MODULE *aes*

EXTENDS *Naturals*, *Sequences*, *Integers*

VARIABLES *state*, *roundKey*, *round*, *Nb*, *Nk*, *Nr*

$SBox \triangleq [i \in 1 \,..\, 4 \mapsto [j \in 1 \,..\, 4 \mapsto ((i * j) + 50)\%256]]$

$SubBytes(s) \triangleq$
  $[i \in 1 \,..\, Nb \mapsto [j \in 1 \,..\, Nk \mapsto$
    $SBox[(s[i][j]\%4) + 1][(s[i][j]\%4) + 1]]]$

$ShiftRows(s) \triangleq$
  $[i \in 1 \,..\, Nb \mapsto$
    IF $i = 1$ THEN $s[i]$
     ELSE $[j \in 1 \,..\, Nk \mapsto s[i][((j + i - 2)\%Nk) + 1]]]$

$Multiply(a,\, b) \triangleq$
  LET $result \triangleq$ IF $b = 1$ THEN a ELSE IF $b = 2$ THEN $(a * 2)\%256$ ELSE $(a * 3)\%256$
  IN $result$

$MixColumns(s) \triangleq$
  $[i \in 1 \,..\, Nk \mapsto$
    LET $s0 \triangleq s[1][i]$
        $s1 \triangleq s[2][i]$
        $s2 \triangleq s[3][i]$
        $s3 \triangleq s[4][i]$
    IN $[j \in 1 \,..\, Nb \mapsto$
        IF $j = 1$ THEN $(Multiply(s0,\, 2) + Multiply(s1,\, 3) + s2 + s3)\%256$
         ELSE IF $j = 2$ THEN $(s0 + Multiply(s1,\, 2) + Multiply(s2,\, 3) + s3)\%256$
         ELSE IF $j = 3$ THEN $(s0 + s1 + Multiply(s2,\, 2) + Multiply(s3,\, 3))\%256$
         ELSE $(Multiply(s0,\, 3) + s1 + s2 + Multiply(s3,\, 2))\%256]]$

$AddRoundKey(s,\, k) \triangleq$
  $[i \in 1 \,..\, Nb \mapsto [j \in 1 \,..\, Nk \mapsto (s[i][j] + k[i][j])\%256]]$

$Round(s,\, k) \triangleq$
  LET $newState \triangleq MixColumns(ShiftRows(SubBytes(s)))$
  IN $AddRoundKey(newState,\, k)$

$NextRound \triangleq$
  $\land\ round < Nr$
  $\land\ state' = Round(state,\, roundKey)$
  $\land\ roundKey' = roundKey$
  $\land\ Nb' = Nb$
  $\land\ Nk' = Nk$
  $\land\ Nr' = Nr$
  $\land\ round' = round + 1$

$$
\begin{array}{l}
\mathit{Init} \triangleq \\
\quad \land \mathit{state} = [i \in 1 \,..\, 4 \mapsto [j \in 1 \,..\, 4 \mapsto (i-1) * 4 + j]] \\
\quad \land \mathit{roundKey} = [i \in 1 \,..\, 4 \mapsto [j \in 1 \,..\, 4 \mapsto (i + j + 40)\%256]] \\
\quad \land \mathit{round} = 0 \\
\quad \land \mathit{Nb} = 4 \\
\quad \land \mathit{Nk} = 4 \\
\quad \land \mathit{Nr} = 10
\end{array}
$$

$$
\begin{array}{l}
\mathit{Spec} \triangleq \\
\quad \mathit{Init} \land \Box[\mathit{NextRound}]_{\langle \mathit{state},\, \mathit{round},\, \mathit{roundKey},\, \mathit{Nb},\, \mathit{Nk},\, \mathit{Nr} \rangle}
\end{array}
$$