```
────────────────────── MODULE sha256 ──────────────────────
EXTENDS Integers, Sequences, TLC, Reals, Bitwise

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

A0 ≜ 13
B0 ≜ 17
C0 ≜ 19
D0 ≜ 23
E0 ≜ 29
F0 ≜ 13
G0 ≜ 17
H0 ≜ 19

Divide(x, y)    ≜ x ÷ y

ModAdd(x, y) ≜ ((x + y)%(2^8))
ModSub(x, y) ≜ ((x − y)%(2^8))
ModMul(x, y) ≜ ((x ∗ y)%(2 ^8))
RightRotate(x, c) ≜ shiftR(x, c) ÷ (2^(32−c))


Ch(x, y, z) ≜ (x & y) | ((Not(x)) & z)
Maj(x, y, z) ≜ (x & y) | (x & z) | (y & z)
Sigma0(x) ≜ (RightRotate(x, 2)^^RightRotate(x, 13))^^RightRotate(x, 22)
Sigma1(x) ≜ (RightRotate(x, 6)^^RightRotate(x, 11))^^RightRotate(x, 25)
s0(x) ≜ (RightRotate(x, 7)^^RightRotate(x, 18))^^(x ÷ (2^3))
s1(x) ≜ (RightRotate(x, 17)^^RightRotate(x, 19))^^(x ÷ (2^10))

K ≜ ⟨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⟩

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 = 13
    ∧ B = 17
    ∧ C = 19
    ∧ D = 23
    ∧ E = 29
    ∧ F = 13
    ∧ G = 17
    ∧ H = 19
    ∧ S0 = 0
    ∧ S1 = 0
    ∧ digest = ⟨⟩
    ∧ Message = ⟨⟩

Preprocess ≜
  LET msg ≜ Append(Message, 0)
  IN    ∧ Len(msg)%512 = 448
        ∧ Message′ = Append(msg, Len(Message)%(2^{64}))

FinalCombine ≜
    ∧ A′ = ModAdd(A, A0)
    $\land B' = ModAdd(B, B0)$
    $\land C' = ModAdd(C, C0)$
    $\land D' = ModAdd(D, D0)$
    $\land E' = ModAdd(E, E0)$
    $\land F' = ModAdd(F, F0)$
    $\land G' = ModAdd(G, G0)$
    $\land H' = ModAdd(H, H0)$
    $\land digest' = \langle A', B', C', D', E', F', G', H' \rangle$
    $\land \textsc{unchanged} \ \langle S0, S1, Message \rangle$

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

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