AES 알고리즘

1771397 이민우

한성대학교 HANSUNG UNIVERSITY

유튜브 주소 : https://youtu.be/0IY1zzvWFFw

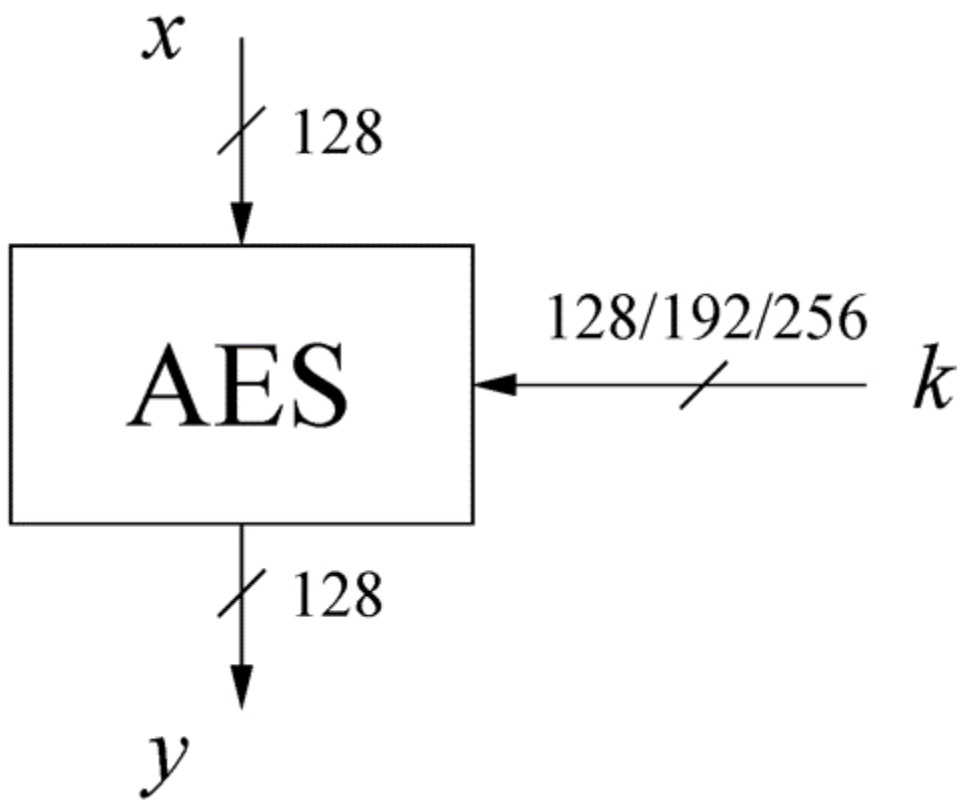
CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

AES 알고리즘 개요

- AES 입력 출력 과정

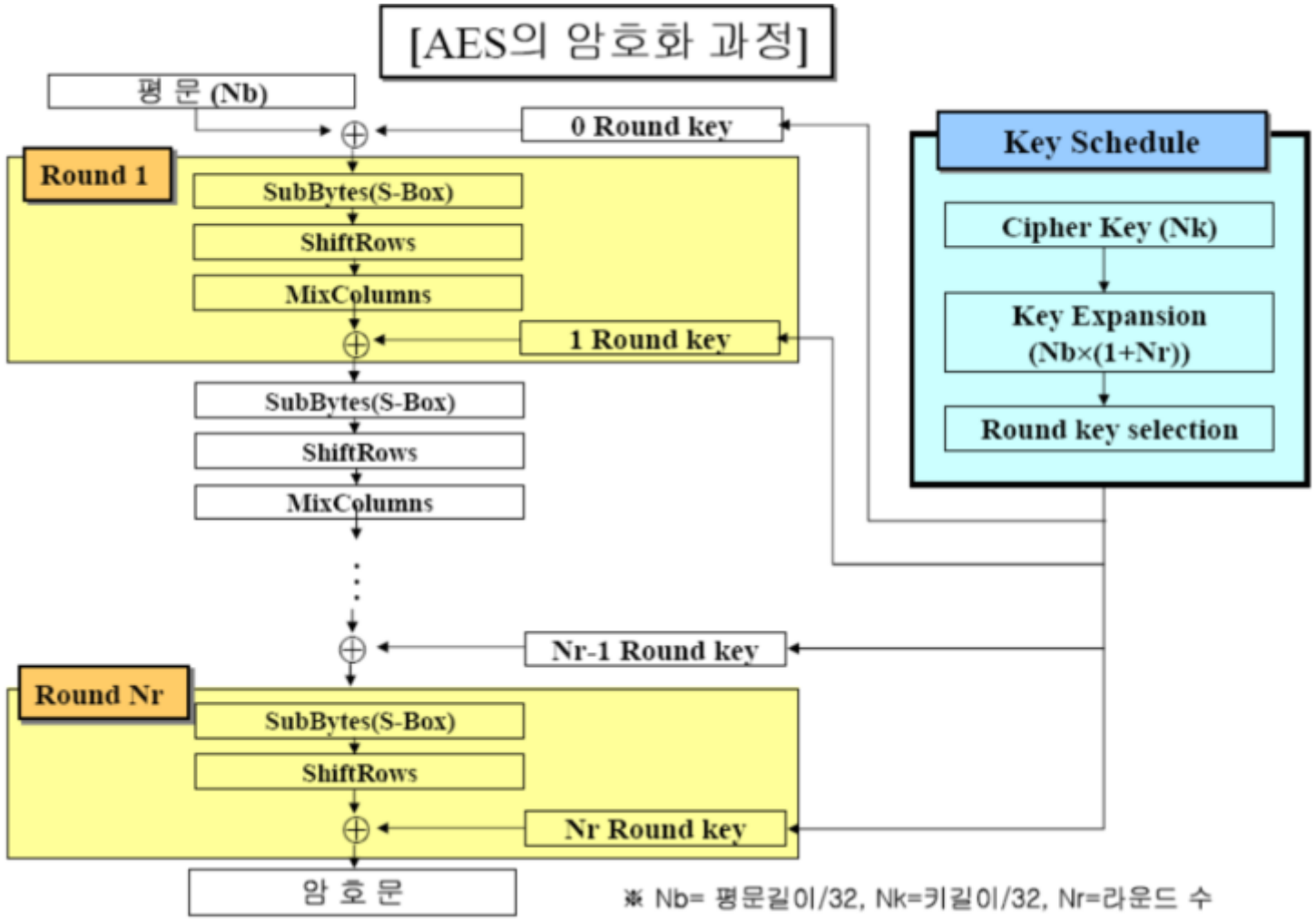


AES 알고리즘 개요

- 키 길이와 라운드 수

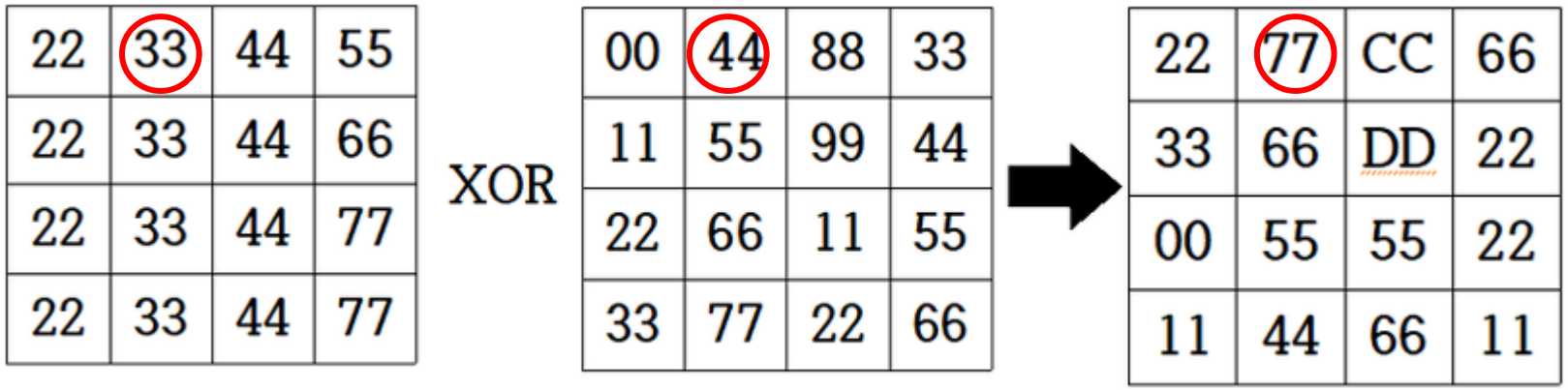
key lengths	# rounds = n_r
128 bit	10
192 bit	12
256 bit	14

AES 암호화 과정


[AES의 암호화 과정]
평 문 (Nb)
0 Round key
Round 1
SubBytes(S-Box)
ShiftRows
MixColumns
1 Round key
SubBytes(S-Box)
ShiftRows
MixColumns
Nr-1 Round key
Round Nr
SubBytes(S-Box)
ShiftRows
Nr Round key
암 호 문
Key Schedule
Cipher Key (Nk)
Key Expansion
(Nb×(1+Nr))
Round key selection
※ Nb= 평문길이/32, Nk=키길이/32, Nr=라운드 수

각 계층 동작 원리

- 키 덧셈 계층



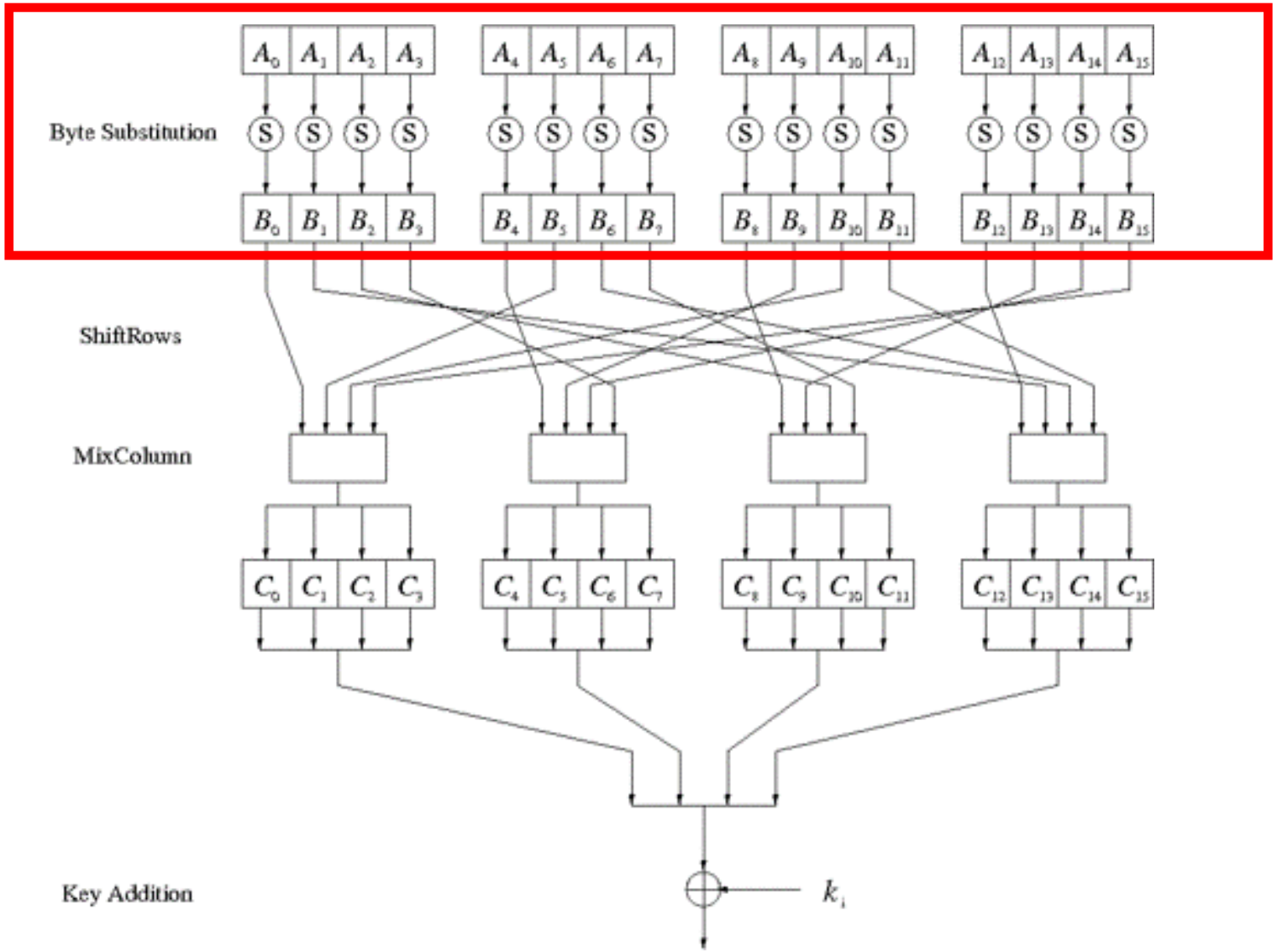
Ex) 33 ⊕ 44

00110011
⊕
01000100

01110111 = $77_{(16)}$

각 계층 동작 원리

- 바이트 환자 계층



A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

AES에서 데이터의 상태 (STATE) – 행렬 구조

각 계층 동작 원리

- S-box(substitution box)

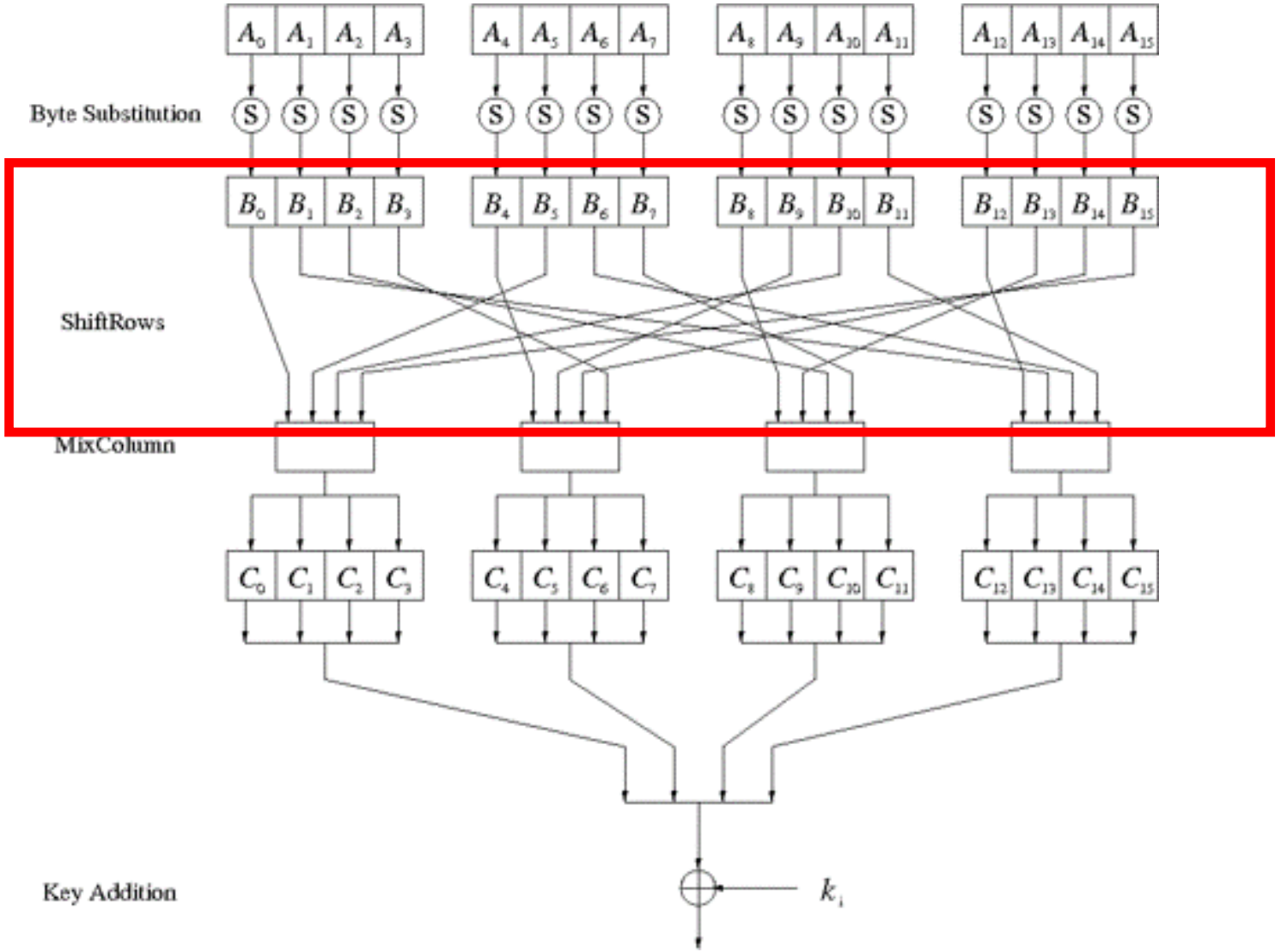
Ex) A7 -> 5C

		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

각 계층 동작 원리

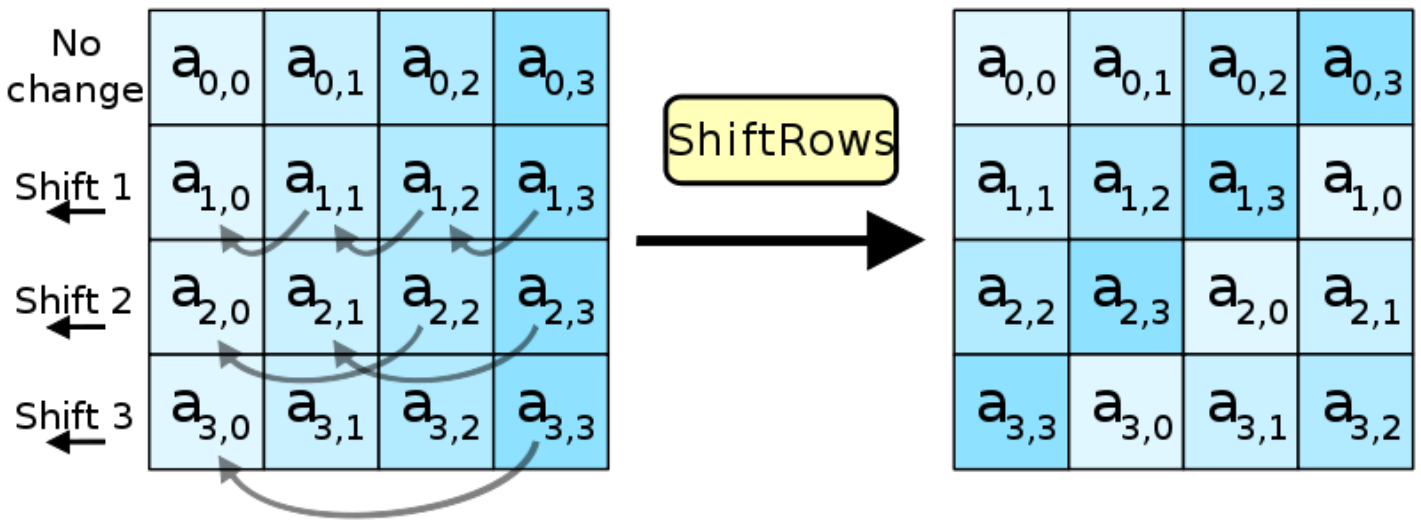
- Shift Rows 계층

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}



각 계층 동작 원리

- Shift Rows 계층

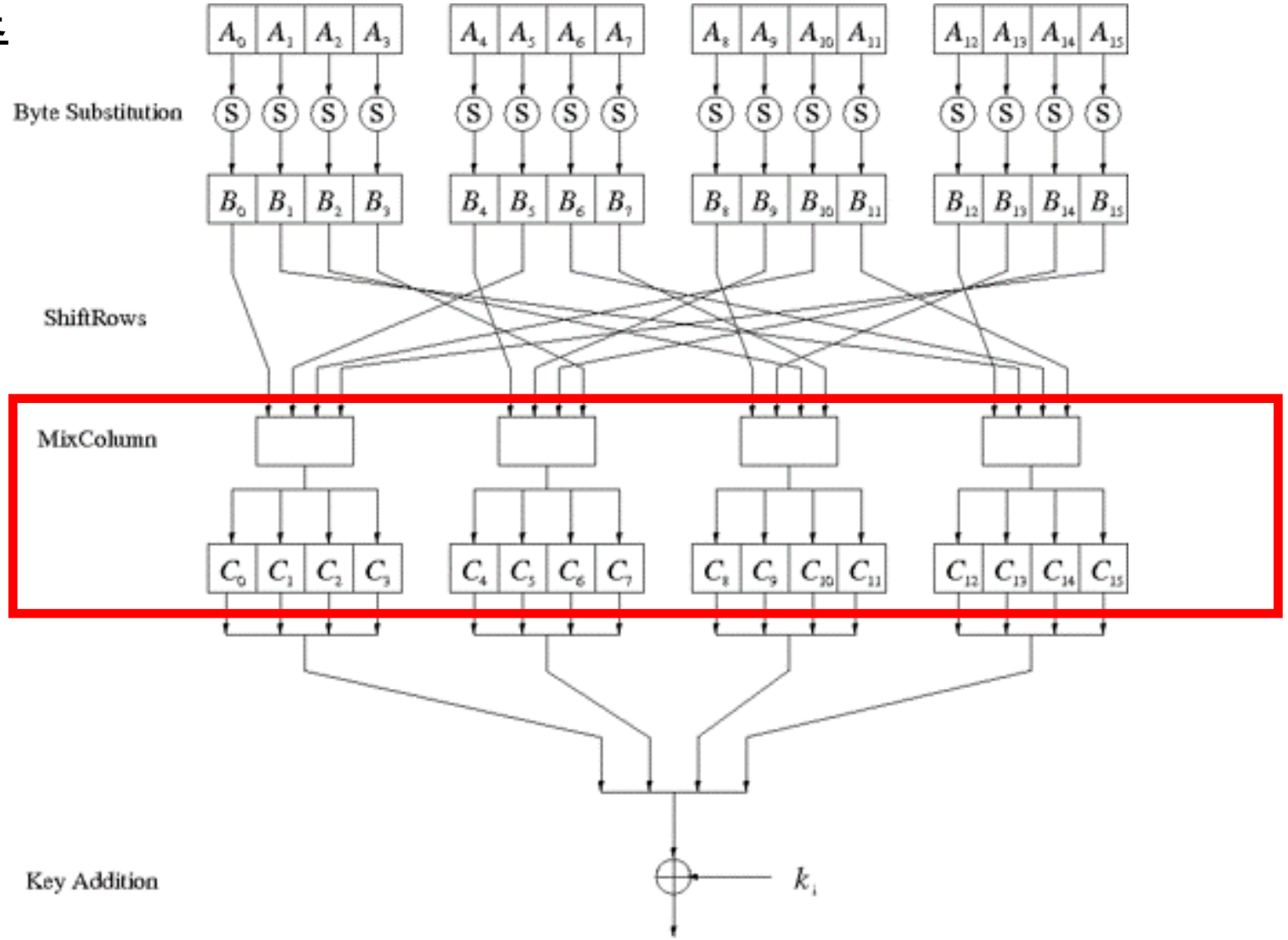


93	f5	4b	33
c3	33	c1	93
63	fc	fc	93
82	1b	33	82

93	f5	4b	33
33	c1	93	c3
fc	93	63	fc
82	82	1b	33

각 계층 동작 원리

- Mix Column 계층



각 계층 동작 원리

- Mix Column 계층

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

2*a0 + 3*a1 + 1*a2 + 1*a3 = b0

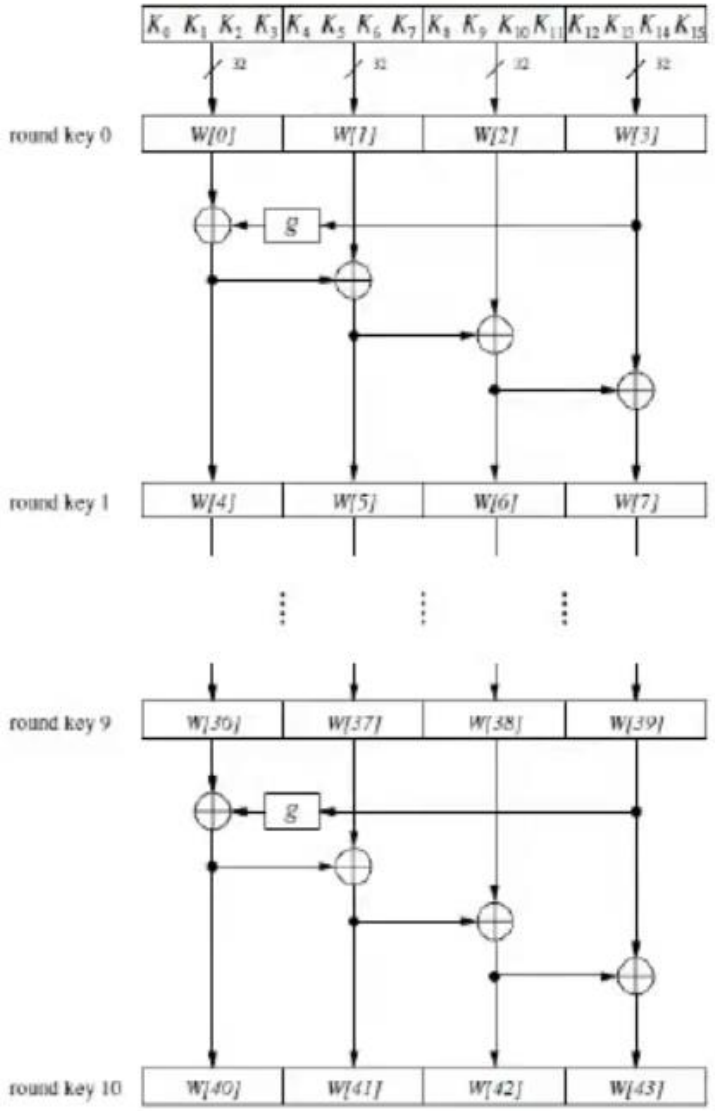
1*a0 + 2*a1 + 3*a2 + 1*a3 = b1

1*a0 + 1*a1 + 2*a2 + 3*a3 = b2

3*a0 + 1*a1 + 1*a2 + 2*a3 = b3

각 계층 동작 원리

- 키 스케줄

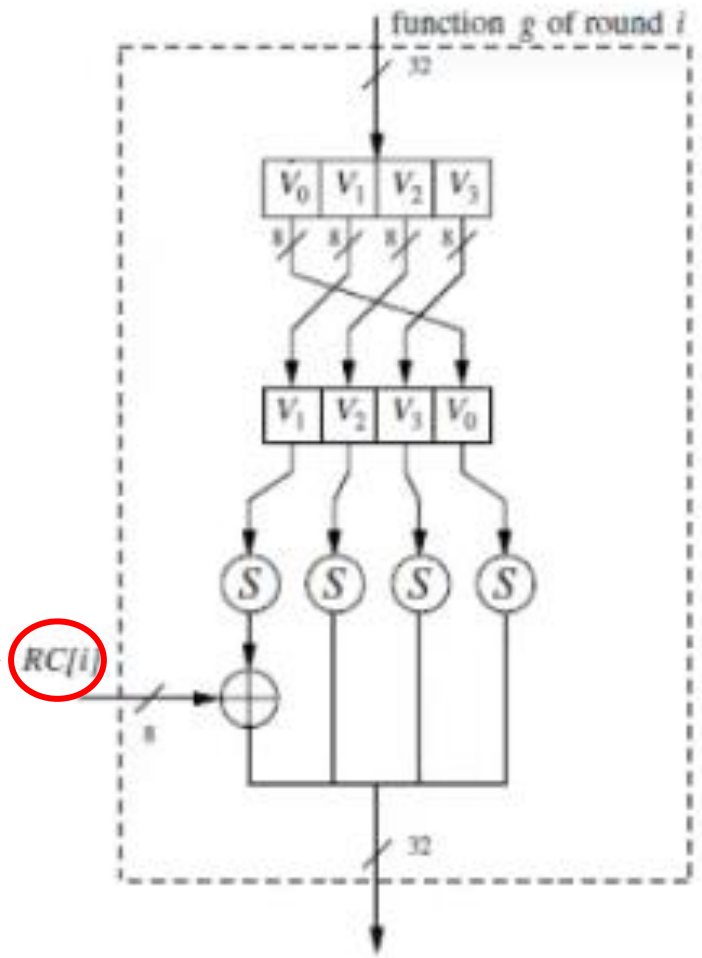


각 계층 동작 원리

- 키 스케줄

$$RC[1] = x^0 = (00000001)_2,$$
$$RC[2] = x^1 = (00000010)_2,$$
$$RC[3] = x^2 = (00000100)_2,$$
$$\vdots$$
$$RC[10] = x^9 = (00110110)_2.$$

라운드 계수



Q & A