MODULE *hmac*

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

VARIABLES *message*, *key*, *sentHash*, *processedHash*, *equalityCheck*, *A*, *B*, *C*, *D*, *AA*, *BB*, *CC*, *DD*, *M*, *K*

$Prime \triangleq \{x \in 2 \,..\, 12 : \forall\, y \in 2 \,..\, (x-1) : x\%y \neq 0\}$

$BLOCK\_SIZE \triangleq 64$

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

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

$MD5(m) \triangleq$
LET
ProcessChunk$(chunk) \triangleq$
LET $P \triangleq [j \in 0 \,..\, 15 \mapsto SubSeq(m,\, (chunk-1) * 512 + j * 32 + 1,\, (chunk-1) * 512 + (j +$
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
$\land\, F' = F + A + K[i] + P[g]$
$\land\, A' = D$
$\land\, D' = C$
$\land\, C' = B$
$\land\, B' = B + LeftRotate(F',\, S[i])$
$\land\, A' = A + AA$
$\land\, B' = B + BB$
$\land\, C' = C + CC$
$\land\, D' = D + DD$
digest $\triangleq \langle A,\, B,\, C,\, D \rangle$
IN
digest

$ExtendedKey \triangleq$ IF $Len(key) > BLOCK\_SIZE$ THEN $MD5(key)$ ELSE $Append(key, \langle 0 \rangle^{(BLOCK\_SIZE - Len}$

$ipad \triangleq [i \in 1 \,..\, Len(ExtendedKey) \mapsto ExtendedKey[i]^{54}]$
$opad \triangleq [i \in 1 \,..\, Len(ExtendedKey) \mapsto ExtendedKey[i]^{92}]$

$HashFunction(m, k) \triangleq$
LET
$innerHash \triangleq MD5(ipad \circ m)$
$resultHash \triangleq MD5(opad \circ innerHash)$
IN
$resultHash$

$SendHash \triangleq$
$\land\ sentHash' = HashFunction(message, ExtendedKey)$
$\land$ UNCHANGED $\langle message, key, processedHash, equalityCheck, A, B, C, D, AA, BB, CC, DD, K, S, M$

$ProcessHash \triangleq$
$\land\ processedHash' = HashFunction(message, ExtendedKey)$
$\land$ UNCHANGED $\langle message, key, sentHash, equalityCheck, A, B, C, D, AA, BB, CC, DD, K, S, M \rangle$

$CompareHashes \triangleq$
$\land\ equalityCheck' = (sentHash = processedHash)$
$\land$ UNCHANGED $\langle message, key, sentHash, processedHash, A, B, C, D, AA, BB, CC, DD, K, S, M \rangle$

$Init \triangleq$
$\land\ message = GenS(18)$
$\land\ key = GenK(18)$
$\land\ sentHash = \langle\rangle$
$\land\ processedHash = \langle\rangle$
$\land\ equalityCheck = $ FALSE
$\land\ A \in Prime$
$\land\ B \in Prime$
$\land\ C \in Prime$
$\land\ D \in Prime$
$\land\ K = GenK(18)$
$\land\ S = GenS(18)$
$\land\ AA = A$
$\land\ BB = B$
$\land\ CC = C$
$\land\ DD = D$
$\land\ M = \langle\rangle$

$Next \triangleq$
$\lor\ SendHash$
$\lor\ ProcessHash$
$\lor\ CompareHashes$

$$Spec \triangleq Init \wedge \Box[Next]_{\langle message,\, key,\, sentHash,\, processedHash,\, equalityCheck,\, A,\, B,\, C,\, D,\, AA,\, BB,\, CC,\, DD,\, M,\, K,\, S\rangle}$$