

AES

김현지

<https://youtu.be/QwPoLBUVhO4>

Contents

01. AES

02. 동작

03. 구현



01. 배경



AES 구조

❖ AES - 128 / 192 / 256 (key의 길이)

- 각각 10 / 12 / 14 round

❖ 블록 암호 & SPN 구조

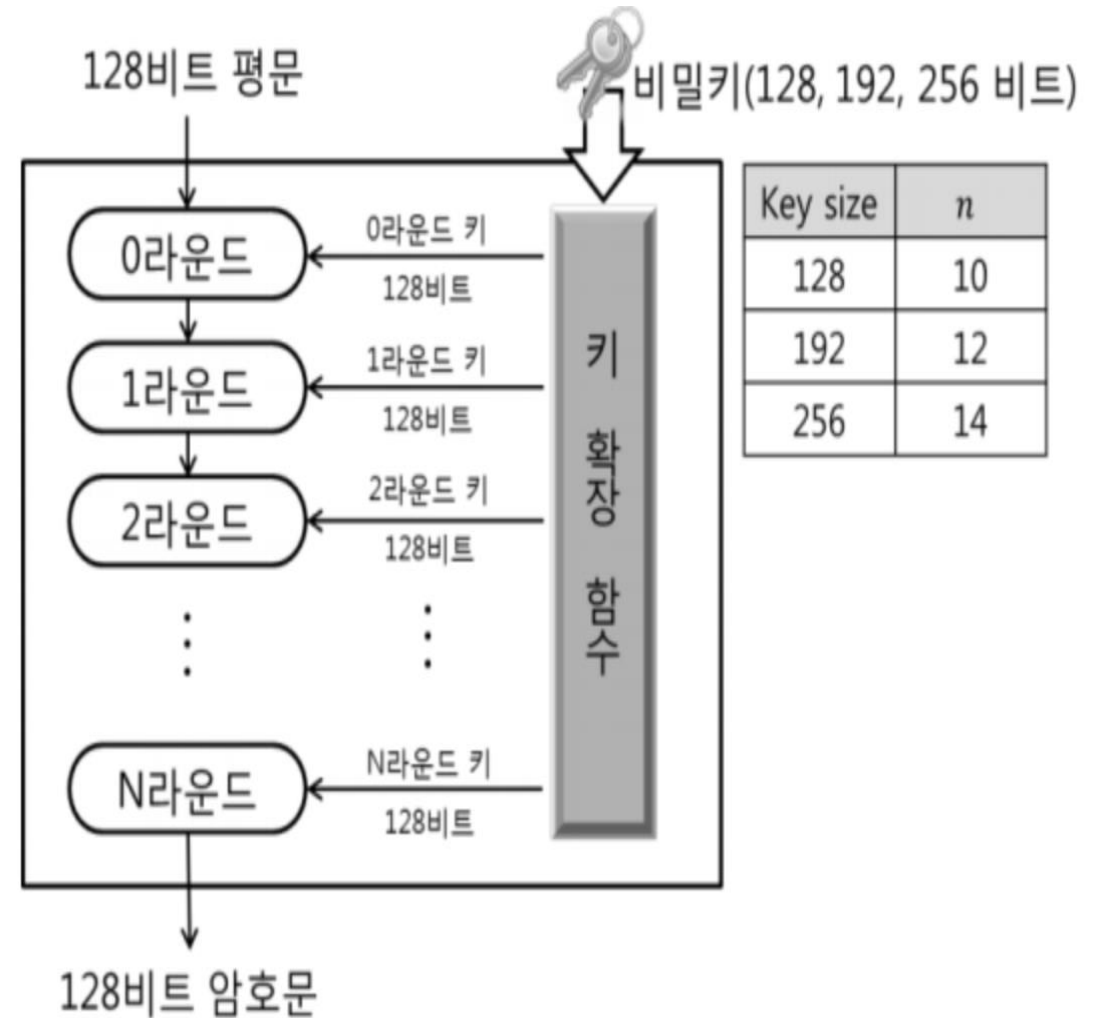
- 블록 크기 = 128bits
- 병렬 연산 가능 (속도 빠름)
- 별도의 복호화 모듈 필요

❖ 128 bit Key로 한번에 암호화

❖ DES에 비해 key의 길이, 블록 크기 증가 / round 감소

❖ State

- 16 byte (=128 bits) 의 4x4 행렬
- Block이 state로 표현



AES 수학적 배경

❖ GF(2⁸) 상에서의 확장체 연산

- AES에서 유한체는 256개의 원소를 포함 → 체의 원소 각각이 하나의 Byte로 표현 가능
 - 각 원소는 다항식 형태로 표현 : $A \in GF(2^8), A(x) = x^7 + x^6 + x^3 + x + 1 = 11001011$
- 계산 결과가 GF(2⁸)상의 원소가 되도록 연산
 - 이 때, mod 256이 아닌 mod P(x) 상에서의 연산 : $P(x) = x^8 + x^4 + x^3 + x + 1$
- GF(2⁸)상의 역원 : Subbyte 과정에서 쓰이는 S-box는 각 원소에 대한 역원을 미리 계산한 Lookup Table

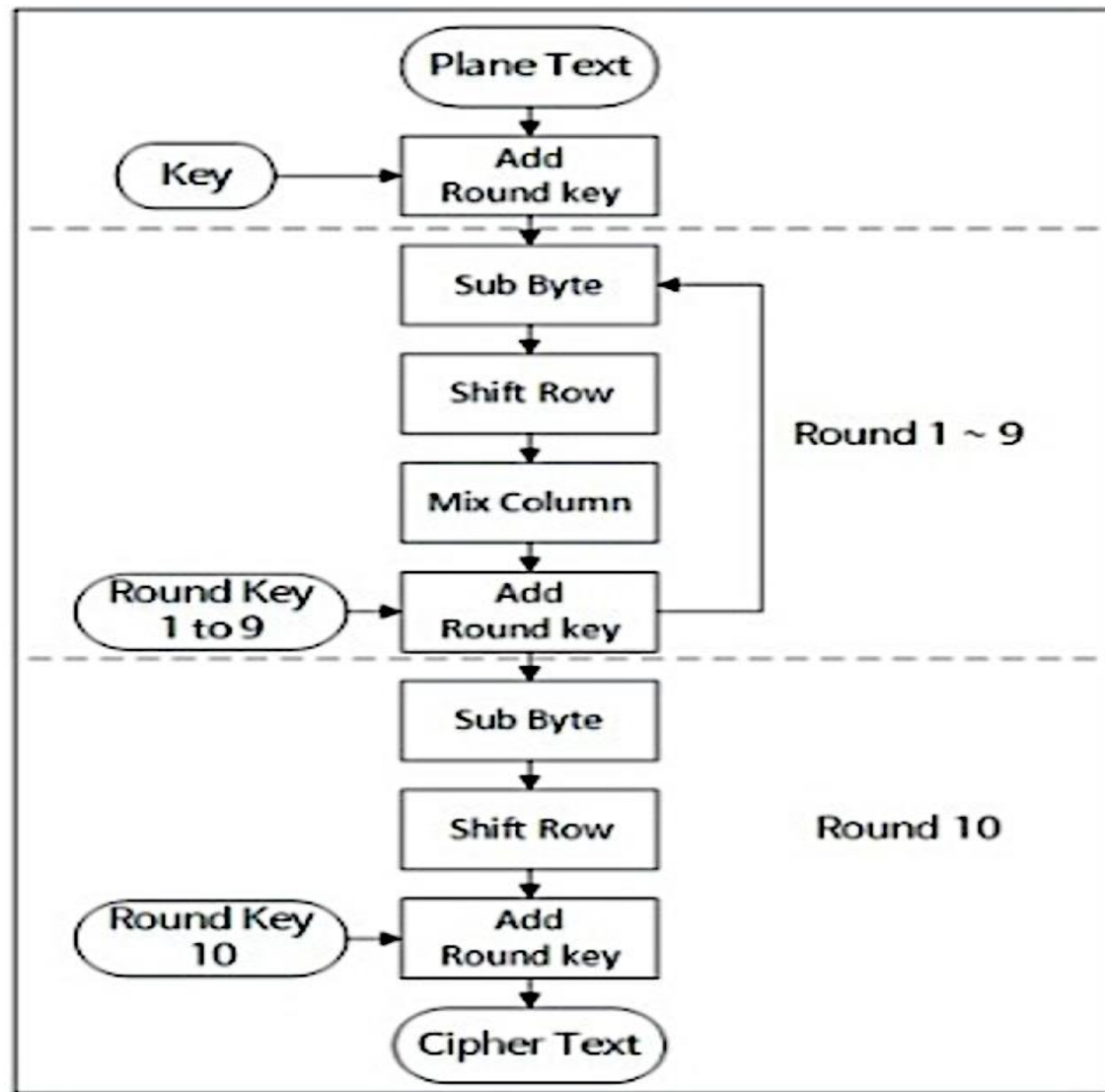
02. 동작



AES

❖ 동작원리

- 각 round에는 4가지 연산
 - Sub Byte / Shift Row / Mix Column / Add Round Key
 - 치환 연산 3개, 단순 shift 1개
- 0 round : Add Round-key (preprocessing)
- 10 round : Mix column 수행 x
- Round-key는 키 확장 함수에 의해 생성
 - Round마다 다른 key 사용
 - round-key : 128bit



AES

❖ Plain text(128 bit) → State

H	A	N	S	U	N	G	U	N	I	V	E	R	S	I	T
48	41	4E	53	55	4E	47	55	4E	49	56	45	52	53	49	54

48	55	4E	52
41	4E	49	53
4E	47	56	49
53	55	45	54

Plain Text

AES

❖0-round : Add Round-Key

48	55	4E	52
41	4E	49	53
4E	47	56	49
53	55	45	54

Plain Text

\oplus

11	55	4F	F0
22	44	A2	B1
33	11	9D	33
44	22	3C	52

Cipher Key

=

59	00	01	A2
63	0A	EB	E2
7D	56	CB	7A
17	77	79	06

Add Round-key
Output

AES

❖ Sub Byte

59	00	01	A2
63	0A	EB	E2
7D	56	CB	7A
17	77	79	06

Sub byte
Input

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

S-box

=

CB	63	7C	3A
FB	67	E9	98
FF	B1	1F	DA
F0	F5	B6	6F

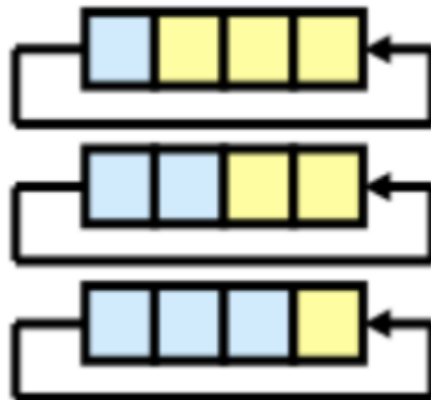
Sub Byte
Output

AES

❖ Shift-Row

CB	63	7C	3A
FB	67	E9	98
FF	B1	1F	DA
F0	F5	B6	6F

Shift-row
Input



=

CB	63	7C	3A
67	E9	98	FB
1F	DA	FF	B1
6F	F0	F5	B6

Shift-Row
Output

AES

❖ Mix-Column

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Mix-Column
Matrix

*

CB	63	7C	3A
67	E9	98	FB
1F	DA	FF	B1
6F	F0	F5	B6

State

=

54	CC	41	65
4B	2F	B8	A9
23	2E	05	79
E0	6D	12	73

Mix-Column
Output

AES

❖ Mix

- 1 * input

- input

- 2 * input

- Overflow 발생 시, 최상위 비트는 떼어버림 (9 → 8-bits)
→ 해당 결과 값 $\oplus 0x1B$

- 3 * input

- 1 * input + 2 * input

- ** 0x1B를 XOR하는 이유?**

- : GF(2⁸)상에서의 기약다항식 $P(x) = x^8 + x^4 + x^3 + x + 1$

- overflow 발생 (8bit초과) 시, x^8 이상의 다항식 항은 확장체 나눗셈 연산 통해 제거
 - 곱해지는 값이 최대 03 (= $x + 1$)이므로 x^8 을 초과하지 않음
 - $x^8 \equiv (x^4 + x^3 + x + 1) \pmod{P(x)} \rightarrow$ 같은 값인 $x^4 + x^3 + x + 1$ 를 더해줌
 - 00011011 = 0x1B

Mix-Column

Output

65

A9

79

73

AES

❖ Mix-Column 다항식 계산

02	03	01	01	*	CB
01	02	03	01		67
01	01	02	03		1F
03	01	01	02		6F

$$\rightarrow (02 * CB) \oplus (03 * 67) \oplus (01 * 1F) \oplus (01 * 6F)$$

$$i) CB = 11001011 = x^7 + x^6 + x^3 + x + 1$$

$$02 = 00000010 = x$$

$$02 * CB = x(x^7 + x^6 + x^3 + x + 1) = x^8 + x^7 + x^4 + x^2 + x$$

$$x^8 \equiv x^4 + x^3 + x + 1 \pmod{P(x)} \quad x^8 + x^7 + x^4 + x^2 + x = x^4 + x^3 + x + 1 + x^7 + x^4 + x^2 + x$$

$$= x^7 + x^3 + x^2 + 1 = 10001101_2 = 1D_{(16)}$$

$$ii) 03 * 67 = (x+1)(x^6 + x^5 + x^2 + x + 1) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$01100111 = x^6 + x^5 + x^3 + 1 = 10101001_2 = A9_{(16)}$$

$$iii) 01 * 1F = 1F, 01 * 6F = 6F$$

$$\therefore 1D \oplus A9 \oplus 1F \oplus 6F = 54_{(16)}$$

* 0x1B XOR 이용하여 계산한 값과 동일

=

54	CC	41	65
4B	2F	B8	A9
23	2E	05	79
E0	6D	12	73

Mix-Column
Output

AES

❖ Add Round-key

54	CC	41	65
4B	2F	B8	A9
23	2E	05	79
E0	6D	12	73

Add Round-key
Input

\oplus

D8	8D	C2	32
E1	A5	07	B6
33	22	BF	8C
C8	EA	D6	84

Round-key

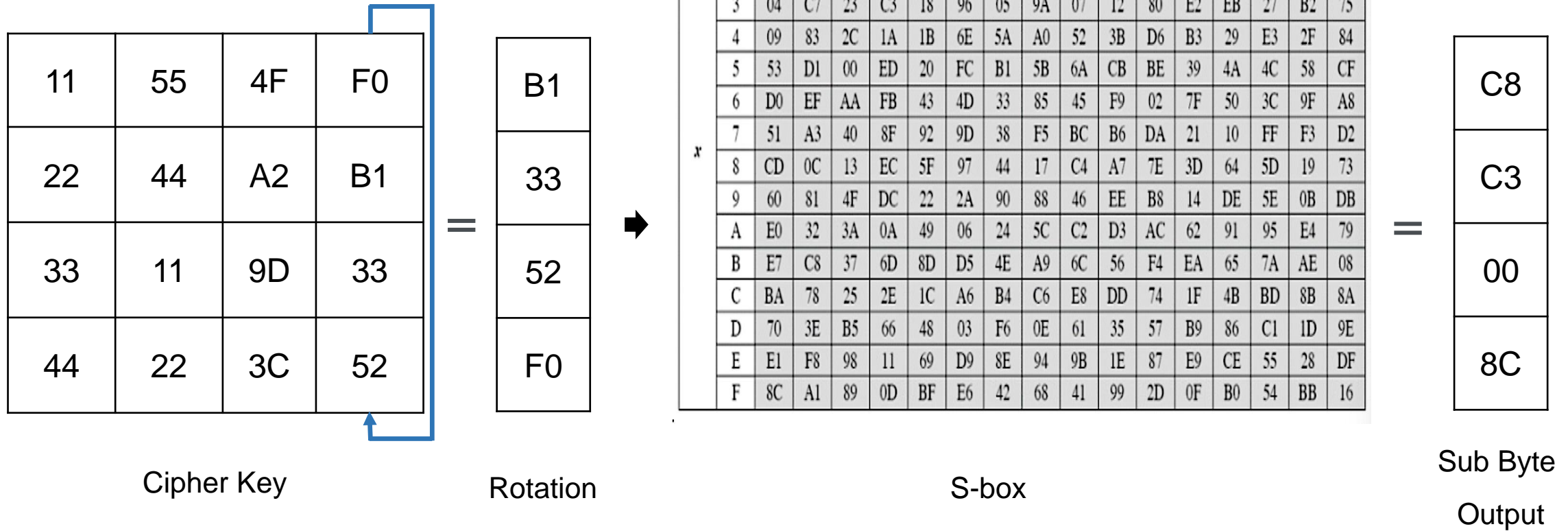
=

8C	41	83	57
AA	8A	BF	1F
10	0C	BA	F5
28	87	C4	F7

Round 종료

AES

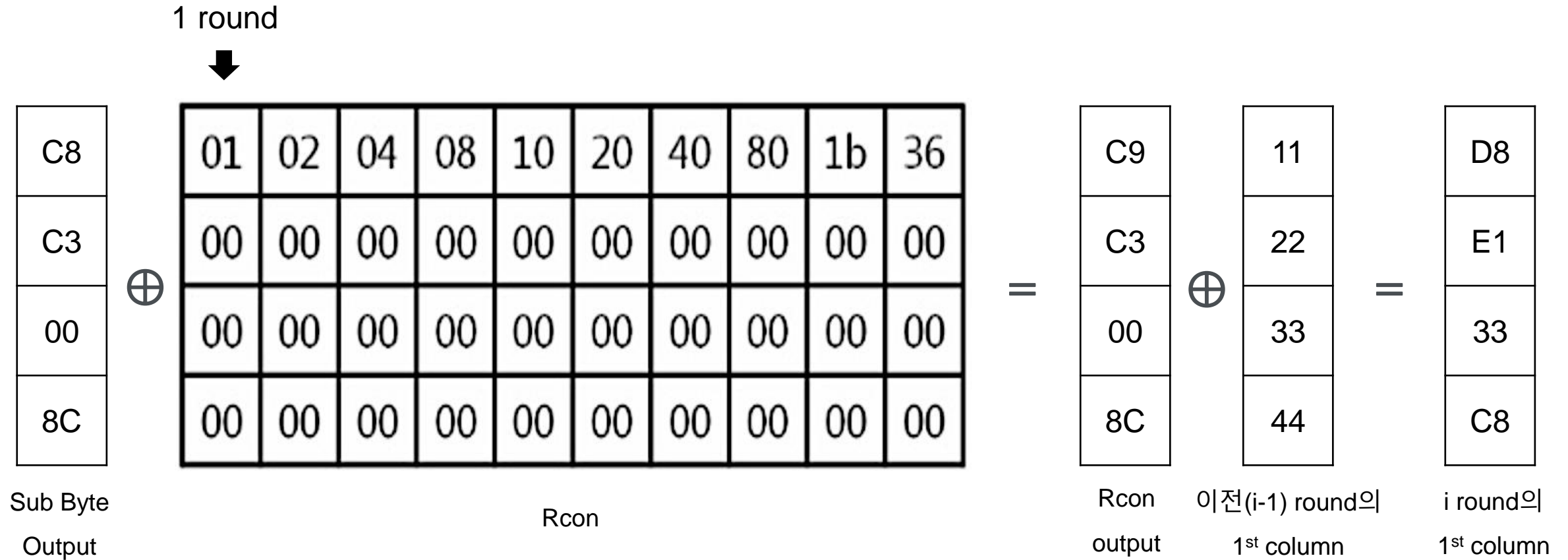
❖ Key Scheduling



AES

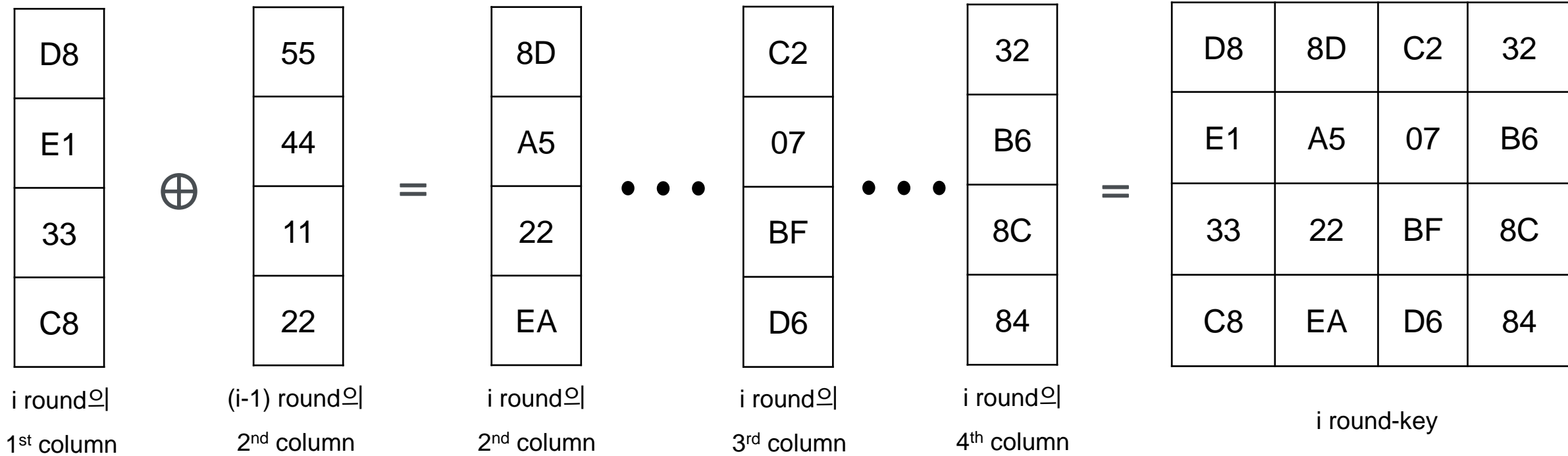
❖ Key Scheduling

* i round의 Round key 구하는 경우



AES

❖ Key Scheduling



03. 구현



AES

u8 w[176];

$w[16*i+j+0]$	$w[]$	$w[]$	$w[]$
$w[16*i+j+4]$	$w[]$	$w[]$	$w[]$
$w[16*i+j+8]$	$w[]$	$w[]$	$w[]$
$w[16*i+j+12]$	$w[]$	$w[]$	$w[]$

```
for(int j = 1 ; j < 4 ; j++){  
    w[16*i + (0+j)] = w[16*(i-1) + 0+j] ^ w[16*i + (j-1) + 0]; //  
    w[16*i + (4+j)] = w[16*(i-1) + 4+j] ^ w[16*i + (j-1) + 4]; //  
    w[16*i + (8+j)] = w[16*(i-1) + 8+j] ^ w[16*i + (j-1) + 8]; //  
    w[16*i + (12+j)] = w[16*(i-1) + 12+j] ^ w[16*i + (j-1) + 12]; //  
}
```

AES

```
for(int i = 1 ; i < 11 ; i++){
    // 이전 라운드의 마지막 열을 연산에 사용하기 위해 temp[]에 저장
    temp[0] = w[16 * (i-1) + 4*0 + 3]; // 16 * (i-1) --> 이전 round key의 맨 처음 요소 : w[0], w[16]...
    temp[1] = w[16 * (i-1) + 4*1 + 3]; // 4*1, 4*2...--> 이전 round key의 맨 처음 열, +3 --> 마지막 열
    temp[2] = w[16 * (i-1) + 4*2 + 3]; |
    temp[3] = w[16 * (i-1) + 4*3 + 3];
```

$w[16*(i-1)]$	$w[]$	$w[]$	$w[16*(i-1) + 4*0 + 3]$
$w[16*(i-1) + 4*1]$	$w[]$	$w[]$	$w[16*(i-1) + 4*1 + 3]$
$w[16*(i-1) + 4*2]$	$w[]$	$w[]$	$w[16*(i-1) + 4*2 + 3]$
$w[16*(i-1) + 4*3]$	$w[]$	$w[]$	$w[16*(i-1) + 4*3 + 3]$

$w[16]$	$w[17]$	$w[18]$	$w[19]$
$w[20]$	$w[21]$	$w[22]$	$w[23]$
$w[24]$	$w[25]$	$w[26]$	$w[27]$
$w[28]$	$w[29]$	$w[30]$	$w[31]$

* 2 round : $w[32] \sim w[47]$
 → 1 round의 마지막 열 사용

Input = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

The Round Key values are taken from the Key Expansion example in Appendix A.

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key Value																																																																																
input	<table><tr><td>32</td><td>88</td><td>31</td><td>e0</td></tr><tr><td>43</td><td>5a</td><td>31</td><td>37</td></tr><tr><td>f6</td><td>30</td><td>98</td><td>07</td></tr><tr><td>a8</td><td>8d</td><td>a2</td><td>34</td></tr></table>	32	88	31	e0	43	5a	31	37	f6	30	98	07	a8	8d	a2	34	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td>2b</td><td>28</td><td>ab</td><td>09</td></tr><tr><td>7e</td><td>ae</td><td>f7</td><td>cf</td></tr><tr><td>15</td><td>d2</td><td>15</td><td>4f</td></tr><tr><td>16</td><td>a6</td><td>88</td><td>3c</td></tr></table> ⊕=	2b	28	ab	09	7e	ae	f7	cf	15	d2	15	4f	16	a6	88	3c
	32	88	31	e0																																																																																	
	43	5a	31	37																																																																																	
	f6	30	98	07																																																																																	
	a8	8d	a2	34																																																																																	
2b	28	ab	09																																																																																		
7e	ae	f7	cf																																																																																		
15	d2	15	4f																																																																																		
16	a6	88	3c																																																																																		
1	<table><tr><td>19</td><td>a0</td><td>9a</td><td>e9</td></tr><tr><td>3d</td><td>f4</td><td>c6</td><td>f8</td></tr><tr><td>e3</td><td>e2</td><td>8d</td><td>48</td></tr><tr><td>be</td><td>2b</td><td>2a</td><td>08</td></tr></table>	19	a0	9a	e9	3d	f4	c6	f8	e3	e2	8d	48	be	2b	2a	08	<table><tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr><tr><td>27</td><td>bf</td><td>b4</td><td>41</td></tr><tr><td>11</td><td>98</td><td>5d</td><td>52</td></tr><tr><td>ae</td><td>f1</td><td>e5</td><td>30</td></tr></table>	d4	e0	b8	1e	27	bf	b4	41	11	98	5d	52	ae	f1	e5	30	<table><tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr><tr><td>bf</td><td>b4</td><td>41</td><td>27</td></tr><tr><td>5d</td><td>52</td><td>11</td><td>98</td></tr><tr><td>30</td><td>ae</td><td>f1</td><td>e5</td></tr></table>	d4	e0	b8	1e	bf	b4	41	27	5d	52	11	98	30	ae	f1	e5	<table><tr><td>04</td><td>e0</td><td>48</td><td>28</td></tr><tr><td>66</td><td>cb</td><td>f8</td><td>06</td></tr><tr><td>81</td><td>19</td><td>d3</td><td>26</td></tr><tr><td>e5</td><td>9a</td><td>7a</td><td>4c</td></tr></table>	04	e0	48	28	66	cb	f8	06	81	19	d3	26	e5	9a	7a	4c	<table><tr><td>a0</td><td>88</td><td>23</td><td>2a</td></tr><tr><td>fa</td><td>54</td><td>a3</td><td>6c</td></tr><tr><td>fe</td><td>2c</td><td>39</td><td>76</td></tr><tr><td>17</td><td>b1</td><td>39</td><td>05</td></tr></table> ⊕=	a0	88	23	2a	fa	54	a3	6c	fe	2c	39	76	17	b1	39	05
	19	a0	9a	e9																																																																																	
	3d	f4	c6	f8																																																																																	
	e3	e2	8d	48																																																																																	
	be	2b	2a	08																																																																																	
d4	e0	b8	1e																																																																																		
27	bf	b4	41																																																																																		
11	98	5d	52																																																																																		
ae	f1	e5	30																																																																																		
d4	e0	b8	1e																																																																																		
bf	b4	41	27																																																																																		
5d	52	11	98																																																																																		
30	ae	f1	e5																																																																																		
04	e0	48	28																																																																																		
66	cb	f8	06																																																																																		
81	19	d3	26																																																																																		
e5	9a	7a	4c																																																																																		
a0	88	23	2a																																																																																		
fa	54	a3	6c																																																																																		
fe	2c	39	76																																																																																		
17	b1	39	05																																																																																		
2	<table><tr><td>a4</td><td>68</td><td>6b</td><td>02</td></tr><tr><td>9c</td><td>9f</td><td>5b</td><td>6a</td></tr><tr><td>7f</td><td>35</td><td>ea</td><td>50</td></tr><tr><td>f2</td><td>2b</td><td>43</td><td>49</td></tr></table>	a4	68	6b	02	9c	9f	5b	6a	7f	35	ea	50	f2	2b	43	49	<table><tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr><tr><td>de</td><td>db</td><td>39</td><td>02</td></tr><tr><td>d2</td><td>96</td><td>87</td><td>53</td></tr><tr><td>89</td><td>f1</td><td>1a</td><td>3b</td></tr></table>	49	45	7f	77	de	db	39	02	d2	96	87	53	89	f1	1a	3b	<table><tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr><tr><td>db</td><td>39</td><td>02</td><td>de</td></tr><tr><td>87</td><td>53</td><td>d2</td><td>96</td></tr><tr><td>3b</td><td>89</td><td>f1</td><td>1a</td></tr></table>	49	45	7f	77	db	39	02	de	87	53	d2	96	3b	89	f1	1a	<table><tr><td>58</td><td>1b</td><td>db</td><td>1b</td></tr><tr><td>4d</td><td>4b</td><td>e7</td><td>6b</td></tr><tr><td>ca</td><td>5a</td><td>ca</td><td>b0</td></tr><tr><td>f1</td><td>ac</td><td>a8</td><td>e5</td></tr></table>	58	1b	db	1b	4d	4b	e7	6b	ca	5a	ca	b0	f1	ac	a8	e5	<table><tr><td>f2</td><td>7a</td><td>59</td><td>73</td></tr><tr><td>c2</td><td>96</td><td>35</td><td>59</td></tr><tr><td>95</td><td>b9</td><td>80</td><td>f6</td></tr><tr><td>f2</td><td>43</td><td>7a</td><td>7f</td></tr></table> ⊕=	f2	7a	59	73	c2	96	35	59	95	b9	80	f6	f2	43	7a	7f
	a4	68	6b	02																																																																																	
	9c	9f	5b	6a																																																																																	
	7f	35	ea	50																																																																																	
	f2	2b	43	49																																																																																	
49	45	7f	77																																																																																		
de	db	39	02																																																																																		
d2	96	87	53																																																																																		
89	f1	1a	3b																																																																																		
49	45	7f	77																																																																																		
db	39	02	de																																																																																		
87	53	d2	96																																																																																		
3b	89	f1	1a																																																																																		
58	1b	db	1b																																																																																		
4d	4b	e7	6b																																																																																		
ca	5a	ca	b0																																																																																		
f1	ac	a8	e5																																																																																		
f2	7a	59	73																																																																																		
c2	96	35	59																																																																																		
95	b9	80	f6																																																																																		
f2	43	7a	7f																																																																																		
3	<table><tr><td>aa</td><td>61</td><td>82</td><td>68</td></tr><tr><td>8f</td><td>dd</td><td>d2</td><td>32</td></tr><tr><td>5f</td><td>e3</td><td>4a</td><td>46</td></tr><tr><td>03</td><td>ef</td><td>d2</td><td>9a</td></tr></table>	aa	61	82	68	8f	dd	d2	32	5f	e3	4a	46	03	ef	d2	9a	<table><tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr><tr><td>73</td><td>c1</td><td>b5</td><td>23</td></tr><tr><td>cf</td><td>11</td><td>d6</td><td>5a</td></tr><tr><td>7b</td><td>df</td><td>b5</td><td>b8</td></tr></table>	ac	ef	13	45	73	c1	b5	23	cf	11	d6	5a	7b	df	b5	b8	<table><tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr><tr><td>c1</td><td>b5</td><td>23</td><td>73</td></tr><tr><td>d6</td><td>5a</td><td>cf</td><td>11</td></tr><tr><td>b8</td><td>7b</td><td>df</td><td>b5</td></tr></table>	ac	ef	13	45	c1	b5	23	73	d6	5a	cf	11	b8	7b	df	b5	<table><tr><td>75</td><td>20</td><td>53</td><td>bb</td></tr><tr><td>ec</td><td>0b</td><td>c0</td><td>25</td></tr><tr><td>09</td><td>63</td><td>cf</td><td>d0</td></tr><tr><td>93</td><td>33</td><td>7c</td><td>dc</td></tr></table>	75	20	53	bb	ec	0b	c0	25	09	63	cf	d0	93	33	7c	dc	<table><tr><td>3d</td><td>47</td><td>1e</td><td>6d</td></tr><tr><td>80</td><td>16</td><td>23</td><td>7a</td></tr><tr><td>47</td><td>fe</td><td>7e</td><td>88</td></tr><tr><td>7d</td><td>3e</td><td>44</td><td>3b</td></tr></table> ⊕=	3d	47	1e	6d	80	16	23	7a	47	fe	7e	88	7d	3e	44	3b
	aa	61	82	68																																																																																	
	8f	dd	d2	32																																																																																	
	5f	e3	4a	46																																																																																	
	03	ef	d2	9a																																																																																	
ac	ef	13	45																																																																																		
73	c1	b5	23																																																																																		
cf	11	d6	5a																																																																																		
7b	df	b5	b8																																																																																		
ac	ef	13	45																																																																																		
c1	b5	23	73																																																																																		
d6	5a	cf	11																																																																																		
b8	7b	df	b5																																																																																		
75	20	53	bb																																																																																		
ec	0b	c0	25																																																																																		
09	63	cf	d0																																																																																		
93	33	7c	dc																																																																																		
3d	47	1e	6d																																																																																		
80	16	23	7a																																																																																		
47	fe	7e	88																																																																																		
7d	3e	44	3b																																																																																		
4	<table><tr><td>48</td><td>67</td><td>4d</td><td>d6</td></tr><tr><td>6c</td><td>1d</td><td>e3</td><td>5f</td></tr><tr><td>4e</td><td>9d</td><td>b1</td><td>58</td></tr><tr><td>ee</td><td>0d</td><td>38</td><td>e7</td></tr></table>	48	67	4d	d6	6c	1d	e3	5f	4e	9d	b1	58	ee	0d	38	e7	<table><tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr><tr><td>50</td><td>a4</td><td>11</td><td>cf</td></tr><tr><td>2f</td><td>5e</td><td>c8</td><td>6a</td></tr><tr><td>28</td><td>d7</td><td>07</td><td>94</td></tr></table>	52	85	e3	f6	50	a4	11	cf	2f	5e	c8	6a	28	d7	07	94	<table><tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr><tr><td>a4</td><td>11</td><td>cf</td><td>50</td></tr><tr><td>c8</td><td>6a</td><td>2f</td><td>5e</td></tr><tr><td>94</td><td>28</td><td>d7</td><td>07</td></tr></table>	52	85	e3	f6	a4	11	cf	50	c8	6a	2f	5e	94	28	d7	07	<table><tr><td>0f</td><td>60</td><td>6f</td><td>5e</td></tr><tr><td>d6</td><td>31</td><td>c0</td><td>b3</td></tr><tr><td>da</td><td>38</td><td>10</td><td>13</td></tr><tr><td>a9</td><td>bf</td><td>6b</td><td>01</td></tr></table>	0f	60	6f	5e	d6	31	c0	b3	da	38	10	13	a9	bf	6b	01	<table><tr><td>ef</td><td>a8</td><td>b6</td><td>db</td></tr><tr><td>44</td><td>52</td><td>71</td><td>0b</td></tr><tr><td>a5</td><td>5b</td><td>25</td><td>ad</td></tr><tr><td>41</td><td>7f</td><td>3b</td><td>00</td></tr></table> ⊕=	ef	a8	b6	db	44	52	71	0b	a5	5b	25	ad	41	7f	3b	00
	48	67	4d	d6																																																																																	
	6c	1d	e3	5f																																																																																	
	4e	9d	b1	58																																																																																	
	ee	0d	38	e7																																																																																	
52	85	e3	f6																																																																																		
50	a4	11	cf																																																																																		
2f	5e	c8	6a																																																																																		
28	d7	07	94																																																																																		
52	85	e3	f6																																																																																		
a4	11	cf	50																																																																																		
c8	6a	2f	5e																																																																																		
94	28	d7	07																																																																																		
0f	60	6f	5e																																																																																		
d6	31	c0	b3																																																																																		
da	38	10	13																																																																																		
a9	bf	6b	01																																																																																		
ef	a8	b6	db																																																																																		
44	52	71	0b																																																																																		
a5	5b	25	ad																																																																																		
41	7f	3b	00																																																																																		
5	<table><tr><td>e0</td><td>c8</td><td>d9</td><td>85</td></tr><tr><td>92</td><td>63</td><td>b1</td><td>b8</td></tr><tr><td>7f</td><td>63</td><td>35</td><td>be</td></tr><tr><td>e8</td><td>c0</td><td>50</td><td>01</td></tr></table>	e0	c8	d9	85	92	63	b1	b8	7f	63	35	be	e8	c0	50	01	<table><tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr><tr><td>4f</td><td>fb</td><td>c8</td><td>6c</td></tr><tr><td>d2</td><td>fb</td><td>96</td><td>ae</td></tr><tr><td>9b</td><td>ba</td><td>53</td><td>7c</td></tr></table>	e1	e8	35	97	4f	fb	c8	6c	d2	fb	96	ae	9b	ba	53	7c	<table><tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr><tr><td>fb</td><td>c8</td><td>6c</td><td>4f</td></tr><tr><td>96</td><td>ae</td><td>d2</td><td>fb</td></tr><tr><td>7c</td><td>9b</td><td>ba</td><td>53</td></tr></table>	e1	e8	35	97	fb	c8	6c	4f	96	ae	d2	fb	7c	9b	ba	53	<table><tr><td>25</td><td>bd</td><td>b6</td><td>4c</td></tr><tr><td>d1</td><td>11</td><td>3a</td><td>4c</td></tr><tr><td>a9</td><td>d1</td><td>33</td><td>c0</td></tr><tr><td>ad</td><td>68</td><td>8e</td><td>b0</td></tr></table>	25	bd	b6	4c	d1	11	3a	4c	a9	d1	33	c0	ad	68	8e	b0	<table><tr><td>d4</td><td>7c</td><td>ca</td><td>11</td></tr><tr><td>d1</td><td>83</td><td>f2</td><td>f9</td></tr><tr><td>c6</td><td>9d</td><td>b8</td><td>15</td></tr><tr><td>f8</td><td>87</td><td>bc</td><td>bc</td></tr></table> ⊕=	d4	7c	ca	11	d1	83	f2	f9	c6	9d	b8	15	f8	87	bc	bc
	e0	c8	d9	85																																																																																	
	92	63	b1	b8																																																																																	
	7f	63	35	be																																																																																	
	e8	c0	50	01																																																																																	
e1	e8	35	97																																																																																		
4f	fb	c8	6c																																																																																		
d2	fb	96	ae																																																																																		
9b	ba	53	7c																																																																																		
e1	e8	35	97																																																																																		
fb	c8	6c	4f																																																																																		
96	ae	d2	fb																																																																																		
7c	9b	ba	53																																																																																		
25	bd	b6	4c																																																																																		
d1	11	3a	4c																																																																																		
a9	d1	33	c0																																																																																		
ad	68	8e	b0																																																																																		
d4	7c	ca	11																																																																																		
d1	83	f2	f9																																																																																		
c6	9d	b8	15																																																																																		
f8	87	bc	bc																																																																																		

6	<table><tr><td>f1</td><td>c1</td><td>7c</td><td>5d</td></tr><tr><td>00</td><td>92</td><td>c8</td><td>b5</td></tr><tr><td>6f</td><td>4c</td><td>8b</td><td>d5</td></tr><tr><td>55</td><td>ef</td><td>32</td><td>0c</td></tr></table>	f1	c1	7c	5d	00	92	c8	b5	6f	4c	8b	d5	55	ef	32	0c	<table><tr><td>a1</td><td>78</td><td>10</td><td>4c</td></tr><tr><td>63</td><td>4f</td><td>e8</td><td>d5</td></tr><tr><td>a8</td><td>29</td><td>3d</td><td>03</td></tr><tr><td>fc</td><td>df</td><td>23</td><td>fe</td></tr></table>	a1	78	10	4c	63	4f	e8	d5	a8	29	3d	03	fc	df	23	fe	<table><tr><td>a1</td><td>78</td><td>10</td><td>4c</td></tr><tr><td>4f</td><td>e8</td><td>d5</td><td>63</td></tr><tr><td>3d</td><td>03</td><td>a8</td><td>29</td></tr><tr><td>fe</td><td>fc</td><td>df</td><td>23</td></tr></table>	a1	78	10	4c	4f	e8	d5	63	3d	03	a8	29	fe	fc	df	23	<table><tr><td>4b</td><td>2c</td><td>33</td><td>37</td></tr><tr><td>86</td><td>4a</td><td>9d</td><td>d2</td></tr><tr><td>8d</td><td>89</td><td>f4</td><td>18</td></tr><tr><td>6d</td><td>80</td><td>e8</td><td>d8</td></tr></table>	4b	2c	33	37	86	4a	9d	d2	8d	89	f4	18	6d	80	e8	d8	<table><tr><td>6d</td><td>11</td><td>db</td><td>ca</td></tr><tr><td>88</td><td>0b</td><td>f9</td><td>00</td></tr><tr><td>a3</td><td>3e</td><td>86</td><td>93</td></tr><tr><td>7a</td><td>fd</td><td>41</td><td>fd</td></tr></table>	6d	11	db	ca	88	0b	f9	00	a3	3e	86	93	7a	fd	41	fd	⊕	=
	f1	c1	7c	5d																																																																																			
	00	92	c8	b5																																																																																			
	6f	4c	8b	d5																																																																																			
55	ef	32	0c																																																																																				
a1	78	10	4c																																																																																				
63	4f	e8	d5																																																																																				
a8	29	3d	03																																																																																				
fc	df	23	fe																																																																																				
a1	78	10	4c																																																																																				
4f	e8	d5	63																																																																																				
3d	03	a8	29																																																																																				
fe	fc	df	23																																																																																				
4b	2c	33	37																																																																																				
86	4a	9d	d2																																																																																				
8d	89	f4	18																																																																																				
6d	80	e8	d8																																																																																				
6d	11	db	ca																																																																																				
88	0b	f9	00																																																																																				
a3	3e	86	93																																																																																				
7a	fd	41	fd																																																																																				
7	<table><tr><td>26</td><td>3d</td><td>e8</td><td>fd</td></tr><tr><td>0e</td><td>41</td><td>64</td><td>d2</td></tr><tr><td>2e</td><td>b7</td><td>72</td><td>8b</td></tr><tr><td>17</td><td>7d</td><td>a9</td><td>25</td></tr></table>	26	3d	e8	fd	0e	41	64	d2	2e	b7	72	8b	17	7d	a9	25	<table><tr><td>f7</td><td>27</td><td>9b</td><td>54</td></tr><tr><td>ab</td><td>83</td><td>43</td><td>b5</td></tr><tr><td>31</td><td>a9</td><td>40</td><td>3d</td></tr><tr><td>f0</td><td>ff</td><td>d3</td><td>3f</td></tr></table>	f7	27	9b	54	ab	83	43	b5	31	a9	40	3d	f0	ff	d3	3f	<table><tr><td>f7</td><td>27</td><td>9b</td><td>54</td></tr><tr><td>83</td><td>43</td><td>b5</td><td>ab</td></tr><tr><td>40</td><td>3d</td><td>31</td><td>a9</td></tr><tr><td>3f</td><td>f0</td><td>ff</td><td>d3</td></tr></table>	f7	27	9b	54	83	43	b5	ab	40	3d	31	a9	3f	f0	ff	d3	<table><tr><td>14</td><td>46</td><td>27</td><td>34</td></tr><tr><td>15</td><td>16</td><td>46</td><td>2a</td></tr><tr><td>b5</td><td>15</td><td>56</td><td>d8</td></tr><tr><td>bf</td><td>ec</td><td>d7</td><td>43</td></tr></table>	14	46	27	34	15	16	46	2a	b5	15	56	d8	bf	ec	d7	43	<table><tr><td>4e</td><td>5f</td><td>84</td><td>4e</td></tr><tr><td>54</td><td>5f</td><td>a6</td><td>a6</td></tr><tr><td>f7</td><td>c9</td><td>4f</td><td>dc</td></tr><tr><td>0e</td><td>f3</td><td>b2</td><td>4f</td></tr></table>	4e	5f	84	4e	54	5f	a6	a6	f7	c9	4f	dc	0e	f3	b2	4f	⊕	=
	26	3d	e8	fd																																																																																			
	0e	41	64	d2																																																																																			
	2e	b7	72	8b																																																																																			
17	7d	a9	25																																																																																				
f7	27	9b	54																																																																																				
ab	83	43	b5																																																																																				
31	a9	40	3d																																																																																				
f0	ff	d3	3f																																																																																				
f7	27	9b	54																																																																																				
83	43	b5	ab																																																																																				
40	3d	31	a9																																																																																				
3f	f0	ff	d3																																																																																				
14	46	27	34																																																																																				
15	16	46	2a																																																																																				
b5	15	56	d8																																																																																				
bf	ec	d7	43																																																																																				
4e	5f	84	4e																																																																																				
54	5f	a6	a6																																																																																				
f7	c9	4f	dc																																																																																				
0e	f3	b2	4f																																																																																				
8	<table><tr><td>5a</td><td>19</td><td>a3</td><td>7a</td></tr><tr><td>41</td><td>49</td><td>e0</td><td>8c</td></tr><tr><td>42</td><td>dc</td><td>19</td><td>04</td></tr><tr><td>b1</td><td>1f</td><td>65</td><td>0c</td></tr></table>	5a	19	a3	7a	41	49	e0	8c	42	dc	19	04	b1	1f	65	0c	<table><tr><td>be</td><td>d4</td><td>0a</td><td>da</td></tr><tr><td>83</td><td>3b</td><td>e1</td><td>64</td></tr><tr><td>2c</td><td>86</td><td>d4</td><td>f2</td></tr><tr><td>c8</td><td>c0</td><td>4d</td><td>fe</td></tr></table>	be	d4	0a	da	83	3b	e1	64	2c	86	d4	f2	c8	c0	4d	fe	<table><tr><td>be</td><td>d4</td><td>0a</td><td>da</td></tr><tr><td>3b</td><td>e1</td><td>64</td><td>83</td></tr><tr><td>d4</td><td>f2</td><td>2c</td><td>86</td></tr><tr><td>fe</td><td>c8</td><td>c0</td><td>4d</td></tr></table>	be	d4	0a	da	3b	e1	64	83	d4	f2	2c	86	fe	c8	c0	4d	<table><tr><td>00</td><td>b1</td><td>54</td><td>fa</td></tr><tr><td>51</td><td>c8</td><td>76</td><td>1b</td></tr><tr><td>2f</td><td>89</td><td>6d</td><td>99</td></tr><tr><td>d1</td><td>ff</td><td>cd</td><td>ea</td></tr></table>	00	b1	54	fa	51	c8	76	1b	2f	89	6d	99	d1	ff	cd	ea	<table><tr><td>ea</td><td>b5</td><td>31</td><td>7f</td></tr><tr><td>d2</td><td>8d</td><td>2b</td><td>8d</td></tr><tr><td>73</td><td>ba</td><td>f5</td><td>29</td></tr><tr><td>21</td><td>d2</td><td>60</td><td>2f</td></tr></table>	ea	b5	31	7f	d2	8d	2b	8d	73	ba	f5	29	21	d2	60	2f	⊕	=
	5a	19	a3	7a																																																																																			
	41	49	e0	8c																																																																																			
	42	dc	19	04																																																																																			
b1	1f	65	0c																																																																																				
be	d4	0a	da																																																																																				
83	3b	e1	64																																																																																				
2c	86	d4	f2																																																																																				
c8	c0	4d	fe																																																																																				
be	d4	0a	da																																																																																				
3b	e1	64	83																																																																																				
d4	f2	2c	86																																																																																				
fe	c8	c0	4d																																																																																				
00	b1	54	fa																																																																																				
51	c8	76	1b																																																																																				
2f	89	6d	99																																																																																				
d1	ff	cd	ea																																																																																				
ea	b5	31	7f																																																																																				
d2	8d	2b	8d																																																																																				
73	ba	f5	29																																																																																				
21	d2	60	2f																																																																																				
9	<table><tr><td>ea</td><td>04</td><td>65</td><td>85</td></tr><tr><td>83</td><td>45</td><td>5d</td><td>96</td></tr><tr><td>5c</td><td>33</td><td>98</td><td>b0</td></tr><tr><td>f0</td><td>2d</td><td>ad</td><td>c5</td></tr></table>	ea	04	65	85	83	45	5d	96	5c	33	98	b0	f0	2d	ad	c5	<table><tr><td>87</td><td>f2</td><td>4d</td><td>97</td></tr><tr><td>ec</td><td>6e</td><td>4c</td><td>90</td></tr><tr><td>4a</td><td>c3</td><td>46</td><td>e7</td></tr><tr><td>8c</td><td>d8</td><td>95</td><td>a6</td></tr></table>	87	f2	4d	97	ec	6e	4c	90	4a	c3	46	e7	8c	d8	95	a6	<table><tr><td>87</td><td>f2</td><td>4d</td><td>97</td></tr><tr><td>6e</td><td>4c</td><td>90</td><td>ec</td></tr><tr><td>46</td><td>e7</td><td>4a</td><td>c3</td></tr><tr><td>a6</td><td>8c</td><td>d8</td><td>95</td></tr></table>	87	f2	4d	97	6e	4c	90	ec	46	e7	4a	c3	a6	8c	d8	95	<table><tr><td>47</td><td>40</td><td>a3</td><td>4c</td></tr><tr><td>37</td><td>d4</td><td>70</td><td>9f</td></tr><tr><td>94</td><td>e4</td><td>3a</td><td>42</td></tr><tr><td>ed</td><td>a5</td><td>a6</td><td>bc</td></tr></table>	47	40	a3	4c	37	d4	70	9f	94	e4	3a	42	ed	a5	a6	bc	<table><tr><td>ac</td><td>19</td><td>28</td><td>57</td></tr><tr><td>77</td><td>fa</td><td>d1</td><td>5c</td></tr><tr><td>66</td><td>dc</td><td>29</td><td>00</td></tr><tr><td>f3</td><td>21</td><td>41</td><td>6e</td></tr></table>	ac	19	28	57	77	fa	d1	5c	66	dc	29	00	f3	21	41	6e	⊕	=
	ea	04	65	85																																																																																			
	83	45	5d	96																																																																																			
	5c	33	98	b0																																																																																			
f0	2d	ad	c5																																																																																				
87	f2	4d	97																																																																																				
ec	6e	4c	90																																																																																				
4a	c3	46	e7																																																																																				
8c	d8	95	a6																																																																																				
87	f2	4d	97																																																																																				
6e	4c	90	ec																																																																																				
46	e7	4a	c3																																																																																				
a6	8c	d8	95																																																																																				
47	40	a3	4c																																																																																				
37	d4	70	9f																																																																																				
94	e4	3a	42																																																																																				
ed	a5	a6	bc																																																																																				
ac	19	28	57																																																																																				
77	fa	d1	5c																																																																																				
66	dc	29	00																																																																																				
f3	21	41	6e																																																																																				
10	<table><tr><td>eb</td><td>59</td><td>8b</td><td>1b</td></tr><tr><td>40</td><td>2e</td><td>a1</td><td>c3</td></tr><tr><td>f2</td><td>38</td><td>13</td><td>42</td></tr><tr><td>1e</td><td>84</td><td>e7</td><td>d2</td></tr></table>	eb	59	8b	1b	40	2e	a1	c3	f2	38	13	42	1e	84	e7	d2	<table><tr><td>e9</td><td>cb</td><td>3d</td><td>af</td></tr><tr><td>09</td><td>31</td><td>32</td><td>2e</td></tr><tr><td>89</td><td>07</td><td>7d</td><td>2c</td></tr><tr><td>72</td><td>5f</td><td>94</td><td>b5</td></tr></table>	e9	cb	3d	af	09	31	32	2e	89	07	7d	2c	72	5f	94	b5	<table><tr><td>e9</td><td>cb</td><td>3d</td><td>af</td></tr><tr><td>31</td><td>32</td><td>2e</td><td>09</td></tr><tr><td>7d</td><td>2c</td><td>89</td><td>07</td></tr><tr><td>b5</td><td>72</td><td>5f</td><td>94</td></tr></table>	e9	cb	3d	af	31	32	2e	09	7d	2c	89	07	b5	72	5f	94	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table><tr><td>d0</td><td>c9</td><td>e1</td><td>b6</td></tr><tr><td>14</td><td>ee</td><td>3f</td><td>63</td></tr><tr><td>f9</td><td>25</td><td>0c</td><td>0c</td></tr><tr><td>a8</td><td>89</td><td>c8</td><td>a6</td></tr></table>	d0	c9	e1	b6	14	ee	3f	63	f9	25	0c	0c	a8	89	c8	a6	⊕	=
	eb	59	8b	1b																																																																																			
	40	2e	a1	c3																																																																																			
	f2	38	13	42																																																																																			
1e	84	e7	d2																																																																																				
e9	cb	3d	af																																																																																				
09	31	32	2e																																																																																				
89	07	7d	2c																																																																																				
72	5f	94	b5																																																																																				
e9	cb	3d	af																																																																																				
31	32	2e	09																																																																																				
7d	2c	89	07																																																																																				
b5	72	5f	94																																																																																				
d0	c9	e1	b6																																																																																				
14	ee	3f	63																																																																																				
f9	25	0c	0c																																																																																				
a8	89	c8	a6																																																																																				
output	<table><tr><td>39</td><td>02</td><td>dc</td><td>19</td></tr><tr><td>25</td><td>dc</td><td>11</td><td>6a</td></tr><tr><td>84</td><td>09</td><td>85</td><td>0b</td></tr><tr><td>1d</td><td>fb</td><td>97</td><td>32</td></tr></table>	39	02	dc	19	25	dc	11	6a	84	09	85	0b	1d	fb	97	32	<div>* test vector</div>																																																																					
39	02	dc	19																																																																																				
25	dc	11	6a																																																																																				
84	09	85	0b																																																																																				
1d	fb	97	32																																																																																				

Q & A

