

EXTENDS *Naturals, Sequences, Integers*

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

$SBox \triangleq \langle$   
 $\langle 99, 124, 119, 123, 242, 107, 111, 197, 48, 1, 103, 43, 254, 215, 171, 118 \rangle,$   
 $\langle 202, 130, 201, 125, 250, 89, 71, 240, 173, 212, 162, 175, 156, 164, 114, 192 \rangle,$   
 $\langle 183, 253, 147, 38, 54, 63, 247, 204, 52, 165, 229, 241, 113, 216, 49, 21 \rangle,$   
 $\langle 4, 199, 35, 195, 24, 150, 5, 154, 7, 18, 128, 226, 235, 39, 178, 117 \rangle,$   
 $\langle 9, 131, 44, 26, 27, 110, 90, 160, 82, 59, 214, 179, 41, 227, 47, 132 \rangle,$   
 $\langle 83, 209, 0, 237, 32, 252, 177, 91, 106, 203, 190, 57, 74, 76, 88, 207 \rangle,$   
 $\langle 208, 239, 170, 251, 67, 77, 51, 133, 69, 249, 2, 127, 80, 60, 159, 168 \rangle,$   
 $\langle 81, 163, 64, 143, 146, 157, 56, 245, 188, 182, 218, 33, 16, 255, 243, 210 \rangle,$   
 $\langle 205, 12, 19, 236, 95, 151, 68, 23, 196, 167, 126, 61, 100, 93, 25, 115 \rangle,$   
 $\langle 96, 129, 79, 220, 34, 42, 144, 136, 70, 238, 184, 20, 222, 94, 11, 219 \rangle,$   
 $\langle 224, 50, 58, 10, 73, 6, 36, 92, 194, 211, 172, 98, 145, 149, 228, 121 \rangle,$   
 $\langle 231, 200, 55, 109, 141, 213, 78, 169, 108, 86, 244, 234, 101, 122, 174, 8 \rangle,$   
 $\langle 186, 120, 37, 46, 28, 166, 180, 198, 232, 221, 116, 31, 75, 189, 139, 138 \rangle,$   
 $\langle 112, 62, 181, 102, 72, 3, 246, 14, 97, 53, 87, 185, 134, 193, 29, 158 \rangle,$   
 $\langle 225, 248, 152, 17, 105, 217, 142, 148, 155, 30, 135, 233, 206, 85, 40, 223 \rangle,$   
 $\langle 140, 161, 137, 13, 191, 230, 66, 104, 65, 153, 45, 15, 176, 84, 187, 22 \rangle$   
 $\rangle$

$Rcon \triangleq \langle 1, 2, 4, 8, 16, 32, 64, 128, 27, 54 \rangle$

$Xor(a, b) \triangleq (((a + b) \% 256) - ((2 * ((a * b) \% 256)) \% 256)) \% 256$

$RotWord(word) \triangleq \langle word[2], word[3], word[4], word[1] \rangle$

$SubWord(word) \triangleq \langle SBox[(word[1] \% 16) + 1][(word[1] \% 16) + 1],$   
 $SBox[(word[2] \% 16) + 1][(word[2] \% 16) + 1],$   
 $SBox[(word[3] \% 16) + 1][(word[3] \% 16) + 1],$   
 $SBox[(word[4] \% 16) + 1][(word[4] \% 16) + 1] \rangle$

RECURSIVE  $KeyExpansion(-, -)$

$KeyExpansion(initialKey, i) \triangleq$

IF  $i \leq 4$  THEN  $\langle initialKey[1][i], initialKey[2][i], initialKey[3][i], initialKey[4][i] \rangle$

ELSE IF  $i \% 4 = 1$  THEN

LET  $prevKey \triangleq KeyExpansion(initialKey, i - 4)$

$temp \triangleq KeyExpansion(initialKey, i - 1)$

$rconVal \triangleq \langle Rcon[(i \div 4)], 0, 0, 0 \rangle$

$subRotWord \triangleq SubWord(RotWord(temp))$

IN  $[j \in 1 .. 4 \mapsto Xor(prevKey[j], Xor(subRotWord[j], rconVal[j]))]$

ELSE

LET  $prevKey \triangleq KeyExpansion(initialKey, i - 4)$

$temp \triangleq KeyExpansion(initialKey, i - 1)$

IN  $[j \in 1 \dots 4 \mapsto \text{Xor}(\text{prevKey}[j], \text{temp}[j])]$

RECURSIVE  $\text{GFMul}(-, -)$

$\text{GFMul}(a, b) \triangleq$

LET  $\text{temp} \triangleq$  IF  $b = 1$  THEN  $a$

ELSE IF  $b = 2$  THEN IF  $(a * 2) \geq 256$  THEN  $\text{Xor}((a * 2) \% 256, 27)$  ELSE  $(a * 2)$

ELSE IF  $b = 3$  THEN  $\text{Xor}(\text{GFMul}(a, 2), a)$

ELSE IF  $b = 9$  THEN  $\text{Xor}(\text{GFMul}(\text{GFMul}(\text{GFMul}(a, 2), 2), 2), a)$

ELSE IF  $b = 11$  THEN  $\text{Xor}(\text{Xor}(\text{GFMul}(\text{GFMul}(\text{GFMul}(a, 2), 2), 2), \text{GFMul}(a, 2)), a)$

ELSE IF  $b = 13$  THEN  $\text{Xor}(\text{Xor}(\text{GFMul}(\text{GFMul}(\text{GFMul}(a, 2), 2), 2), \text{GFMul}(\text{GFMul}(a, 2), 2)), \text{GFMul}(a, 2))$

ELSE IF  $b = 14$  THEN  $\text{Xor}(\text{GFMul}(\text{GFMul}(\text{GFMul}(a, 2), 2), 2), \text{GFMul}(\text{GFMul}(a, 2), 2))$

ELSE 0

IN  $\text{temp}$

$\text{SubBytes}(s) \triangleq$

$[i \in 1 \dots Nb \mapsto [j \in 1 \dots Nk \mapsto \text{SBox}[(s[i][j] \% 16) + 1][(s[i][j] \% 16) + 1]]]$

$\text{ShiftRows}(s) \triangleq$

$[i \in 1 \dots Nb \mapsto$

IF  $i = 1$  THEN  $s[i]$

ELSE  $[j \in 1 \dots Nk \mapsto s[i][((j + i - 2) \% Nk) + 1]]]$

$\text{InvShiftRows}(s) \triangleq$

$[i \in 1 \dots Nb \mapsto$

IF  $i = 1$  THEN  $s[i]$

ELSE  $[j \in 1 \dots Nk \mapsto s[i][((j - i + Nk) \% Nk) + 1]]]$

$\text{MixColumns}(s) \triangleq$

$[i \in 1 \dots Nk \mapsto$

LET  $s0 \triangleq s[1][i]$

$s1 \triangleq s[2][i]$

$s2 \triangleq s[3][i]$

$s3 \triangleq s[4][i]$

IN  $[j \in 1 \dots Nb \mapsto$

IF  $j = 1$  THEN  $\text{Xor}(\text{Xor}(\text{Xor}(\text{GFMul}(s0, 2), \text{GFMul}(s1, 3)), s2), s3) \% 256$

ELSE IF  $j = 2$  THEN  $\text{Xor}(\text{Xor}(\text{Xor}(s0, \text{GFMul}(s1, 2)), \text{GFMul}(s2, 3)), s3) \% 256$

ELSE IF  $j = 3$  THEN  $\text{Xor}(\text{Xor}(\text{Xor}(s0, s1), \text{GFMul}(s2, 2)), \text{GFMul}(s3, 3)) \% 256$

ELSE  $\text{Xor}(\text{Xor}(\text{Xor}(\text{GFMul}(s0, 3), s1), s2), \text{GFMul}(s3, 2)) \% 256]$

$\text{InvMixColumns}(s) \triangleq$

$[i \in 1 \dots Nk \mapsto$

LET  $s0 \triangleq s[1][i]$

$s1 \triangleq s[2][i]$

$s2 \triangleq s[3][i]$

$s3 \triangleq s[4][i]$

```

IN  [j ∈ 1 .. Nb ↦
    IF j = 1 THEN Xor(Xor(Xor(GFMul(s0, 14), GFMul(s1, 11)), GFMul(s2, 13)), GFMul(s3, 9),
    ELSE IF j = 2 THEN Xor(Xor(Xor(GFMul(s0, 9), GFMul(s1, 14)), GFMul(s2, 11)), GFMul(s3, 13),
    ELSE IF j = 3 THEN Xor(Xor(Xor(GFMul(s0, 13), GFMul(s1, 9)), GFMul(s2, 14)), GFMul(s3, 11),
    ELSE Xor(Xor(Xor(GFMul(s0, 11), s1), s2), GFMul(s3, 14))%256]]

AddRoundKey(s, k) ≜
  [i ∈ 1 .. Nb ↦ [j ∈ 1 .. Nk ↦ Xor(s[i][j], k[i][j])]

Round(s, k) ≜
  LET newState ≜ MixColumns(ShiftRows(SubBytes(s)))
  IN AddRoundKey(newState, k)

InvRound(s, k) ≜
  LET newState ≜ SubBytes(InvShiftRows(InvMixColumns(s)))
  IN AddRoundKey(newState, k)

AESProcess(e, s, k) ≜
  IF e THEN Round(s, k)
  ELSE InvRound(s, k)

NextRound ≜
  ∧ round < Nr
  ∧ state' = AESProcess(encrypt, state, roundKey)
  ∧ roundKey' = roundKey
  ∧ Nb' = Nb
  ∧ Nk' = Nk
  ∧ Nr' = Nr
  ∧ round' = round + 1
  ∧ encrypt' = encrypt

Init ≜
  ∧ state = [i ∈ 1 .. 4 ↦ [j ∈ 1 .. 4 ↦ (i - 1) * 4 + j]]
  ∧ round = 0
  ∧ Nb = 4
  ∧ Nk = 4
  ∧ Nr = 10
  ∧ encrypt = FALSE
  ∧ roundKey = [i ∈ 1 .. (4 * (Nr + 1)) ↦ KeyExpansion([k ∈ 1 .. 4 ↦ (k + j + 40)%256]]

Spec ≜
  Init ∧ □[NextRound]⟨state, round, roundKey, Nb, Nk, Nr, encrypt⟩

```

---