MODULE *aes*

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

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

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

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

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

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

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

$MixColumns(s) \triangleq$
  $[i \in 1 \,..\, Nk \mapsto$
    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 $(Multiply(s0,\ 3) + s1 + s2 + Multiply(s3,\ 2))\%256]]$

$InvMixColumns(s) \triangleq$
  $[i \in 1 \,..\, Nk \mapsto$
    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 $(Multiply(s0,\ 14) + Multiply(s1,\ 11) + Multiply(s2,\ 13) + Multiply(s3,\ 9))\%256$
         ELSE IF $j = 2$ THEN $(Multiply(s0,\ 9) + Multiply(s1,\ 14) + Multiply(s2,\ 11) + Multiply(s3,\ 13$
         ELSE IF $j = 3$ THEN $(Multiply(s0,\ 13) + Multiply(s1,\ 9) + Multiply(s2,\ 14) + Multiply(s3,\ 11$

$$\text{ELSE}\ \ (\mathit{Multiply}(s0,\,11) + s1 + s2 + \mathit{Multiply}(s3,\,14))\%256]]$$

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

$$\mathit{Round}(s,\,k) \triangleq$$
$$\text{LET}\ \mathit{newState} \triangleq \mathit{MixColumns}(\mathit{ShiftRows}(\mathit{SubBytes}(s)))$$
$$\text{IN}\quad \mathit{AddRoundKey}(\mathit{newState},\,k)$$
$$\mathit{InvRound}(s,\,k) \triangleq$$
$$\text{LET}\quad \mathit{newState} \triangleq \mathit{SubBytes}(\mathit{InvShiftRows}(\mathit{InvMixColumns}(s)))$$
$$\text{IN}\quad \mathit{AddRoundKey}(\mathit{newState},\,k)$$

$$\mathit{AESProcess}(e,\,s,\,k) \triangleq$$
$$\text{IF}\ e\ \text{THEN}\ \mathit{Round}(s,\,k)$$
$$\text{ELSE}\ \ \mathit{InvRound}(s,\,k)$$

$$\mathit{NextRound} \triangleq$$
$$\land\ \mathit{round} < Nr$$
$$\land\ \mathit{state}' = \mathit{AESProcess}(\mathit{encrypt},\,\mathit{state},\,\mathit{roundKey})$$
$$\land\ \mathit{roundKey}' = \mathit{roundKey}$$
$$\land\ Nb' = Nb$$
$$\land\ Nk' = Nk$$
$$\land\ Nr' = Nr$$
$$\land\ \mathit{round}' = \mathit{round} + 1$$
$$\land\ \mathit{encrypt}' = \mathit{encrypt}$$

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

$$\mathit{Spec} \triangleq$$
$$\mathit{Init} \land \Box[\mathit{NextRound}]_{\langle \mathit{state},\,\mathit{round},\,\mathit{roundKey},\,Nb,\,Nk,\,Nr,\,\mathit{encrypt}\rangle}$$