Fast AES implementation using ARMv8 ASIMD

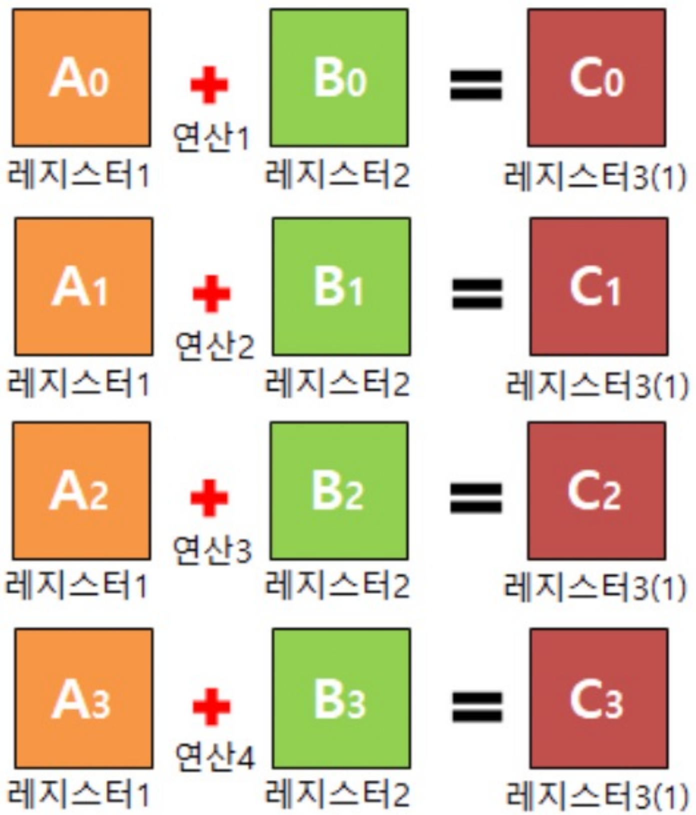
https://youtu.be/c14K3qbpj5U

한성대학교
HANSUNG UNIVERSITY

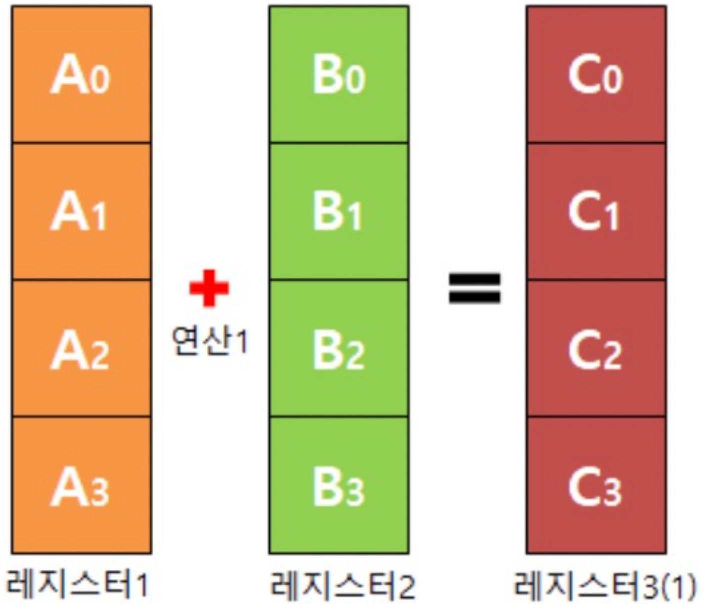
CryptoCraft LAB

ASIMD

- ASIMD (Advanced Single Instruction Multiple Data)
  - 하나의 명령어로 여러 데이터를 한번에 연산 할 수 있음.



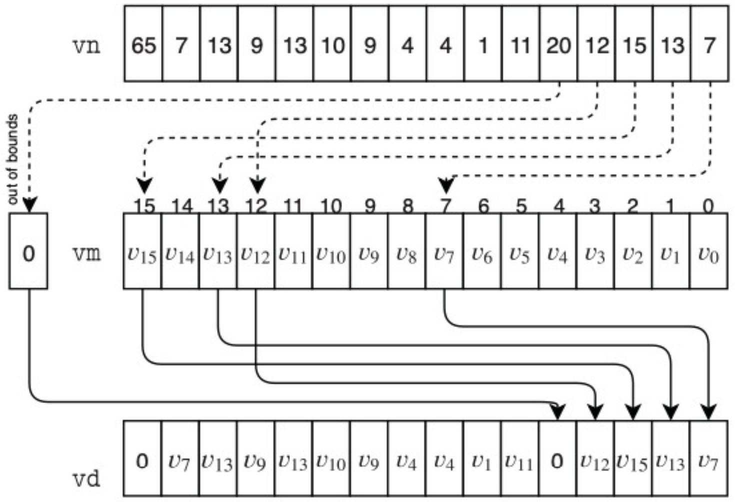
SISD 연산



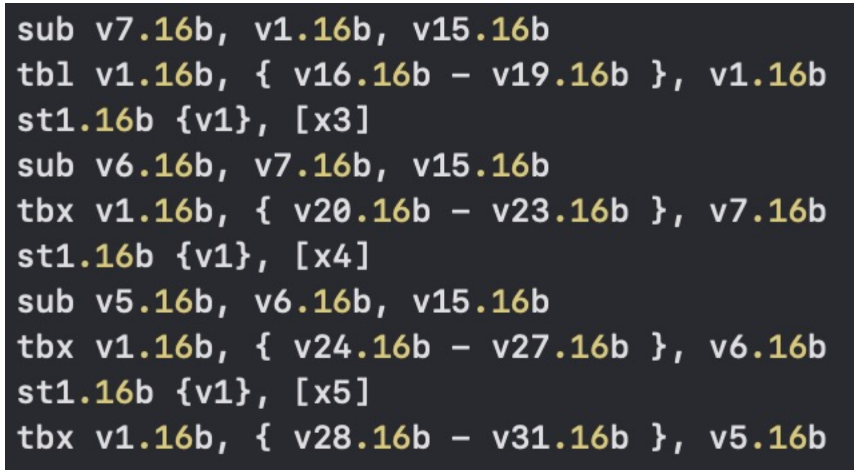
SIMD 연산

SubByte and ShiftRow

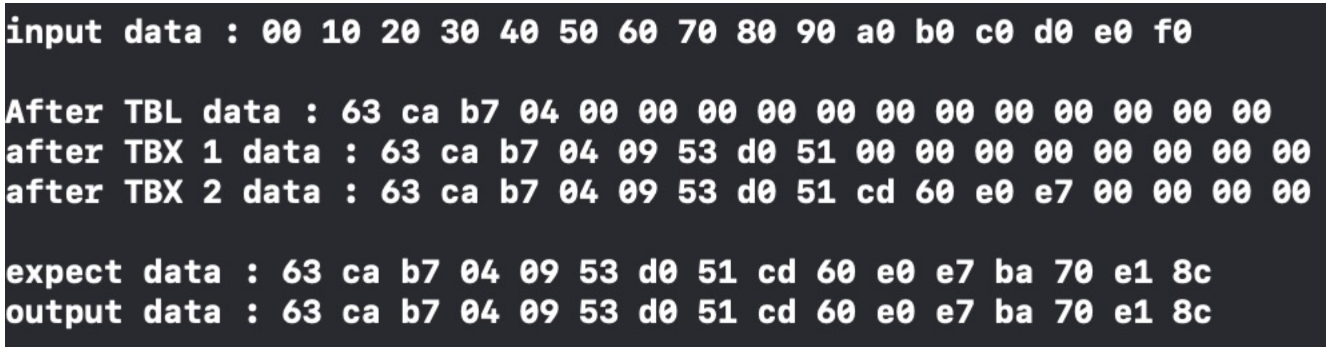
- TBL, TBX 명령어를 통해서 SubByte 구현
  - SBOX Table을 벡터 레지스터에 저장하여 구현
  - v1(input), v15(0x40), v16-v31(table) 16개


vn
65 7 13 9 13 10 9 4 4 1 11 20 12 15 13 7
out of bounds
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
0
vm
v_{15} v_{14} v_{13} v_{12} v_{11} v_{10} v_9 v_8 v_7 v_6 v_5 v_4 v_3 v_2 v_1 v_0
vd
0 v_7 v_{13} v_9 v_{13} v_{10} v_9 v_4 v_4 v_1 v_{11} 0 v_{12} v_{15} v_{13} v_7

(a) tbl vd, {vm}, vn. Lookup table is stored in vm.



```
sub v7.16b, v1.16b, v15.16b
tbl v1.16b, { v16.16b - v19.16b }, v1.16b
st1.16b {v1}, [x3]
sub v6.16b, v7.16b, v15.16b
tbx v1.16b, { v20.16b - v23.16b }, v7.16b
st1.16b {v1}, [x4]
sub v5.16b, v6.16b, v15.16b
tbx v1.16b, { v24.16b - v27.16b }, v6.16b
st1.16b {v1}, [x5]
tbx v1.16b, { v28.16b - v31.16b }, v5.16b
```



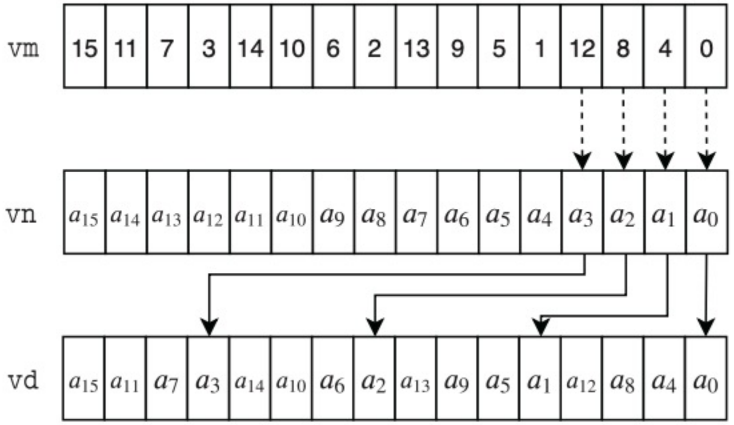
```
input data : 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0

After TBL data : 63 ca b7 04 00 00 00 00 00 00 00 00 00 00 00 00
after TBX 1 data : 63 ca b7 04 09 53 d0 51 00 00 00 00 00 00 00 00
after TBX 2 data : 63 ca b7 04 09 53 d0 51 cd 60 e0 e7 00 00 00 00

expect data : 63 ca b7 04 09 53 d0 51 cd 60 e0 e7 ba 70 e1 8c
output data : 63 ca b7 04 09 53 d0 51 cd 60 e0 e7 ba 70 e1 8c
```

SubByte and ShiftRow

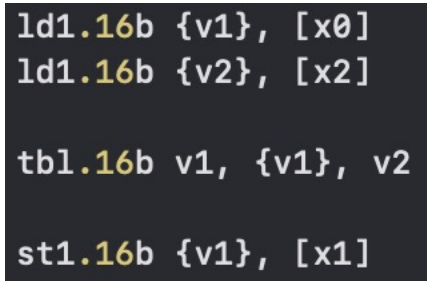
- ShiftRow도 TBL 명령어를 활용하여 구현

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

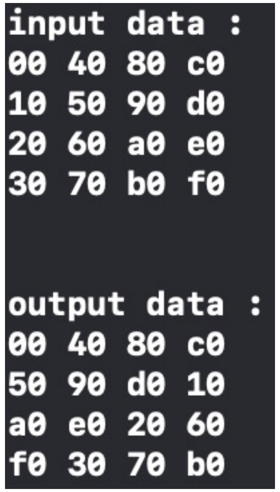
0	4	8	12
5	9	13	1
10	14	2	6
15	3	7	11


vm
15 11 7 3 14 10 6 2 13 9 5 1 12 8 4 0
vn
a_{15} a_{14} a_{13} a_{12} a_{11} a_{10} a_9 a_8 a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
vd
a_{15} a_{11} a_7 a_3 a_{14} a_{10} a_6 a_2 a_{13} a_9 a_5 a_1 a_{12} a_8 a_4 a_0

(b) **tbl vd, {vn}, vm**. The permutation pattern is held in **vm**.



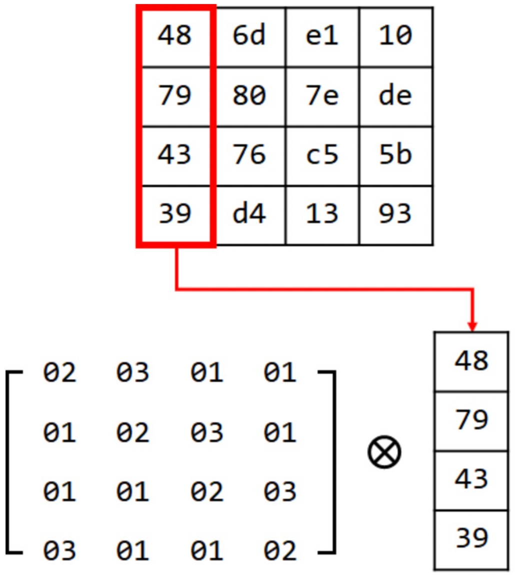
```
ld1.16b {v1}, [x0]
ld1.16b {v2}, [x2]

tbl.16b v1, {v1}, v2

st1.16b {v1}, [x1]
```



```
input data :
00 40 80 c0
10 50 90 d0
20 60 a0 e0
30 70 b0 f0


output data :
00 40 80 c0
50 90 d0 10
a0 e0 20 60
f0 30 70 b0
```

MixColumns

- Mixcolumn 구현을 위해 수식을 조금 다르게 바꾼다?



48	6d	e1	10
79	80	7e	de
43	76	c5	5b
39	d4	13	93

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \otimes \begin{bmatrix} 48 \\ 79 \\ 43 \\ 39 \end{bmatrix}$$

$$A' = \begin{bmatrix} a'_{0,j} \\ a'_{1,j} \\ a'_{2,j} \\ a'_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} = \begin{bmatrix} a_{0,j} & a_{3,j} & a_{2,j} & a_{1,j} \\ a_{1,j} & a_{0,j} & a_{3,j} & a_{2,j} \\ a_{2,j} & a_{1,j} & a_{0,j} & a_{3,j} \\ a_{3,j} & a_{2,j} & a_{1,j} & a_{0,j} \end{bmatrix} \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} =$$

$$= 2 \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} + \begin{bmatrix} a_{3,j} \\ a_{0,j} \\ a_{1,j} \\ a_{2,j} \end{bmatrix} + \begin{bmatrix} a_{2,j} \\ a_{3,j} \\ a_{0,j} \\ a_{1,j} \end{bmatrix} + 3 \begin{bmatrix} a_{1,j} \\ a_{2,j} \\ a_{3,j} \\ a_{0,j}. \end{bmatrix} . \qquad (2)$$

MixColumns

$$
\begin{aligned}
A' = \begin{bmatrix} \mathrm{a}'_{0,j} \\ \mathrm{a}'_{1,j} \\ \mathrm{a}'_{2,j} \\ \mathrm{a}'_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} \mathrm{a}_{0,j} \\ \mathrm{a}_{1,j} \\ \mathrm{a}_{2,j} \\ \mathrm{a}_{3,j} \end{bmatrix} &= \begin{bmatrix} \mathrm{a}_{0,j} & \mathrm{a}_{3,j} & \mathrm{a}_{2,j} & \mathrm{a}_{1,j} \\ \mathrm{a}_{1,j} & \mathrm{a}_{0,j} & \mathrm{a}_{3,j} & \mathrm{a}_{2,j} \\ \mathrm{a}_{2,j} & \mathrm{a}_{1,j} & \mathrm{a}_{0,j} & \mathrm{a}_{3,j} \\ \mathrm{a}_{3,j} & \mathrm{a}_{2,j} & \mathrm{a}_{1,j} & \mathrm{a}_{0,j} \end{bmatrix} \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} = \\
= 2 \underset{\text{A}}{\begin{bmatrix} \mathrm{a}_{0,j} \\ \mathrm{a}_{1,j} \\ \mathrm{a}_{2,j} \\ \mathrm{a}_{3,j} \end{bmatrix}} + \underset{\text{RotRight(A)}}{\begin{bmatrix} \mathrm{a}_{3,j} \\ \mathrm{a}_{0,j} \\ \mathrm{a}_{1,j} \\ \mathrm{a}_{2,j} \end{bmatrix}} + \underset{\text{Rev32(A)}}{\begin{bmatrix} \mathrm{a}_{2,j} \\ \mathrm{a}_{3,j} \\ \mathrm{a}_{0,j} \\ \mathrm{a}_{1,j} \end{bmatrix}} + 3 \underset{\text{RotLeft(A)}}{\begin{bmatrix} \mathrm{a}_{1,j} \\ \mathrm{a}_{2,j} \\ \mathrm{a}_{3,j} \\ \mathrm{a}_{0,j}. \end{bmatrix}} .
\end{aligned}
\tag{2}
$$

$$
\mathtt{RotLeft}(A) = (a_1, a_2, a_3, a_0), \qquad \mathtt{Rev32}(A) = (a_2, a_3, a_0, a_1),
$$

$$
\mathtt{RotRight}(A) = (a_3, a_0, a_1, a_2).
$$

$$
\mathtt{RotLeft}^2(X) = \mathtt{Rev32}(X) \text{ and } \mathtt{RotRight}(X) = \mathtt{Rev32}(\mathtt{RotLeft}(X))
$$

$$
A' = (2A + \mathtt{RotLeft}^2(A)) + \mathtt{RotLeft}((2A + \mathtt{RotLeft}^2(A)) + A), \tag{3}
$$

MixColumns

$$
\begin{aligned}
A' &= (2A + \texttt{RotLeft}^2(A)) + \texttt{RotLeft}((2A + \texttt{RotLeft}^2(A)) + A)\\
B' &= (2B + \texttt{RotLeft}^2(B)) + \texttt{RotLeft}((2B + \texttt{RotLeft}^2(B)) + B)\\
C' &= (2C + \texttt{RotLeft}^2(C)) + \texttt{RotLeft}((2C + \texttt{RotLeft}^2(C)) + C)\\
D' &= (2D + \texttt{RotLeft}^2(D)) + \texttt{RotLeft}((2D + \texttt{RotLeft}^2(D)) + D)
\end{aligned} .
$$

$$S = [A, B, C, D],$$

$$
\begin{aligned}
\texttt{RotLeft\_128}(S) &= [\texttt{RotLeft}(A), \texttt{RotLeft}(B), \texttt{RotLeft}(C), \texttt{RotLeft}(D)],\\
\texttt{Rev32\_128}(S) &= [\texttt{Rev32}(A), \texttt{Rev32}(B), \texttt{Rev32}(C), \texttt{Rev32}(D)],\\
\texttt{RotRight\_128}(S) &= [\texttt{RotRight}(A), \texttt{RotRight}(B), \texttt{RotRight}(C), \texttt{RotRight}(D)],\\
2S &= [2A, 2B, 2C, 2D].
\end{aligned}
$$

$$\Big\downarrow$$

$$
\begin{aligned}
\texttt{MixColumns}(S) = {} & (2S + \texttt{RotLeft\_128}^2(S))\\
& + \texttt{RotLeft\_128}((2S + \texttt{RotLeft\_128}^2(S)) + S).
\end{aligned} \tag{5}
$$

MixColumns

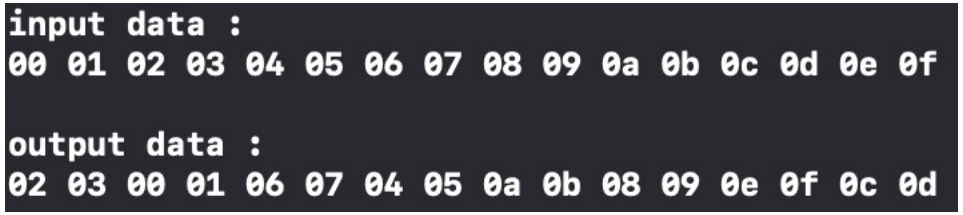
$\texttt{Rev32}(A) = (a_2, a_3, a_0, a_1),$

$$\mathrm{S} = [\ \mathrm{a}_{0,0}\ \mathrm{a}_{0,1}\ \mathrm{a}_{0,2}\ \mathrm{a}_{0,3}\ \mathrm{a}_{1,0}\ \mathrm{a}_{1,1}\ \mathrm{a}_{1,2}\ \mathrm{a}_{1,3}\ \mathrm{a}_{2,0}\ \mathrm{a}_{2,1}\ \mathrm{a}_{2,2}\ \mathrm{a}_{2,3}\ \mathrm{a}_{3,0}\ \mathrm{a}_{3,1}\ \mathrm{a}_{3,2}\ \mathrm{a}_{3,3}\ ]$$

$$\downarrow \mathrm{S}' = \texttt{vrev32q\_u16}(\mathrm{A})$$

$$\mathrm{S}' = [\ \mathrm{a}_{0,2}\ \mathrm{a}_{0,3}\ \mathrm{a}_{0,0}\ \mathrm{a}_{0,1}\ \mathrm{a}_{1,2}\ \mathrm{a}_{1,3}\ \mathrm{a}_{1,2}\ \mathrm{a}_{1,1}\ \mathrm{a}_{2,2}\ \mathrm{a}_{2,3}\ \mathrm{a}_{2,0}\ \mathrm{a}_{2,1}\ \mathrm{a}_{3,2}\ \mathrm{a}_{3,3}\ \mathrm{a}_{3,0}\ \mathrm{a}_{3,1}\ ].$$

REV32.8H v1, v1



```
input data :
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

output data :
02 03 00 01 06 07 04 05 0a 0b 08 09 0e 0f 0c 0d
```

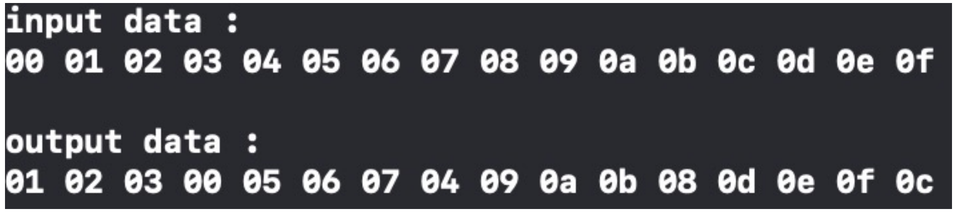
$\texttt{RotLeft}(A) = (a_1, a_2, a_3, a_0).$

$$\mathrm{S} = [\ \mathrm{a}_{0,0}\ \mathrm{a}_{0,1}\ \mathrm{a}_{0,2}\ \mathrm{a}_{0,3}\ \mathrm{a}_{1,0}\ \mathrm{a}_{1,1}\ \mathrm{a}_{1,2}\ \mathrm{a}_{1,3}\ \mathrm{a}_{2,0}\ \mathrm{a}_{2,1}\ \mathrm{a}_{2,2}\ \mathrm{a}_{2,3}\ \mathrm{a}_{3,0}\ \mathrm{a}_{3,1}\ \mathrm{a}_{3,2}\ \mathrm{a}_{3,3}\ ]$$

$$\downarrow \begin{array}{l} \mathrm{T} = \texttt{vrev32q\_u8}(\mathrm{S}) \\ \mathrm{S}' = \texttt{vtrn2q\_u8}(\mathrm{S},\ \mathrm{T}) \end{array}$$

$$\mathrm{S}' = [\ \mathrm{a}_{0,1}\ \mathrm{a}_{0,2}\ \mathrm{a}_{0,3}\ \mathrm{a}_{0,0}\ \mathrm{a}_{1,1}\ \mathrm{a}_{1,2}\ \mathrm{a}_{1,3}\ \mathrm{a}_{1,0}\ \mathrm{a}_{2,1}\ \mathrm{a}_{2,2}\ \mathrm{a}_{2,3}\ \mathrm{a}_{2,0}\ \mathrm{a}_{3,1}\ \mathrm{a}_{3,2}\ \mathrm{a}_{3,3}\ \mathrm{a}_{3,0}\ ].$$

REV32.16b v2, v1
TRN2.16b v1, v1, v2



```
input data :
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

output data :
01 02 03 00 05 06 07 04 09 0a 0b 08 0d 0e 0f 0c
```

MixColumns

$$A' = \begin{bmatrix} \mathrm{a}'_{0,j} \\ \mathrm{a}'_{1,j} \\ \mathrm{a}'_{2,j} \\ \mathrm{a}'_{3,j} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 03\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} \mathrm{a}_{0,j} \\ \mathrm{a}_{1,j} \\ \mathrm{a}_{2,j} \\ \mathrm{a}_{3,j} \end{bmatrix} = \begin{bmatrix} 2(\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) + \mathrm{a}_{1,j} + (\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) \\ 2(\mathrm{a}_{1,j} + \mathrm{a}_{2,j}) + \mathrm{a}_{0,j} + (\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) \\ 2(\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) + \mathrm{a}_{3,j} + (\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) \\ 2(\mathrm{a}_{3,j} + \mathrm{a}_{0,j}) + \mathrm{a}_{2,j} + (\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) \end{bmatrix}. \qquad (6)$$

$$\begin{aligned} \mathrm{a}_{0,j} + \mathrm{a}_{1,j} + \mathrm{a}_{2,j} + \mathrm{a}_{3,j} &= \mathrm{a}'_{0,j} + \mathrm{a}'_{1,j} + \mathrm{a}'_{2,j} + \mathrm{a}'_{3,j} \\ \mathrm{a}'_{0,j} + \mathrm{a}'_{1,j} &= 2(\mathrm{a}_{0,j} + \mathrm{a}_{2,j}) + \mathrm{a}_{0,j} + \mathrm{a}_{1,j} \\ \mathrm{a}'_{2,j} + \mathrm{a}'_{3,j} &= 2(\mathrm{a}_{0,j} + \mathrm{a}_{2,j}) + \mathrm{a}_{2,j} + \mathrm{a}_{3,j}. \end{aligned}$$

$$\boxed{\begin{aligned} \mathrm{a}'_{0,j} &= 2(\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) + \mathrm{a}_{1,j} + (\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) \\ \mathrm{a}'_{1,j} &= 2(\mathrm{a}_{0,j} + \mathrm{a}_{2,j}) + \mathbf{a'_{0,j}} + (\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) \\ \mathrm{a}'_{2,j} &= 2(\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) + \mathrm{a}_{3,j} + (\mathrm{a}_{0,j} + \mathrm{a}_{1,j}) \\ \mathrm{a}'_{3,j} &= 2(\mathrm{a}_{0,j} + \mathrm{a}_{2,j}) + \mathbf{a'_{2,j}} + (\mathrm{a}_{2,j} + \mathrm{a}_{3,j}) \end{aligned}.}$$

감사합니다