

컴퓨터시스템보안

AES



목차

- 1. AES란?**
- 2. AES 원리**
- 3. 장점**

1. AES란?



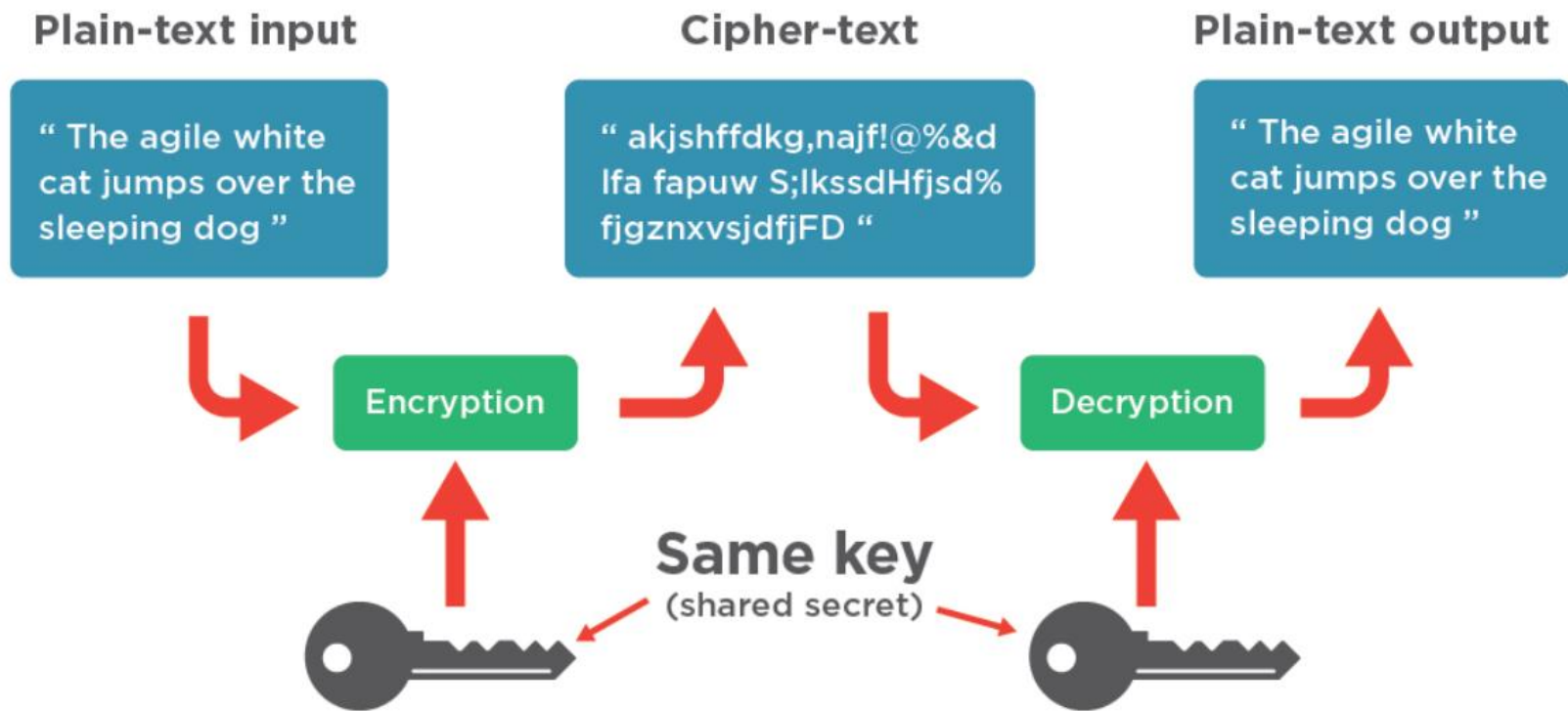
1. AES란?

AES(Advanced Encryption Standard)

- DES의 한계 → 1997년 NIST(미국표준기술연구소) AES알고리즘 공모
- 조건 : 30년 사용가능한 안정성, 128bit 암호블록, 다양한 키의 길이
- Rijmen과 Daemen 개발한 Rijndael 알고리즘 선정(벨기에)
암호화표준(2001년 11월 FIPS-197)
- 평문 입력 : 128bit key 길이 : 128, 192, 256비트 선택

1. AES란?

대칭키 암호 시스템



2. AES 원리



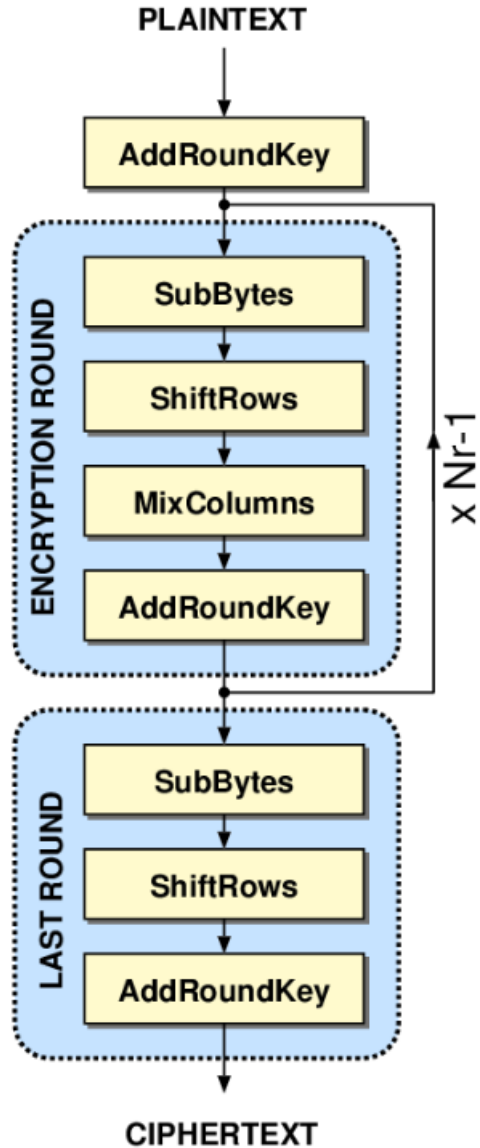
2. AES원리 기본이론

평문 → 128bit → 4X4 행렬

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

- 다항식 연산(덧셈 , 곱셈)
- XOR, MOD
- 소프트웨어상 좋은 성능을 가능하게 함

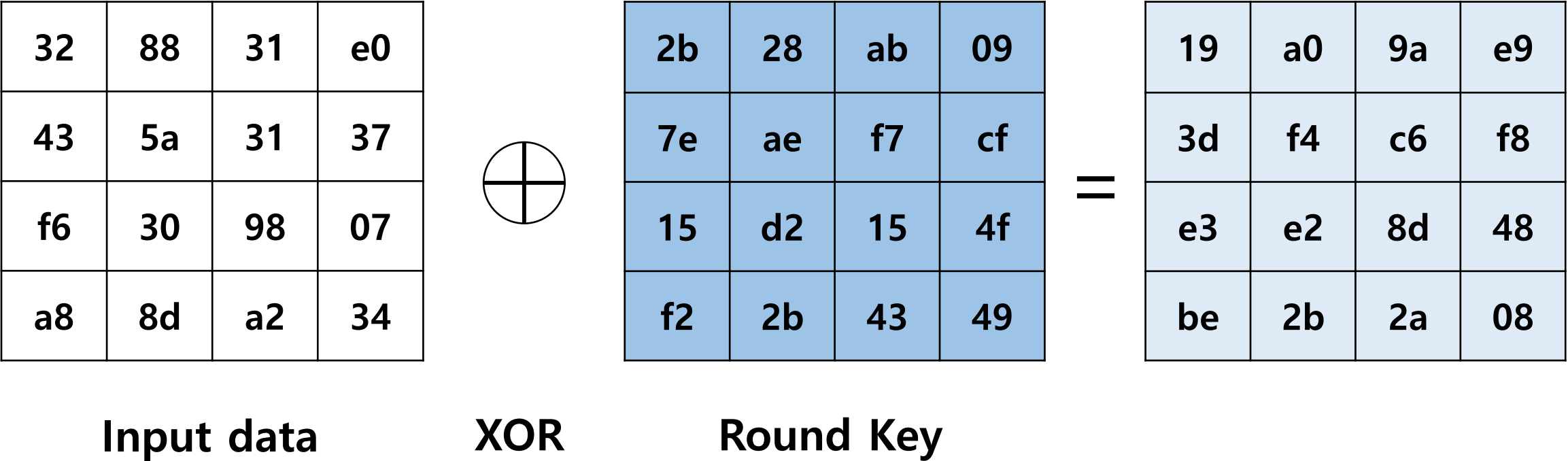
2. AES원리 기본이론

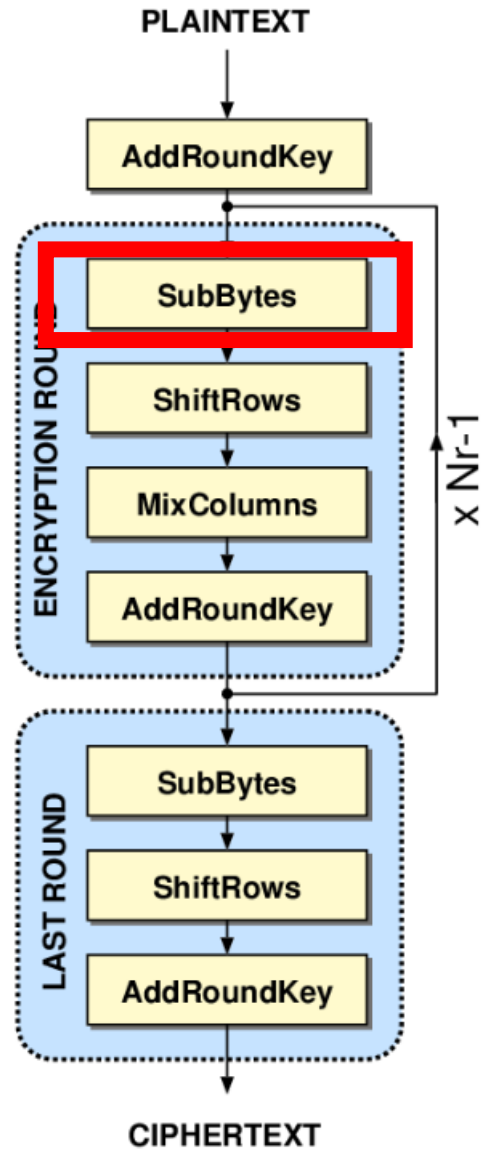


	키 길이 (Nk Word)	블록길이 (Nb Word)	라운드 수 (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

- 각 round는 비선형성 S-BOX 적용
- 마지막 round에 MixColumns 연산을 제외

1. Add Round Key (Round 0)





- 암호문의 비 선형성 제공
- 바이트단위 역변환 가능한 S-BOX 적용

2. Sub Bytes (Round 1)

d4	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	3	7	2b	fe	d7	ab	76	
1	ca	82	c9	7d	fa	59	47	f0	a	d4	2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	3	5	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 (byte substitution table)

2. Sub Bytes (Round 1)

19	a0	9a	e9
27	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	7	1	15	
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	e	27	2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	2	8	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 (byte substitution table)

2. Sub Bytes (Round 1)

19	a0	9a	e9
3d	f4	c6	f8
11	e2	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	b	8	03	f6	0e	61	35	57	b9	86	c1	1d	9e	
e	e1	f8	9	11	9	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	8	5	ef	e6	42	68	41	99	2d	0f	b0	54	bb	16

S-BOX (byte substitution table)

2. Sub Bytes (Round 1)

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
ae	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	41	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7f	ae	8
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	b	a	
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 (byte substitution table)

2. Sub Bytes (Round 1)

19	e0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	1	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	
a	e0	2	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	8	3	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 (byte substitution table)

2. Sub Bytes (Round 1)

19	e0	9a	e9
3d	bf	c6	f8
e3	e2	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	1	9	8e	94	9b	1e	87	e9	ce	55	28	df	
f	8c	a1	89	0	bf	6	42	68	41	99	2d	0f	b0	54	bb	16

S-BOX (byte substitution table)

2. Sub Bytes (Round 1)

19	e0	9a	e9
3d	bf	c6	f8
e3	98	8d	48
be	2b	2a	08

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	3b	36	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e	
e	e1	f1	98	1	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	05	bd	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

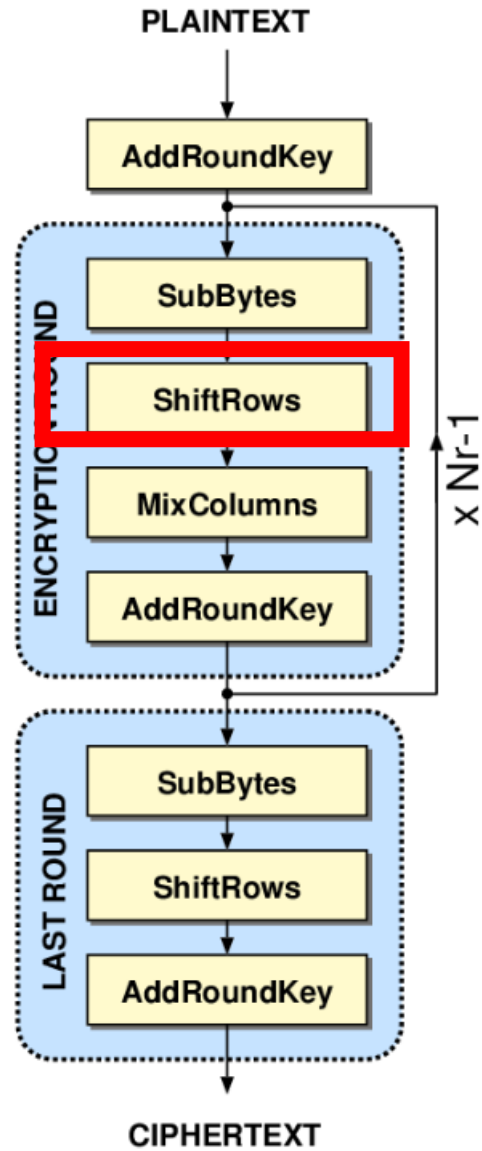
S-BOX (byte substitution table)

2. Sub Bytes (Round 1)

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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 (byte substitution table)



- 행단위 순환 Shift
- 왼쪽으로 이동
- 행마다 shift 수가 다름

3. Shift Rows (Round 1)

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

← 0 byte 왼쪽으로 회전

3. Shift Rows (Round 1)

d4	e0	b8	1e
bf	b4	41	27
11	98	5d	52
ae	f1	e5	30

← 1 byte 왼쪽으로 회전

3. Shift Rows (Round 1)

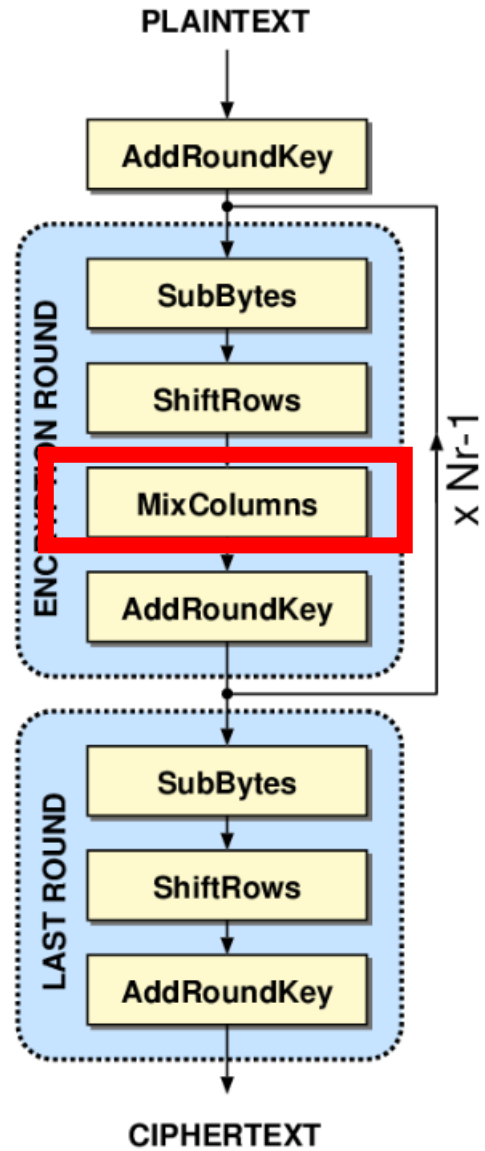
d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
ae	f1	e5	30

← 2 byte 왼쪽으로 회전

3. Shift Rows (Round 1)

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

← 3 byte 왼쪽으로 회전



- 열 단위의 혼합
- 확산 제공

4. Mix Columns (Round 1)

04	e0	b8	1e
66	b4	41	27
81	52	11	98
e5	ae	f1	e5

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} d4 \\ bf \\ 5d \\ 30 \end{pmatrix}$$

4. Mix Columns (Round 1)

04	e0	b8	1e
66	cb	41	27
81	19	11	98
e5	9a	f1	e5

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} e0 \\ b4 \\ 52 \\ ae \end{pmatrix}$$

4. Mix Columns (Round 1)

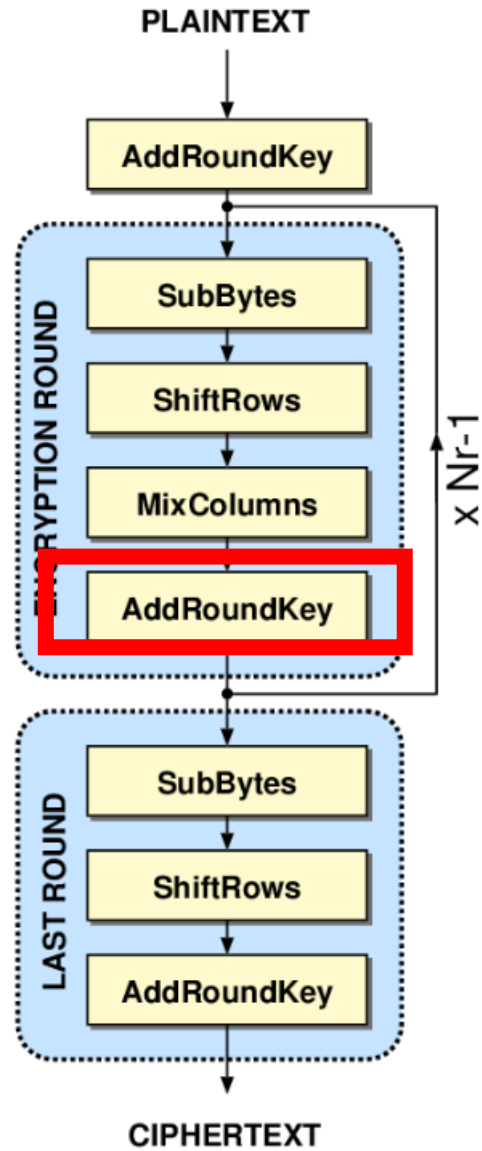
04	e0	48	1e
66	cb	f8	27
81	19	d3	98
e5	9a	7a	e5

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} b8 \\ 41 \\ 11 \\ f1 \end{pmatrix}$$

4. Mix Columns (Round 1)

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} 1e \\ 27 \\ 98 \\ e5 \end{pmatrix}$$



- Round 키와 XOR연산
- Round 키 \rightarrow 암호화 키 생산

- Round key schedule

0-Round key

2b	28	ab	09								
7e	ae	f7	cf								
15	d2	15	4f								
f2	2b	43	49								

cf
4f
49
09

1. 위로 한 칸씩 회전 (Shift)

Rcon

[illegible]

- Round key schedule

0-Round key

2b	28	ab	09								
7e	ae	f7	cf								
15	d2	15	4f								
f2	2b	43	49								



8a
84
eb
01

2. Sub Bytes 과정

Rcon

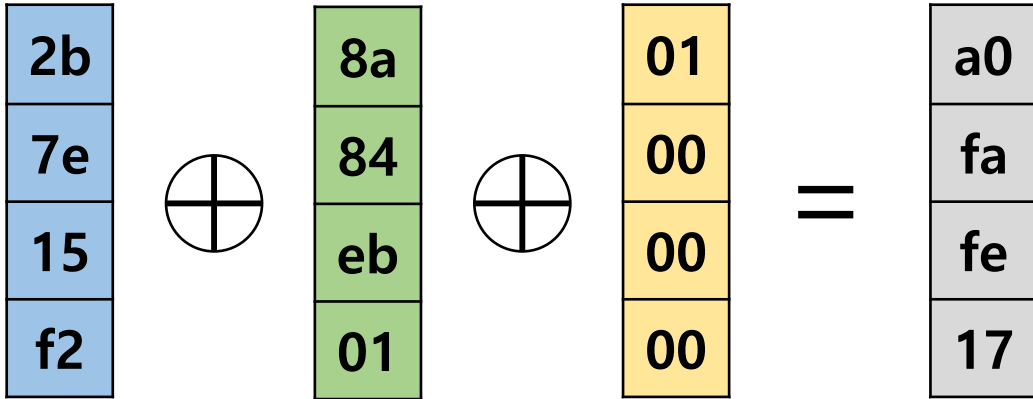
[illegible]

- Round key schedule

0-Round key

2b	28	ab	09	a0								
7e	ae	f7	cf	fa								
15	d2	15	4f	fe								
f2	2b	43	49	17								

● ● ●



3. XOR 연산

Rcon

[illegible]

- Round key schedule

0-Round key

2b	28	ab	09	a0	88						
7e	ae	f7	cf	fa	54						
15	d2	15	4f	fe	2c						
f2	2b	43	49	17	b1						

● ● ●

09	\oplus	a0	$=$	88
cf		fa		54
4f		fe		2c
49		17		b1

4. XOR 연산 반복

Rcon

[illegible]

- Round key schedule

0-Round key

1-Round key

2b	28	ab	09	a0	88	23	2a				
7e	ae	f7	cf	fa	54	a3	6c				
15	d2	15	4f	fe	2c	39	76				
f2	2b	43	49	17	b1	39	05				



Rcon

[illegible]

- Round key schedule

0-Round key				1-Round key							
2b	28	ab	09	a0	88	23	2a	f2			
7e	ae	f7	cf	fa	54	a3	6c	c2			
15	d2	15	4f	fe	2c	39	76	95			
f2	2b	43	49	17	b1	39	05	f2			

● ● ●

Diagram illustrating the XOR operation between two 4-bit values:

a0	50	02	f2
fa	38	00	c2
fe	6b	00	95
17	e5	00	f2

The operation is represented by a circle with a cross inside, and the result is shown with an equals sign.

Rcon

[illegible]

- Round key schedule

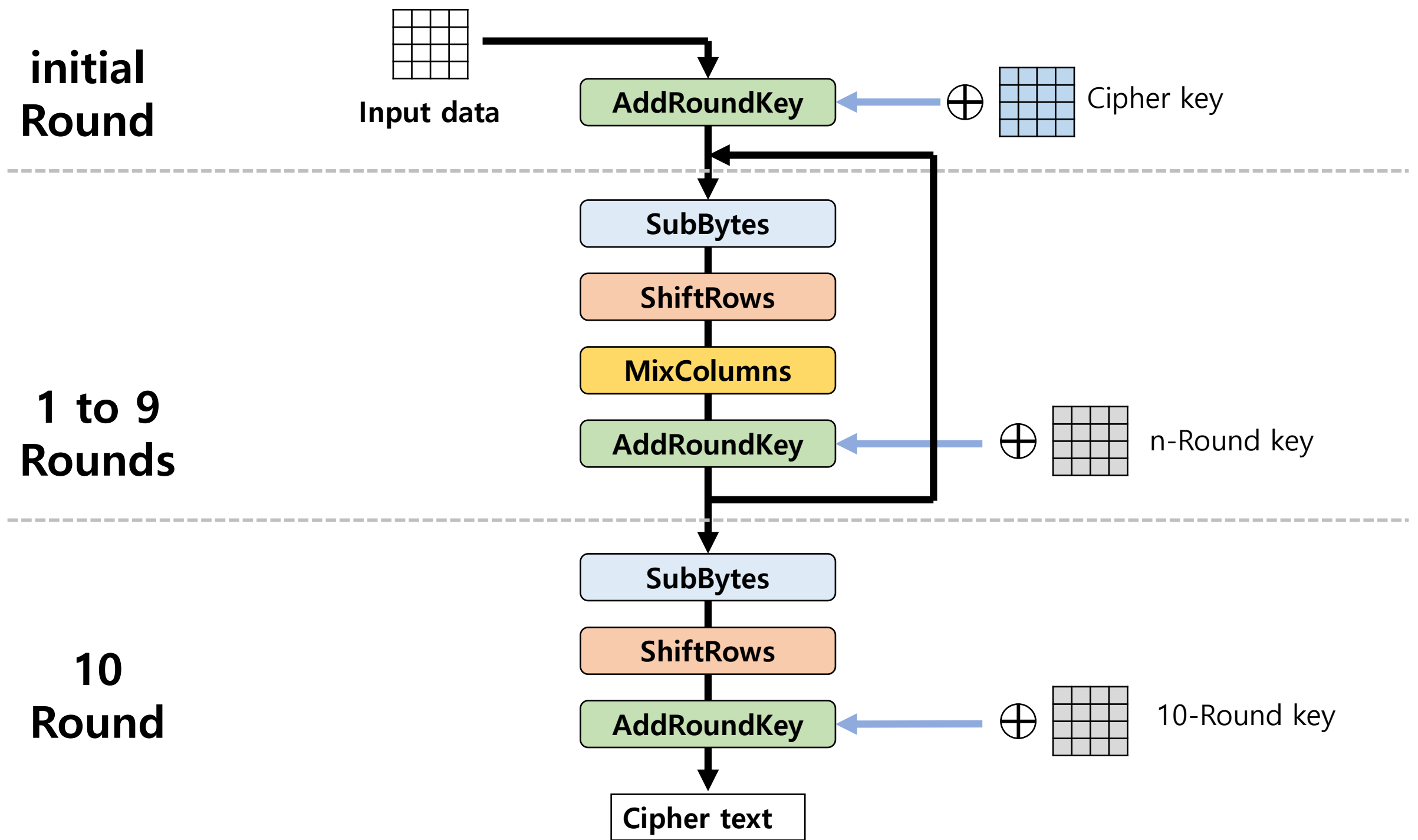
0-Round key				1-Round key				2-Round key			
2b	28	ab	09	a0	88	23	2a	f2	7a	59	73
7e	ae	f7	cf	fa	54	a3	6c	c2	96	35	59
15	d2	15	4f	fe	2c	39	76	95	b9	80	f6
f2	2b	43	49	17	b1	39	05	f2	43	7a	7f

● ● ●

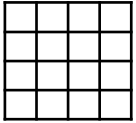
d0	c9	e1	b6
14	ee	3f	63
f9	25	0c	0c
a8	89	c8	a6

Rcon

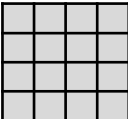
[illegible]



**initial
Round**


Cipher text

AddRoundKey

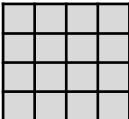
\oplus  10-Round key

**9 to 1
Rounds**

Inv_ShiftRows

Inv_SubBytes

AddRoundKey

\oplus  n-Round key

Inv_MixColumns

**10
Round**

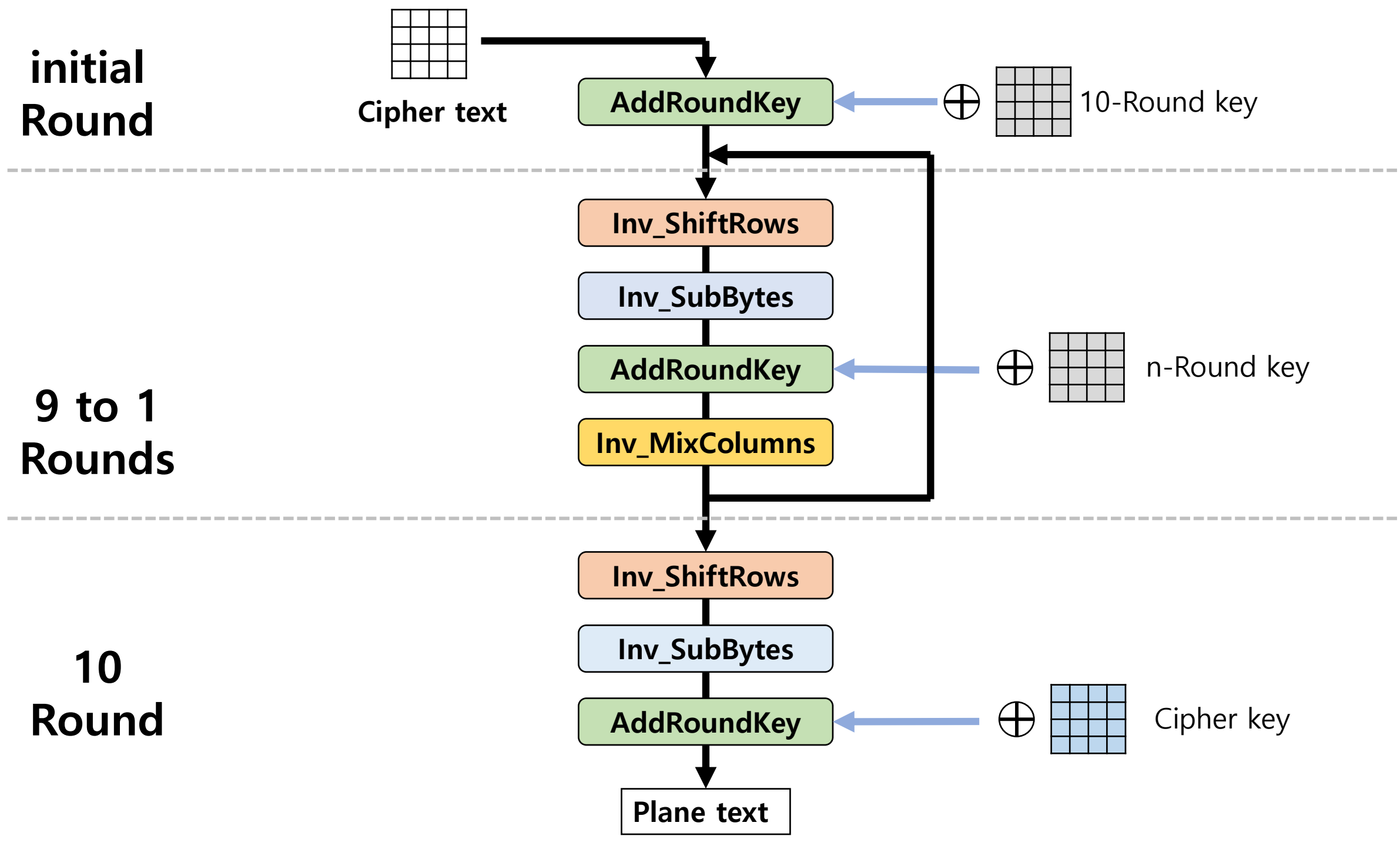
Inv_ShiftRows

Inv_SubBytes

AddRoundKey

\oplus  Cipher key

Plane text



3. 장점



3. 장점

AES(Advanced Encryption Standard)

- 다양한 키 길이의 제공 → 새로운 표준 제작 X
- 수학적 개념(다항식 군), 연산은 단순XOR, Shift → 소프트웨어적 빠른 동작 가능
- SEED,ARIA(국내 알고리즘) →표준이 아니므로 제품화 하여 수출 불가능

