MODULE $md5$

EXTENDS $Integers$, $Sequences$, $FiniteSets$, $Bitwise$

VARIABLES A, B, C, D, AA, BB, CC, DD, M, K, S, $Message$, $digest$

RECURSIVE $shiftL(\_, \_)$
$shiftL(n, pos) \triangleq$
  IF $pos = 0$
  THEN n
  ELSE LET $double(z) \triangleq 2 * z$
       IN $shiftL(double(n), pos - 1)$

$LeftRotate(x, c) \triangleq (shiftL(x, c) \,|\, shiftR(x, 32 - c))\%(2^8)$

$Preprocess \triangleq$
  LET $msg \triangleq Append(Message, 0)$
  IN $\land Len(msg)\%512 = 448$
     $\land Message' = Append(msg, Len(Message)\%(2^{64}))$ Po standardu $MD5$

$ProcessChunk(chunk) \triangleq$
  LET $P \triangleq [j \in 0 \,..\, 15 \mapsto SubSeq(Message, (chunk - 1) * 512 + j * 32 + 1, (chunk - 1) * 512 + (j + 1) * 3$
  IN
    $\land AA' = A$
    $\land BB' = B$
    $\land CC' = C$
    $\land DD' = D$
    $\land \forall i \in 0 \,..\, 63 :$
      LET
        $F \triangleq$ IF $i \in 0 \,..\, 15$ THEN $(B \,\&\, C) \,|\, ((Not(B)) \,\&\, D)$
                  ELSE IF $i \in 16 \,..\, 31$ THEN $(D \,\&\, B) \,|\, ((Not(D)) \,\&\, C)$
                  ELSE IF $i \in 32 \,..\, 47$ THEN $(B \hat{} C) \hat{} D$
                  ELSE $C \hat{} (B \,|\, (Not(D)))$
        $g \triangleq$ IF $i \in 0 \,..\, 15$ THEN i
                  ELSE IF $i \in 16 \,..\, 31$ THEN $(5 * i + 1)\%16$
                  ELSE IF $i \in 32 \,..\, 47$ THEN $(3 * i + 5)\%16$
                  ELSE $(7 * i)\%16$
      IN
        $\land F' = (F + A + K[i] + P[g])\%(2^8)$ Sve operacije su modulo 2^8
        $\land A' = D$
        $\land D' = C$
        $\land C' = B$
        $\land B' = (B + LeftRotate(F', S[i]))\%(2^8)$
    $\land A' = (A + AA)\%(2^8)$
    $\land B' = (B + BB)\%(2^8)$
    $\land C' = (C + CC)\%(2^8)$
    $\land D' = (D + DD)\%(2^8)$

$FinalHash \triangleq$
$\land A' = (A + AA)\%(2^8)$
$\land B' = (B + BB)\%(2^8)$
$\land C' = (C + CC)\%(2^8)$
$\land D' = (D + DD)\%(2^8)$
$\land digest' = \langle A',\ B',\ C',\ D' \rangle$
$\land \text{UNCHANGED } \langle AA,\ BB,\ CC,\ DD,\ Message,\ M,\ K,\ S \rangle$

$Init \triangleq$
$\land A = 67$
$\land B = 31$
$\land C = 19$
$\land D = 47$
$\land K = \langle 19, 55, 50, 72, 59, 8, 66, 34,$
$\quad 29, 14, 9, 17, 19, 23, 45, 80,$
$\quad 84, 27, 77, 35, 97, 84, 25, 1,$
$\quad 96, 7, 65, 76, 43, 20, 4, 12,$
$\quad 25, 85, 95, 93, 97, 48, 22, 15,$
$\quad 67, 4, 43, 30, 41, 74, 18, 16,$
$\quad 64, 21, 57, 75, 49, 58, 18, 3,$
$\quad 20, 12, 20, 88, 4, 49, 66, 90 \rangle$
$\land S = \langle 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22,$
$\quad 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20,$
$\quad 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23,$
$\quad 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21 \rangle$
$\land AA = A$
$\land BB = B$
$\land CC = C$
$\land DD = D$
$\land Message = \langle \rangle$
$\land M = \langle \rangle$
$\land digest = \langle \rangle$

$Next \triangleq$
$\lor Preprocess$
$\lor \exists\, chunk \in 1 \,..\, (Len(Message) \div 512) : ProcessChunk(chunk)$
$\lor FinalHash$

$Spec \triangleq Init \land \Box[Next]_{\langle A,\ B,\ C,\ D,\ AA,\ BB,\ CC,\ DD,\ Message,\ M,\ digest \rangle}$