdd(ModAdd(ModAdd(H, Sigma1(E)), Ch(E, F, G)), K[i]), Wt[i])
          T2 ≜ ModAdd(Sigma0(A), Maj(A, B, C))
        IN
          ∧ H′ = G
          ∧ G′ = F
          ∧ F′ = E
          ∧ E′ = ModAdd(D, T1)
          ∧ D′ = C
          ∧ C′ = B
          ∧ B′ = A
          ∧ A′ = ModAdd(T1, T2)
    ∧ UNCHANGED ⟨S0, S1, Message⟩

Init ≜
    ∧ A = 1779033703
    ∧ B = 3144134277
    ∧ C = 1013904242
    ∧ D = 2773480762
    ∧ E = 1359893119
    ∧ F = 2600822924
    ∧ G = 528734635
    ∧ H = 1541459225
    ∧ S0 = 0
```

$\land\ S1 = 0$
$\land\ digest = \langle\rangle$
$\land\ Message = \langle 72,\ 101,\ 108,\ 108,\ 111\rangle$ Hello

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

$FinalCombine \triangleq$
$\land\ A' = ModAdd(A,\ A0)$
$\land\ B' = ModAdd(B,\ B0)$
$\land\ C' = ModAdd(C,\ C0)$
$\land\ D' = ModAdd(D,\ D0)$
$\land\ E' = ModAdd(E,\ E0)$
$\land\ F' = ModAdd(F,\ F0)$
$\land\ G' = ModAdd(G,\ G0)$
$\land\ H' = ModAdd(H,\ H0)$
$\land\ digest' = \langle A',\ B',\ C',\ D',\ E',\ F',\ G',\ H'\rangle$
$\land$ UNCHANGED $\langle S0,\ S1,\ Message\rangle$

$Next \triangleq$
$\lor\ Preprocess$
$\lor\ \exists\, chunk \in 1\ldots Divide(Len(Message),\ 512) : ProcessChunk(chunk)$
$\lor\ FinalCombine$

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