AES Documentation

Submitted by: Nada Ihab Ahmed Mohamed Abd El-Gawad

Submitted to: Prof. Ayman Wahba | Eng. Ahmed Allam

GP-2019/2020

Cairo, Egypt

Table of contents

AES Top Module

Inputs:

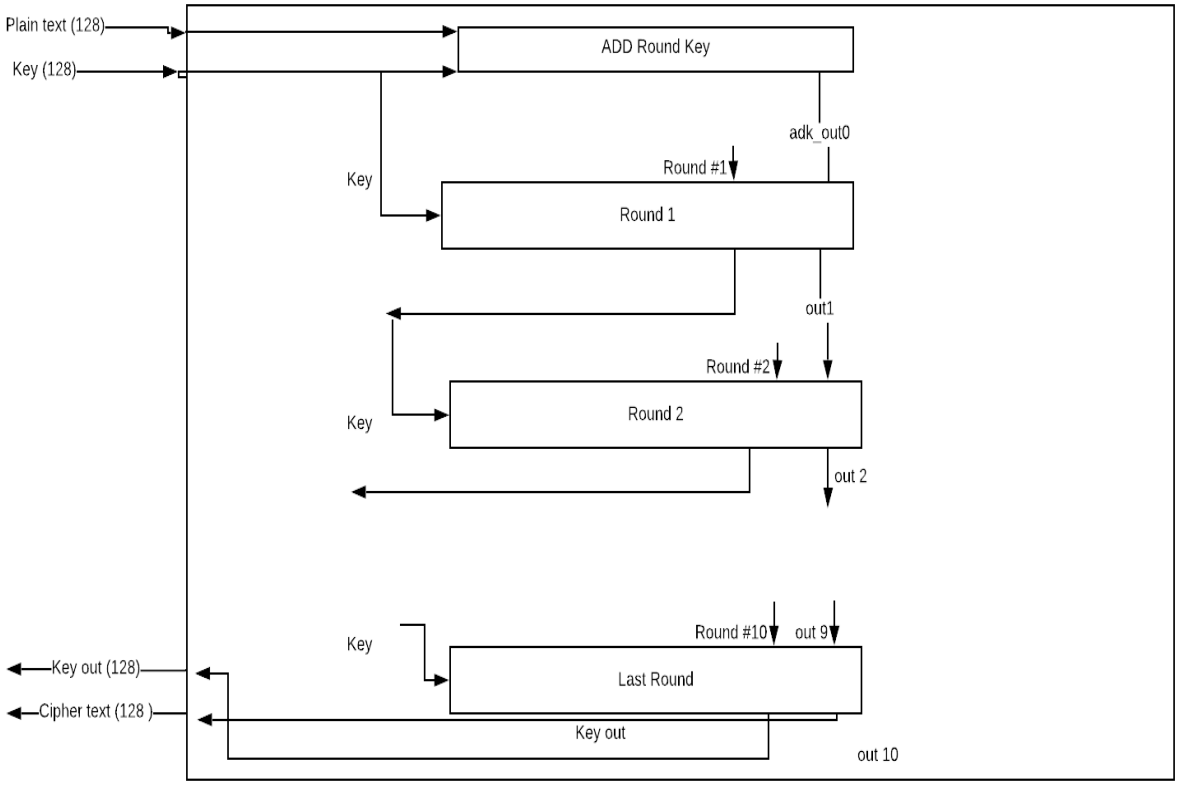
1. Plain text -128 bit wire- (which is sometimes referred to as State)
2. Key -128 bit wire-

Outputs:

1. Cipher text -128 bit register-
2. keyout -128 bit- the final key that have passed by all the shifts (used for testing in AES decryption)

Description:

- AES Top Module consists of an initial ADD Round Key, 9 similar rounds and a last round
- The output of each round (state and keyout) is the input of the next round



AES Round

Inputs:

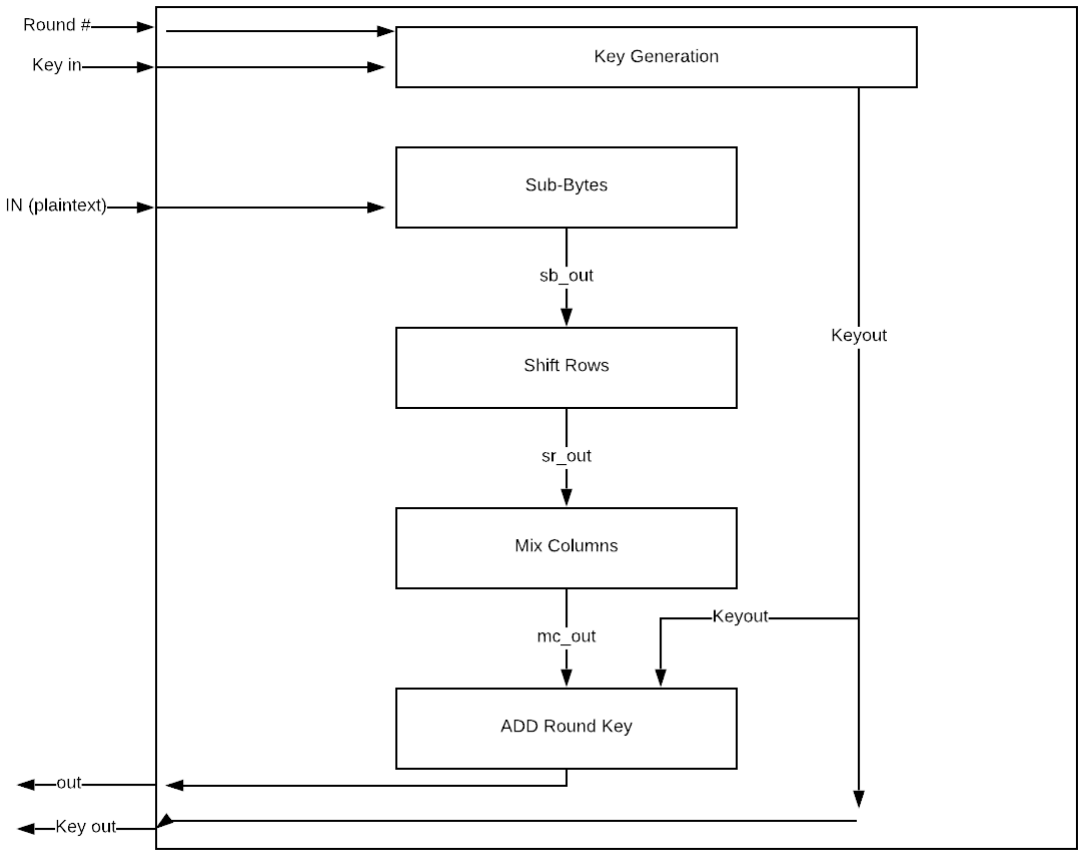
1. in -128 bit wire- (State)
2. round_num -128 bit wire- (Round Number)
3. keyin -128 bit wire- (input key)

Output:

1. keyout -128 bit register- (output of this round and input to the next round)
2. out -128 bit register- (output of this round and input to the next round)

Description:

- the input passes by these modules in order:
  key generation, substitute bytes, shift rows, mix columns, add round key



Substitute Bytes

Inputs:

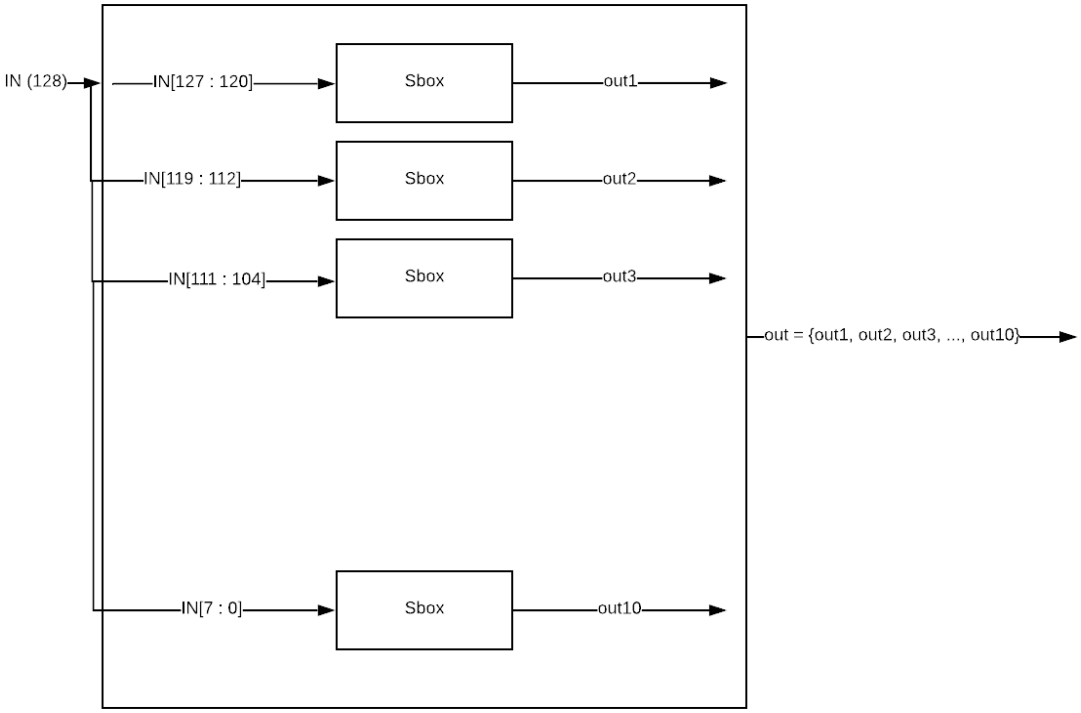
1. in -128 bit wire- (State)

Outputs:

1. out -128 bit register- (output)

Description:

- In this module, every byte from the input is substituted with another byte using the sbox



Shift Rows

Inputs:

1. in -128 bit wire- (state)

Outputs:

1. out -128 bit register- (output)

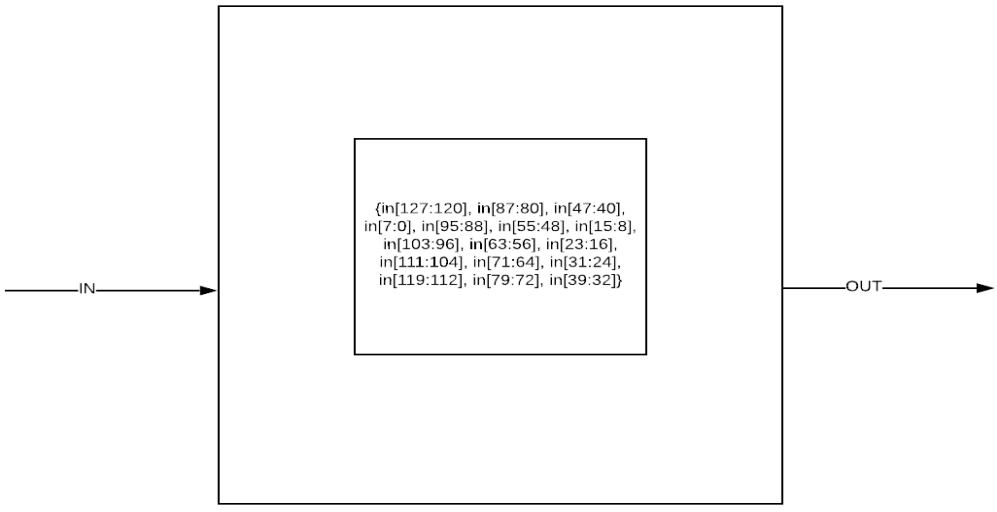
Description:

- Assume input is in the right order (consecutive 16 bytes -> 15, 14, 13, 12, 11, 10, 9, 8, 6, 5, 4, 3, 2, 1, 0) 4 by 4 matrix is as follows:
- Before shifting

$$\begin{bmatrix} 15 & 11 & 7 & 3 \\ 14 & 10 & 6 & 2 \\ 13 & 9 & 5 & 1 \\ 12 & 8 & 4 & 0 \end{bmatrix}$$

- After shifting

$$\begin{bmatrix} 15 & 11 & 7 & 3 \\ 10 & 6 & 2 & 14 \\ 5 & 1 & 13 & 9 \\ 0 & 12 & 8 & 4 \end{bmatrix}$$



Mix Columns

Input:

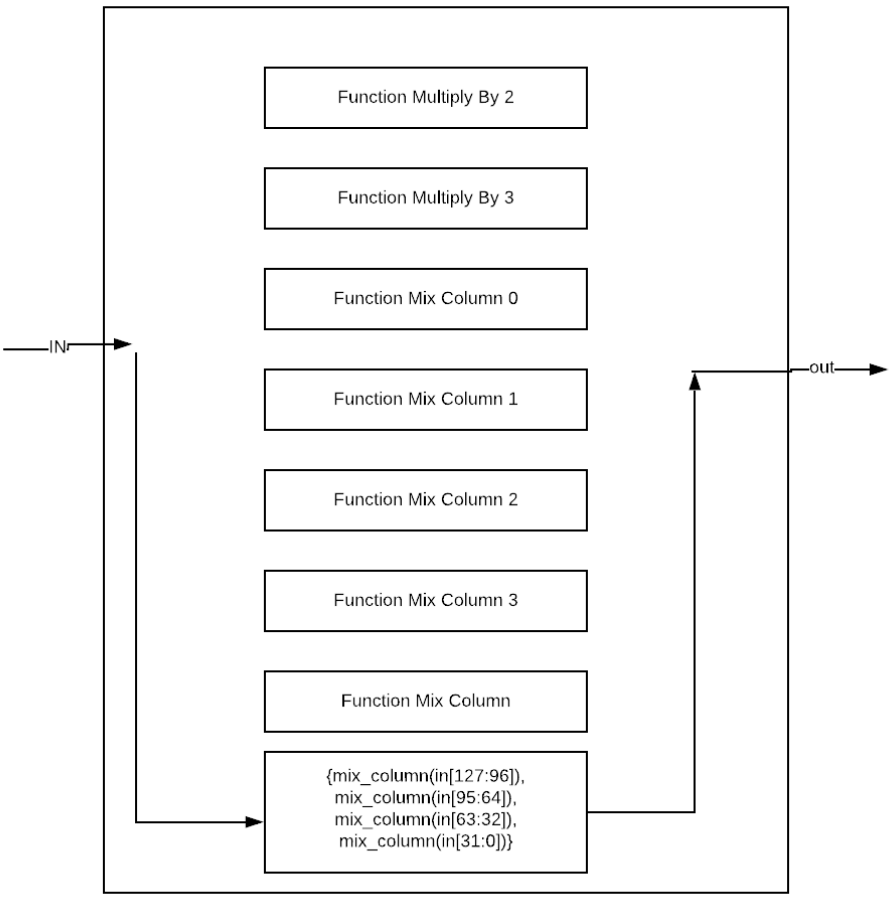
1. in -128 bit wire- (state)

Output:

1. out -128 bit register- (output)

Description:

- The module consists of 7 functions, one in which it multiplies by 2, the 2nd one multiplies by 3 (using modular arithmetic), the 3rd one multiplies and adds with [02 03 01 01] over GF(2^8), the 4th one multiplies and adds with [01 02 03 01] over GF(2^8), the 5th one multiplies and adds with [01 01 02 03] over GF(2^8), the 6th one multiplies and adds with [03 01 01 02] over GF(2^8), the last one is the output matrix



Add Round Key

Inputs:

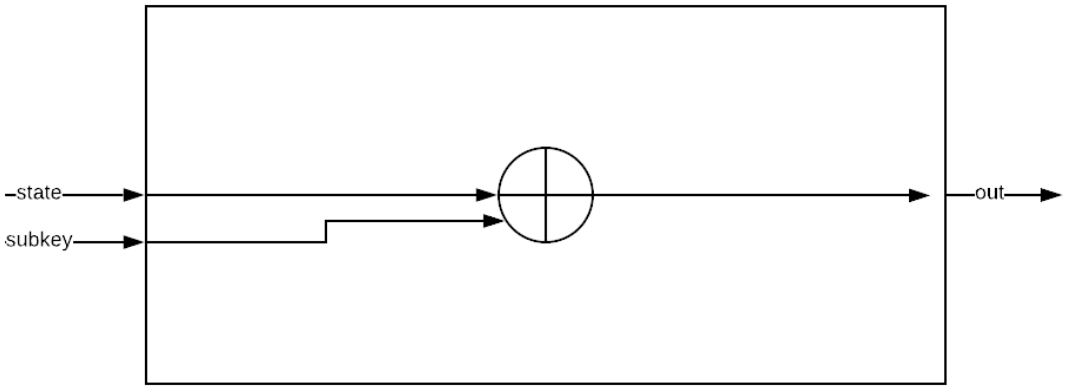
1. State -128 bit wire- (Plaintext after passing by n modules)
2. Subkey -128 bit wire- (specific key for each round)

Outputs:

1. Out -128 bit register- (output)

Description:

- In this module, the state is ored with the Subkey



AES Last Round

Inputs:

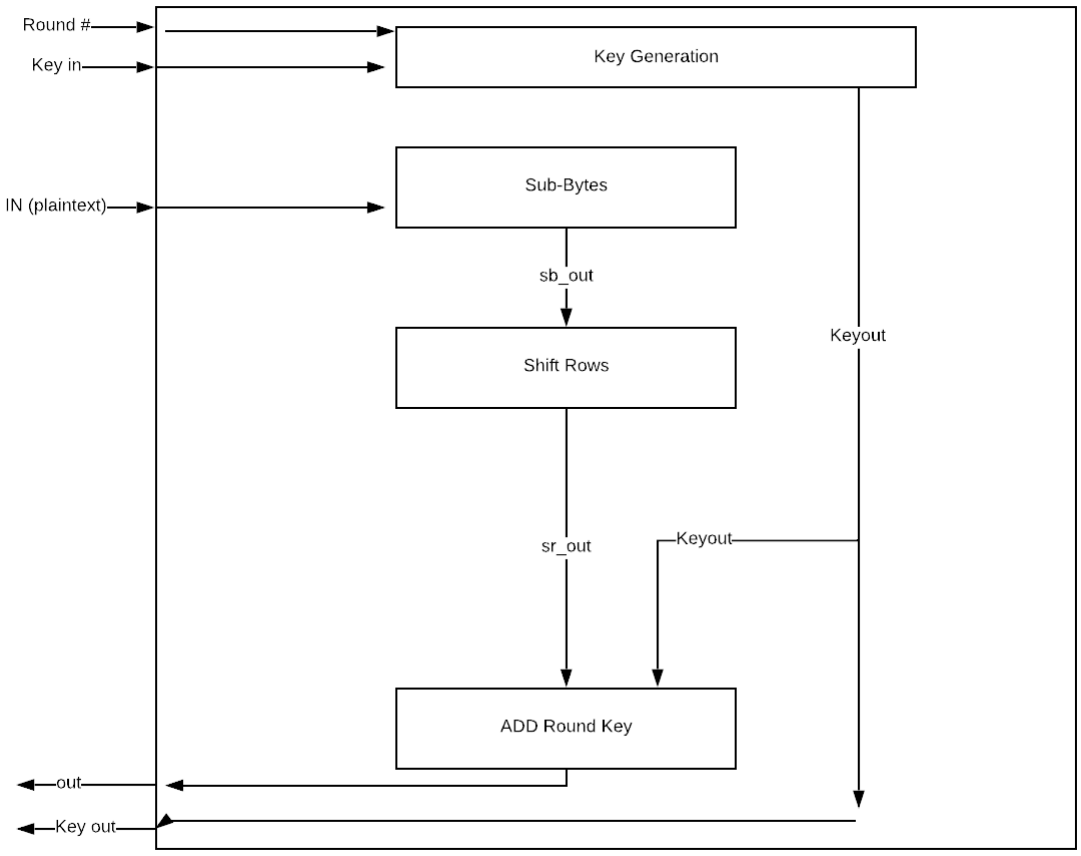
4. in -128 bit wire- (State)
5. round_num -128 bit wire- (Round Number)
6. keyin -128 bit wire- (input key)

Output:

3. keyout -128 bit register- (output of this round and input to the next round)
4. out -128 bit register- (output of this round and input to the next round)

Description:

- the input passes by these modules in order:
  key generation, substitute bytes, shift rows, add round key



Key Generation

Inputs:

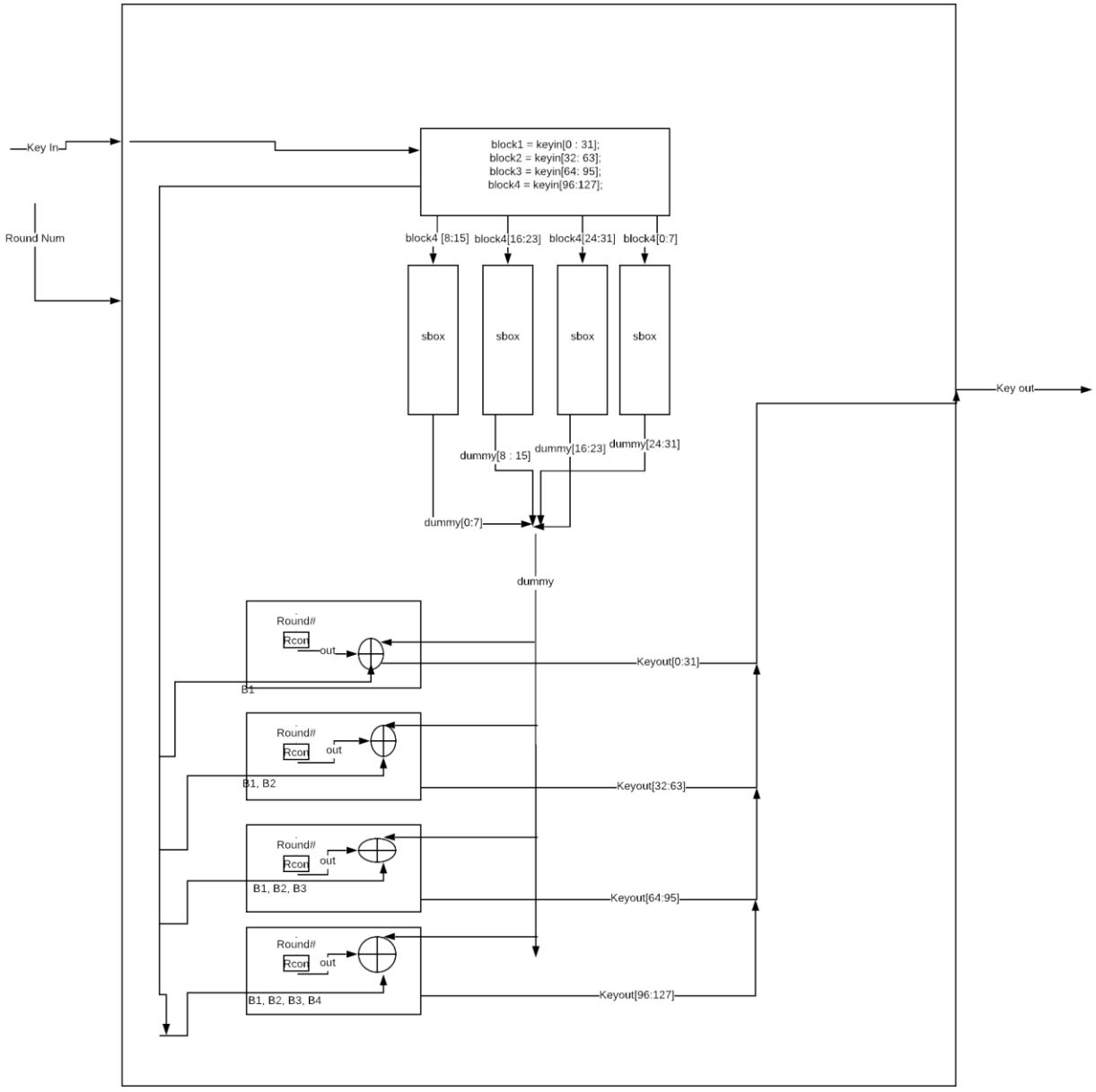
1. Round_num -128 bit wire- (Round Number)
2. Keyin -128 bit wire- (Initial Key)

Outputs:

1. Keyout -128 bit register- output key for each round

Description:

- We divide the key into bytes to form a 4 by 4 matrix
- We pass block4 (the 4th word) by an sbox for substitution
- We XOR the output


Key In
Round Num
block1 = keyin[0 : 31];
block2 = keyin[32: 63];
block3 = keyin[64: 95];
block4 = keyin[96:127];
block4 [8:15]
block4[16:23]
block4[24:31]
block4[0:7]
sbox
sbox
sbox
sbox
Key out
dummy[8 : 15]
dummy[16:23]
dummy[24:31]
dummy[0:7]
dummy
Round#
Rcon
out
B1
Keyout[0:31]
B1, B2
Keyout[32:63]
B1, B2, B3
Keyout[64:95]
B1, B2, B3, B4
Keyout[96:127]