MODULE *ripemd*160

EXTENDS *Reals*, *Sequences*, *TLC*, *Reals*, *Bitwise*

VARIABLES A, B, C, D, E, AA, BB, CC, DD, EE, *digest*, *Message*

$ModAdd(x,\ y) \triangleq ((x + y)\%(2^8))$

$ModSub(x,\ y) \triangleq ((x - y)\%(2^8))$

$ModMul(x,\ y) \triangleq ((x * y)\%(2\ ^8))$

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

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

$F1A(N,\ P,\ Q) \triangleq ((P^Q)^N)$
$F2A(N,\ P,\ Q) \triangleq ((N \,\&\, P) \,|\, (\neg N \,\&\, Q))$
$F3A(N,\ P,\ Q) \triangleq ((N \,|\, \neg P)^Q)$
$F4A(N,\ P,\ Q) \triangleq ((N \,\&\, Q) \,|\, (P \,\&\, \neg Q))$
$F5A(N,\ P,\ Q) \triangleq (N^{(P \,|\, \neg Q)})$

$F1B(N,\ P,\ Q) \triangleq (P^{(N \,|\, \neg Q)})$
$F2B(N,\ P,\ Q) \triangleq ((N \,\&\, Q) \,|\, (P \,\&\, \neg Q))$
$F3B(N,\ P,\ Q) \triangleq ((N \,|\, \neg P)^Q)$
$F4B(N,\ P,\ Q) \triangleq ((N \,\&\, P) \,|\, (\neg N \,\&\, Q))$
$F5B(N,\ P,\ Q) \triangleq ((P^Q)^N)$

$K1A \triangleq 0$
$K2A \triangleq 11$
$K3A \triangleq 13$
$K4A \triangleq 17$
$K5A \triangleq 19$
$K1B \triangleq 23$
$K2B \triangleq 27$
$K3B \triangleq 31$
$K4B \triangleq 37$
$K5B \triangleq 0$

$S1A \triangleq \langle 11, 14, 15, 12, 5, 8, 7, 9, 11, 13, 14, 15, 6, 7, 9, 8\rangle$
$S2A \triangleq \langle 7, 6, 8, 13, 11, 9, 7, 15, 7, 12, 15, 9, 11, 7, 13, 12\rangle$
$S3A \triangleq \langle 11, 13, 6, 7, 14, 9, 15, 8, 2, 12, 4, 13, 6, 8, 13, 15\rangle$
$S4A \triangleq \langle 9, 13, 15, 7, 12, 8, 9, 11, 7, 7, 12, 7, 6, 15, 13, 11\rangle$
$S5A \triangleq \langle 7, 5, 13, 11, 6, 7, 9, 5, 11, 12, 6, 13, 14, 7, 12, 7\rangle$

$S1B \triangleq \langle 8, 9, 11, 13, 15, 7, 12, 8, 6, 4, 14, 15, 8, 11, 10, 7\rangle$
$S2B \triangleq \langle 9, 13, 7, 15, 8, 14, 11, 2, 7, 1, 10, 13, 12, 5, 8, 9\rangle$
$S3B \triangleq \langle 8, 12, 4, 9, 10, 0, 15, 5, 3, 14, 7, 14, 5, 6, 11, 13\rangle$
$S4B \triangleq \langle 5, 6, 11, 14, 10, 2, 4, 9, 7, 8, 15, 11, 13, 9, 3, 1\rangle$
$S5B \triangleq \langle 12, 5, 15, 13, 6, 8, 2, 10, 7, 0, 9, 14, 3, 5, 1, 6\rangle$

$F(N,\ P,\ Q,\ isA,\ num) \triangleq$
IF isA THEN
IF $num = 1$ THEN $F1A(N,\ P,\ Q)$
ELSE IF $num = 2$ THEN $F2A(N,\ P,\ Q)$
ELSE IF $num = 3$ THEN $F3A(N,\ P,\ Q)$
ELSE IF $num = 4$ THEN $F4A(N,\ P,\ Q)$
ELSE $F5A(N,\ P,\ Q)$
ELSE
IF $num = 1$ THEN $F1B(N,\ P,\ Q)$
ELSE IF $num = 2$ THEN $F2B(N,\ P,\ Q)$
ELSE IF $num = 3$ THEN $F3B(N,\ P,\ Q)$
ELSE IF $num = 4$ THEN $F4B(N,\ P,\ Q)$
ELSE $F5B(N,\ P,\ Q)$

$ProcessChunk(chunk) \triangleq$
LET
$P \triangleq [j \in 0\ldots 15 \mapsto SubSeq(Message,\ (chunk-1)*512 + j*32 + 1,\ (chunk-1)*512 + (j+1)*32)]$
IN
$\land\ AA' = A$
$\land\ BB' = B$
$\land\ CC' = C$
$\land\ DD' = D$
$\land\ EE' = E$
$\land\ \forall\, round \in 1\ldots 5 :$
LET
$K1 \triangleq$ IF $round = 1$ THEN $K1A$ ELSE IF $round = 2$ THEN $K2A$ ELSE IF $round = 3$ THEN $K3A$
$S1 \triangleq$ IF $round = 1$ THEN $S1A$ ELSE IF $round = 2$ THEN $S2A$ ELSE IF $round = 3$ THEN $S3A$
$K2 \triangleq$ IF $round = 1$ THEN $K1B$ ELSE IF $round = 2$ THEN $K2B$ ELSE IF $round = 3$ THEN $K3B$
$S2 \triangleq$ IF $round = 1$ THEN $S1B$ ELSE IF $round = 2$ THEN $S2B$ ELSE IF $round = 3$ THEN $S3B$
IN
$\land\ \forall\, i \in 1\ldots 16 :$
LET
$resultA \triangleq F(B,\ C,\ D,\ \text{TRUE},\ round)\%(2^8)$
$resultB \triangleq F(BB,\ CC,\ DD,\ \text{FALSE},\ round)\%(2^8)$
IN
$\land\ A' = LeftRotate(((E + resultA)\hat{}\hat{}K1),\ S1[i])\%(2^8)$
$\land\ E' = D\%(2^8)$
$\land\ D' = LeftRotate(C,\ 10)\%(2^8)$
$\land\ C' = B\%(2^8)$

$\land\ B' = A\%(2^8)$
$\land\ AA' = \mathit{LeftRotate}(((EE + \mathit{resultB})\hat{}\hat{}\ K2),\ S2[i])\%(2^8)$
$\land\ EE' = DD\%(2^8)$
$\land\ DD' = \mathit{LeftRotate}(CC,\ 10)\%(2^8)$
$\land\ CC' = BB\%(2^8)$
$\land\ BB' = AA\%(2^8)$
$\land$ UNCHANGED $\langle \mathit{digest},\ \mathit{Message}\rangle$

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

$\mathit{Init} \triangleq$
$\land\ A = 13$
$\land\ B = 17$
$\land\ C = 19$
$\land\ D = 23$
$\land\ E = 29$
$\land\ AA = 13$
$\land\ BB = 17$
$\land\ CC = 19$
$\land\ DD = 23$
$\land\ EE = 29$
$\land\ \mathit{digest} = \langle\rangle$
$\land\ \mathit{Message} = \langle\rangle$

$\mathit{FinalCombine} \triangleq$
$\land\ A' = \mathit{ModAdd}(A,\ AA)$
$\land\ B' = \mathit{ModAdd}(B,\ BB)$
$\land\ C' = \mathit{ModAdd}(C,\ CC)$
$\land\ D' = \mathit{ModAdd}(D,\ DD)$
$\land\ E' = \mathit{ModAdd}(E,\ EE)$
$\land\ \mathit{digest}' = \langle A',\ B',\ C',\ D',\ E'\rangle$
$\land$ UNCHANGED $\langle AA,\ BB,\ CC,\ DD,\ EE,\ \mathit{Message}\rangle$

$\mathit{Next} \triangleq$
$\lor\ \mathit{Preprocess}$
$\lor\ \exists\ \mathit{chunk} \in 1\ldots(\mathit{Len}(\mathit{Message}) \div 512) : \mathit{ProcessChunk}(\mathit{chunk})$
$\lor\ \mathit{FinalCombine}$

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