MODULE $md5$

EXTENDS *Integers*, *Sequences*, *FiniteSets*

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

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

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

Generisanje generičkih nizova K *i* S

$GenK(n) \triangleq [i \in 0\,..\,(n-1) \mapsto (i * 123456789)\%987654321]$
$GenS(n) \triangleq [i \in 0\,..\,(n-1) \mapsto (i\%4) * 5 + 7]$

Preprocesiranje poruke

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

Obrada svake deonice poruke

$ProcessChunk(chunk) \triangleq$
  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 $(B \land C) \lor ((\neg B) \land D)$
                  ELSE IF $i \in 16\,..\,31$ THEN $(D \land B) \lor ((\neg D) \land C)$
                  ELSE IF $i \in 32\,..\,47$ THEN $((B^C)^D)$
                  ELSE $C^{(B \lor (\neg D))}$
        $g \triangleq$ 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
        $\land\ F' = F + A + K[i] + P[g]$
        $\land\ A' = D$
        $\land\ D' = C$
        $\land\ C' = B$
        $\land\ B' = B + LeftRotate(F',\ S[i])$
    $\land\ A' = A + AA$
    $\land\ B' = B + BB$
    $\land\ C' = C + CC$
    $\land\ D' = D + DD$

Finalni hash

$$FinalHash \triangleq$$
$$\land\ digest' = \langle A,\ B,\ C,\ D\rangle$$
$$\land\ \text{UNCHANGED}\ \langle A,\ B,\ C,\ D,\ AA,\ BB,\ CC,\ DD,\ Message,\ M,\ K,\ S\rangle$$

Inicijalno stanje

$$Init \triangleq$$
$$\land\ A \in 0\,..\,18$$
$$\land\ B \in 0\,..\,18$$
$$\land\ C \in 0\,..\,18$$
$$\land\ D \in 0\,..\,18$$
$$\land\ K = GenK(18)$$
$$\land\ S = GenS(18)$$
$$\land\ AA = A$$
$$\land\ BB = B$$
$$\land\ CC = C$$
$$\land\ DD = D$$
$$\land\ Message = \langle\rangle$$
$$\land\ M = \langle\rangle$$
$$\land\ digest = \langle\rangle$$

Sledeće stanje sistema

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

Specifikacija

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