블록암호

https://youtu.be/sW8W8muMk54

Contents

CryptoCraft LAB

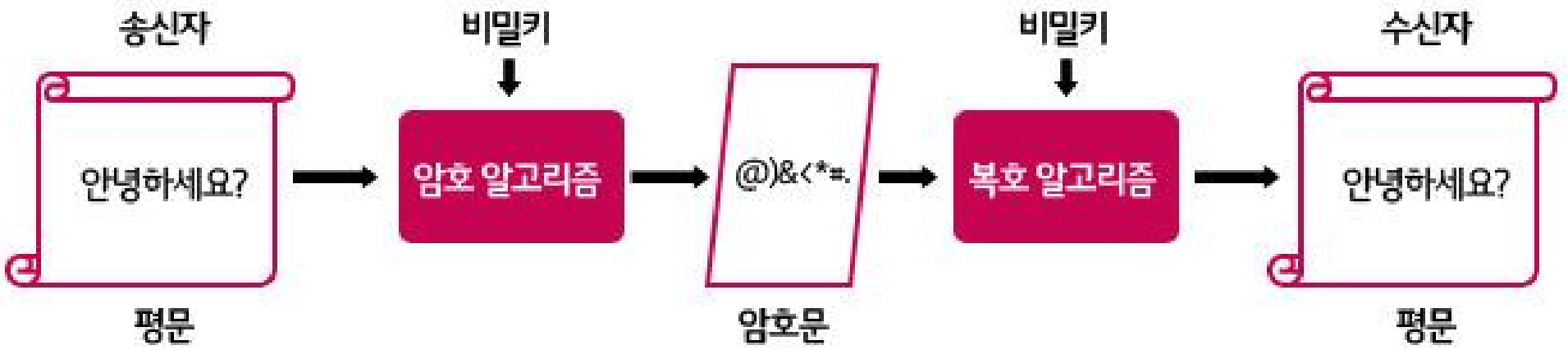
블록암호란?

대칭키 암호 (Symmertric-Key Cipher)

데이터의 단위가 블록!

수차례의 라운드 함수를 통하여 안정성 증가 (혼돈, 확산)

목표 : 키 전수조사 보다 효과적인 공격방법이 없어야 함



블록암호란?

케르크호프스의 원리 (Kerchoffs's Principle)

- 암호 시스템의 모든 것이 알려지더라도 key만 공개되지 않으면 안전하다.

-> 비밀의 크기 = key의 길이

Padding, Parsing

패딩 : 평문 스트림의 길이를 블록 길이의 배수로 맞춰주는 작업 (분할을 위해)

분할 : 패딩된 평문 스트림을 블록 크기로 자름 (마지막 블록이 패딩블록)

블록암호란?

운용모드 (Mode of Operation)

블록 암호	✚	암호화 모드	〓	데이터 암호화
블록 암호	✚	인증 모드	〓	메시지 인증
블록 암호	✚	인증 암호화 모드	〓	데이터 암호화 및 인증
블록 암호	✚	해시 모드	〓	해시 함수

암호화 모드 : ECB, CBC, OFB, CFB, CTR

메시지 인증 모드 : CBC-MAC, CMAC

인증 암호화 모드 : CCM, GCM, OCB

해시 모드 : GCB, MDC-2, MDC-4

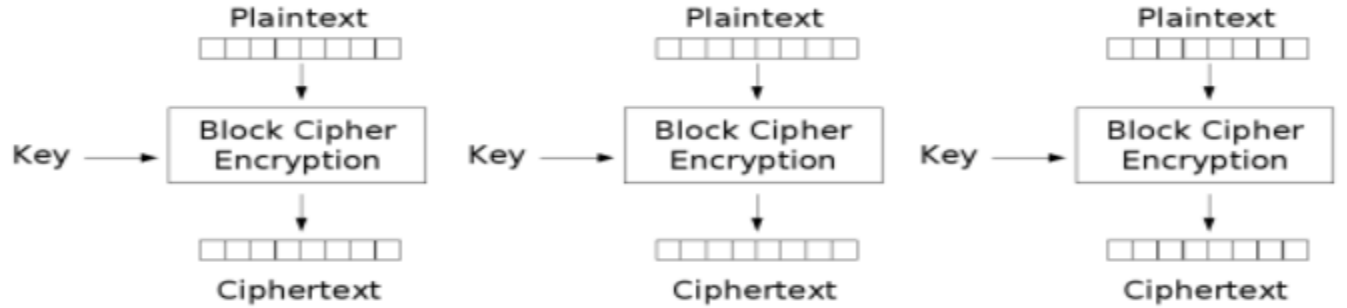
운용모드 : ECB (Electronic CodeBook)

암호화 : $C_i = E_k(P_i)$

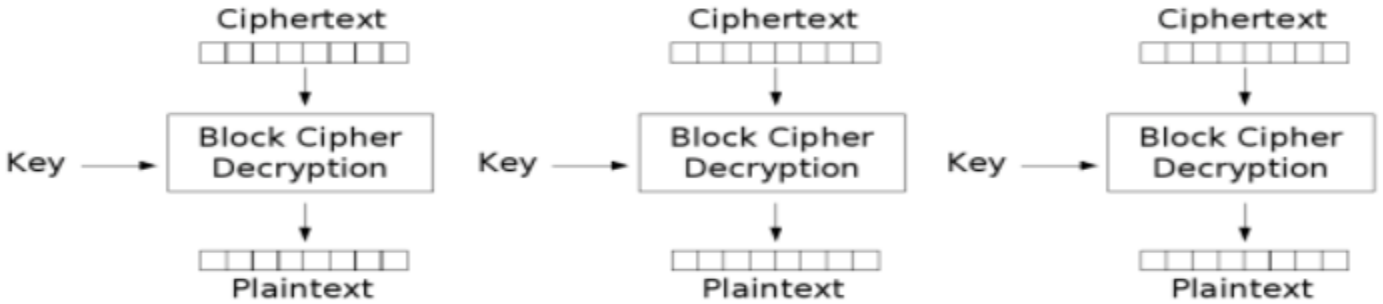
복호화 : $P_i = D_k(C_i)$

특징 : 병렬 연산이 가능하다.

암, 복호화가 빠르다



Electronic Codebook (ECB) mode encryption



블록암호란?

운용모드 : ECB (Electronic CodeBook)

문제점 : 기밀성(Confidentiality) 제공 X

원본 그림 | ECB 방식으로 암호화한 결과 | ECB 이외의 방식으로 암호화한 결과

블록암호란?

운용모드 : CBC (Cipher Block Chaining)

$C_0 = IV$

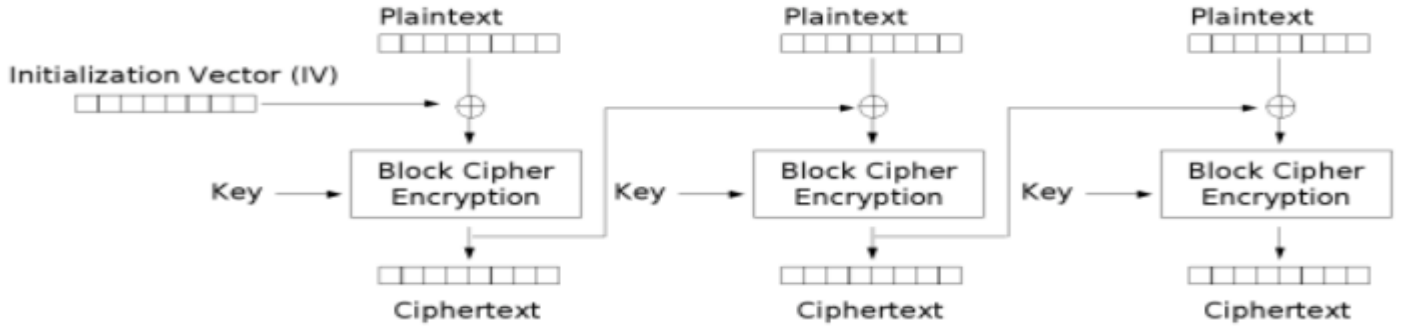
암호화 : $C_i = E_K (P_i \text{ xor } C_{i-1})$

복호화 : $P_i = D_k (C_i) \text{ xor } C_{i-1}$

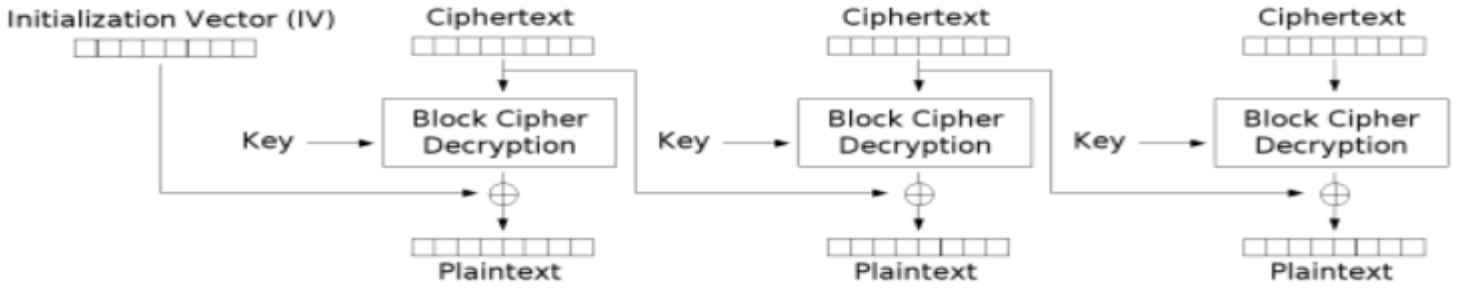
특징 : 전파 성질이 강하다.

복호화 시에만 병렬 연산 가능

전파 성질이 약해짐 (문제x)



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

블록암호란?

운용모드 : CBC (Cipher Block Chaining)

문제점 : 암호문 일치 공격 (생일 역설)

$$\begin{aligned}\bar{p}(n) &= 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \cdots \times \left(1 - \frac{n-1}{365}\right) \\ &= \frac{365 \times 364 \times 363 \times \cdots \times (365-n+1)}{365^n} \\ &= \frac{365!}{365^n (365-n)!}\end{aligned}$$

$$p(n) = 1 - \frac{365!}{365^n (365-n)!}$$

n	$p(n)$
1	0.0%
5	2.7%
10	11.7%
20	41.1%
23	50.7%
30	70.6%
40	89.1%
50	97.0%
60	99.4%
70	99.9%
100	99.99997%
200	99.9999999999999999999999998%
300	$(100 - (6\times10^{-80}))\%$
350	$(100 - (3\times10^{-129}))\%$
365	$(100 - (1.45\times10^{-155}))\%$
366	100%
367	100%

$C_i = C_j$ => C_{i-1} xor P_i = C_{j-1} xor P_j

블록암호란?

운용모드 : CBC (Cipher Block Chaining)

문제점 : 암호문 일치 공격 (생일 역설)

$C_i = C_j$ => C_{i-1} xor P_i = C_{j-1} xor P_j

이므로 P_i를 복구할 수 있다면 P_j 또한 복구할 수 있다.

단, DATA >= $2^{n/2}$의 조건을 깨면 암호문 일치 공격을 피할 수 있다.

블록암호란?

운용모드 : CFB (Cipher FeedBack)

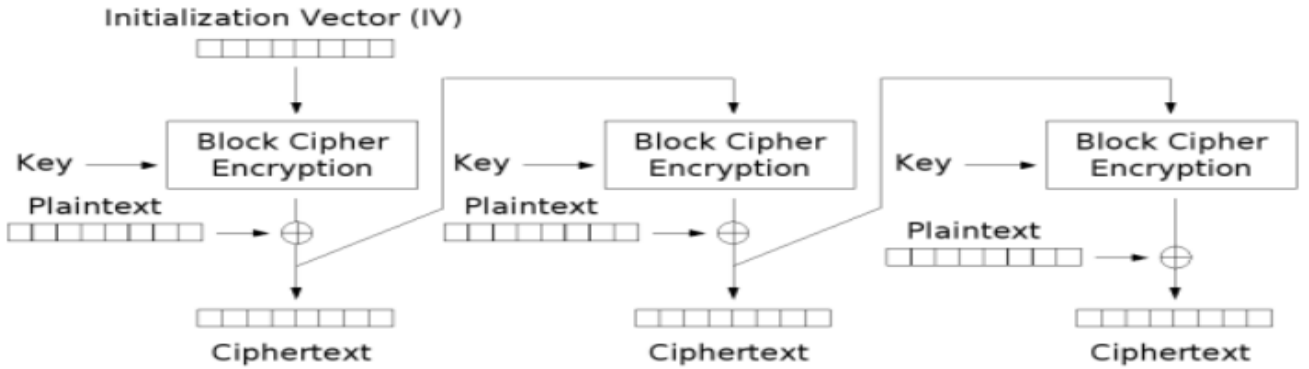
암호화 : $C_i = \begin{cases} \mathrm{IV}, & i = 0 \\ E_K(C_{i-1}) \oplus P_i, & \text{otherwise} \end{cases}$

복호화 : $P_i = E_K(C_{i-1}) \oplus C_i,$

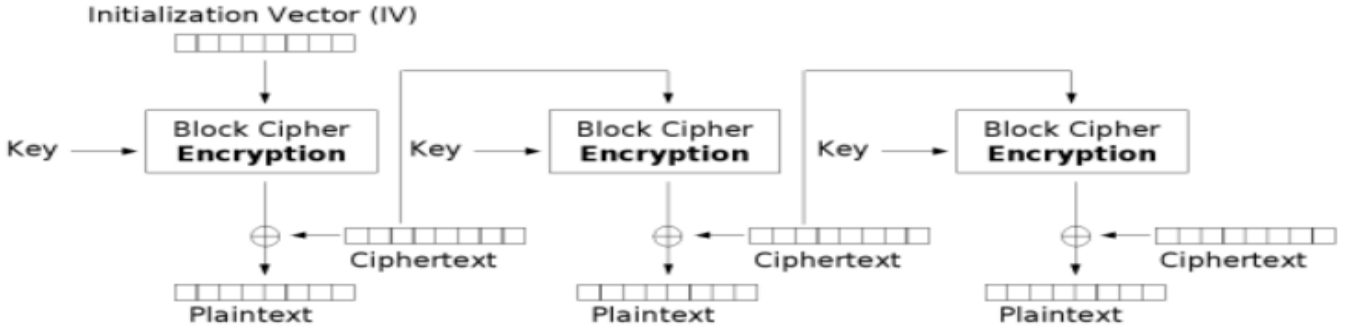
특징 : 복호화 함수가 필요없다.

CBC와 마찬가지로

암호문 일치공격 가능



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption

블록암호란?

운용모드 : OFB (Output FeedBack)

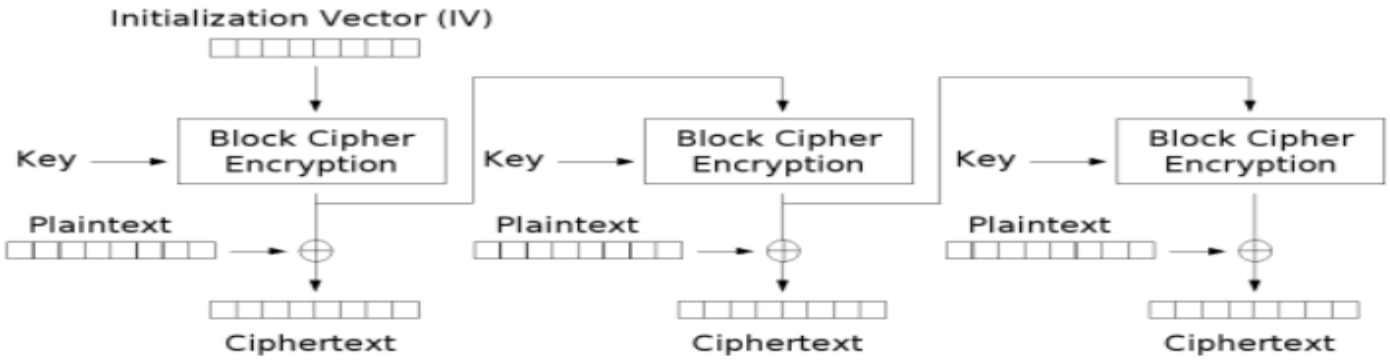
암호화 : $C_j = P_j \oplus O_j,$

복호화 : $P_j = C_j \oplus O_j,$

$O_j = E_K(I_j),$

$I_j = O_{j-1},$

$I_0 = \mathrm{IV}.$

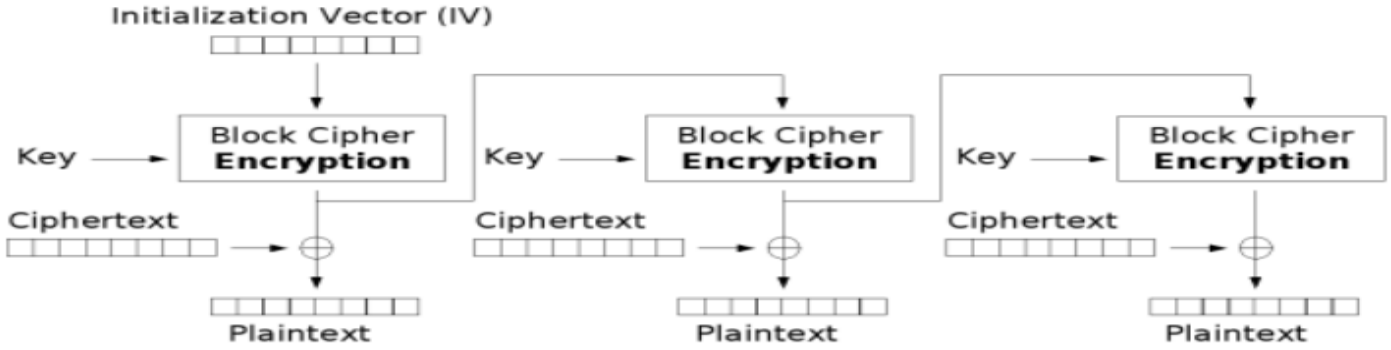


Output Feedback (OFB) mode encryption

특징 : 암호화 및 복호화 함수가 동일

복호화 함수가 필요없다.

사전계산 가능



Output Feedback (OFB) mode decryption

블록암호란?

운용모드 : CTR (CounTeR)

암호화 : $O_i = E_k(CTR_i)$

$C_i = P_i$ xor O_i

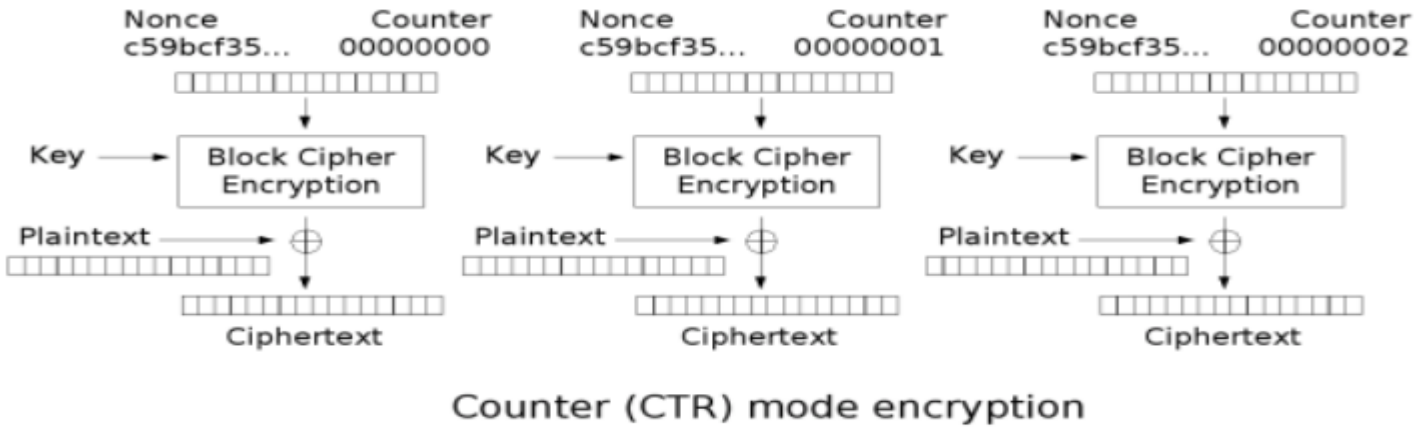
$CTR = CTR_{i-1} + 1$

특징 : 복호화 함수가 필요없다

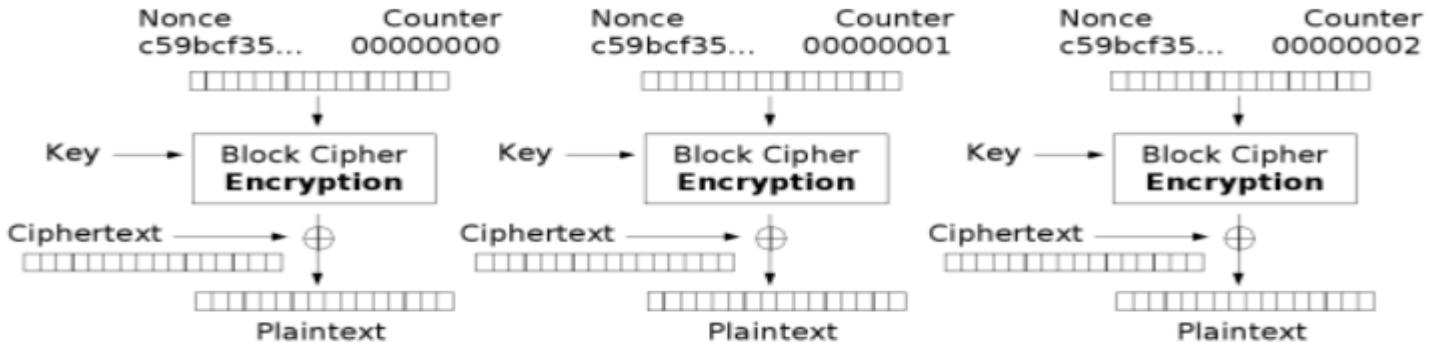
사전 계산 가능

병렬 연산 가능

다중 프로세서에 적합



Counter (CTR) mode encryption



Counter (CTR) mode decryption

블록암호란?

운용모드 : CFB, OFB, CTR

특징 : 블록의 단위에 따라서

CFB-1, OFB-1, CTR-1 (bits단위)

CFB-8, CFB-8, CTR-8 (bytes단위) 로 나눌 수 있음

복호화 함수가 필요없음 (경량화)

블록암호란?

	병렬 연산	복호화 함수	사전계산	취약점
ECB	O	O	X	기밀성 손실
CBC	X	O	X	암호문 일치 공격
CFB	X	X	X	
OFB	X	X	O	없음
CTR	O	X	O	

DES

1999년 DES 암호 해독 대회에서 깨지기 전까지 가장 많이 쓰이던 블록암호

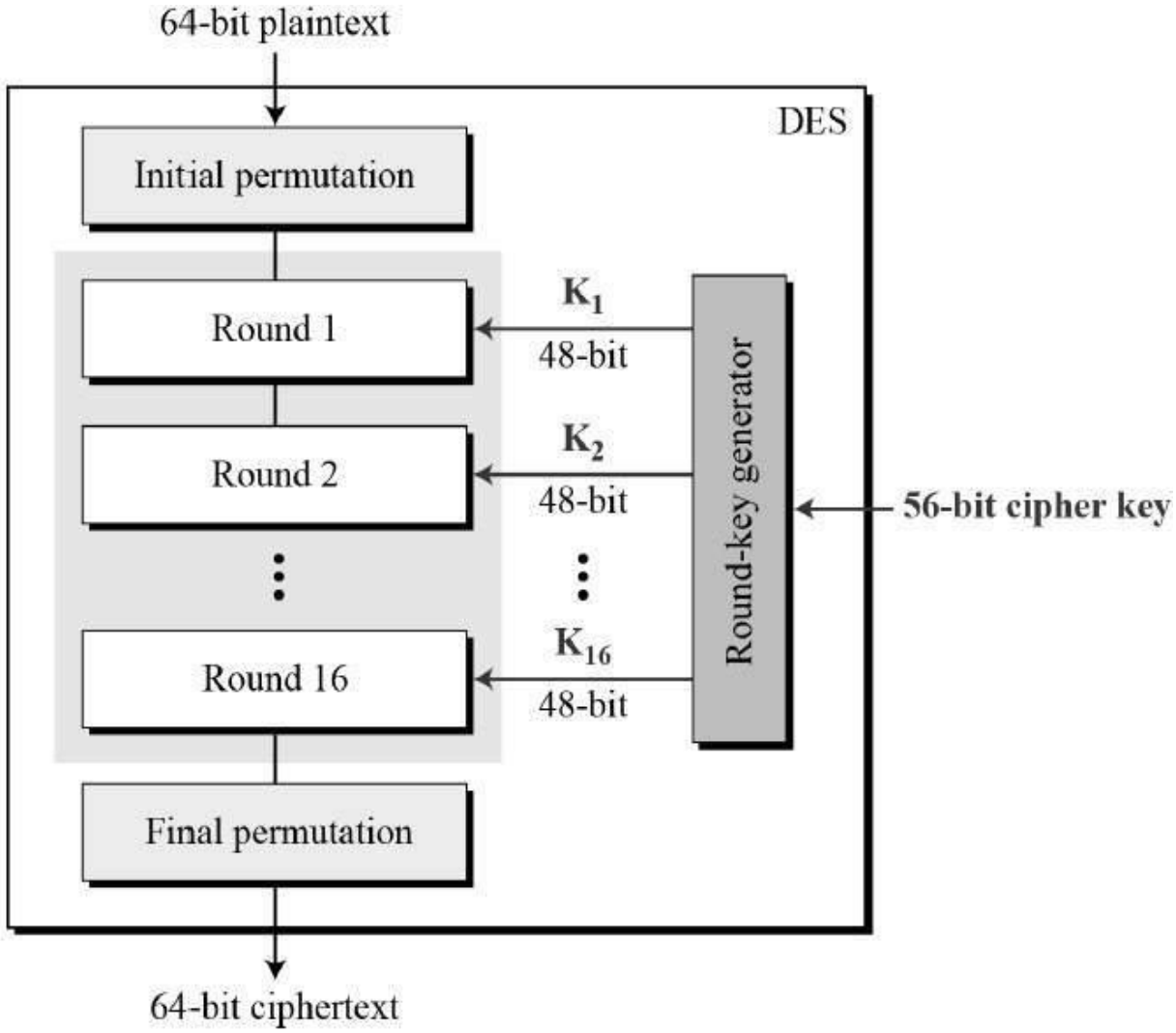
1975년 IBM에서 개발.

1977년 표준화

후대 암호체계에 많은 영향

DES

1. 전체적인 모습

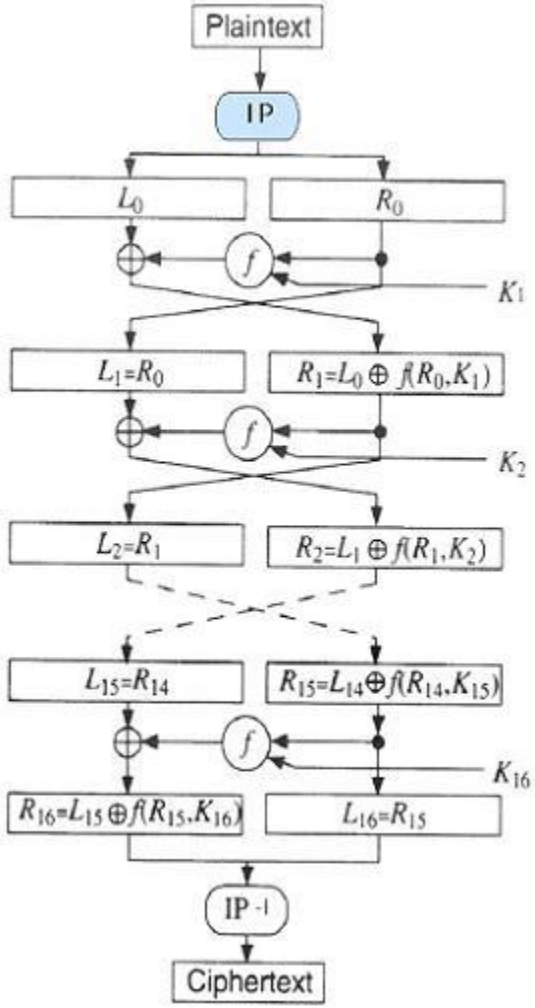

64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
48-bit
K_2
48-bit
K_{16}
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

DES

2. 평문 암호화

Feistel 구조 (경량성)

마지막 라운드에 스왑을 진행하지 않음



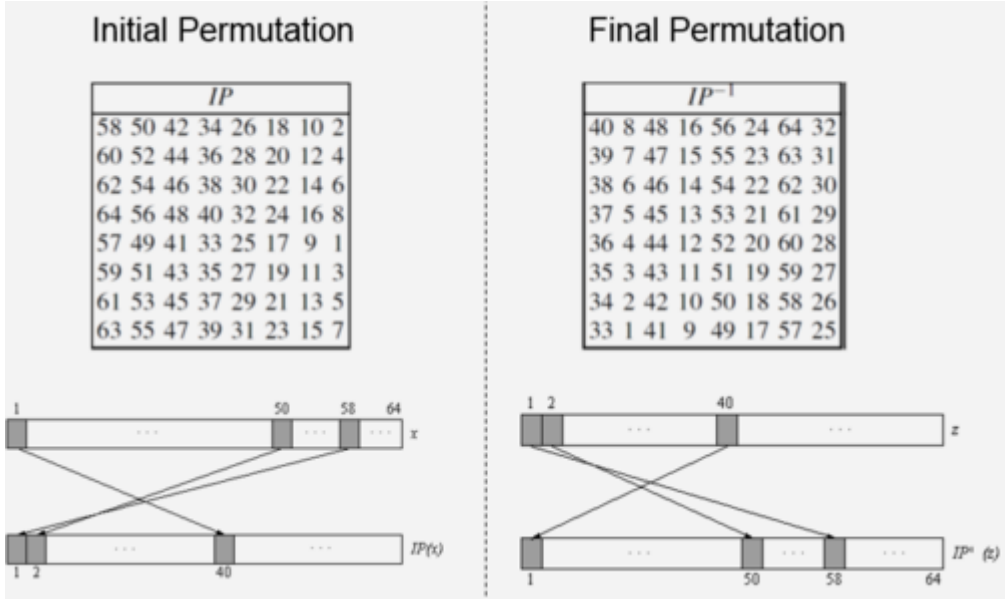
DES

2-1. IP함수

비트들의 위치를 바꾸어 놓는 역할

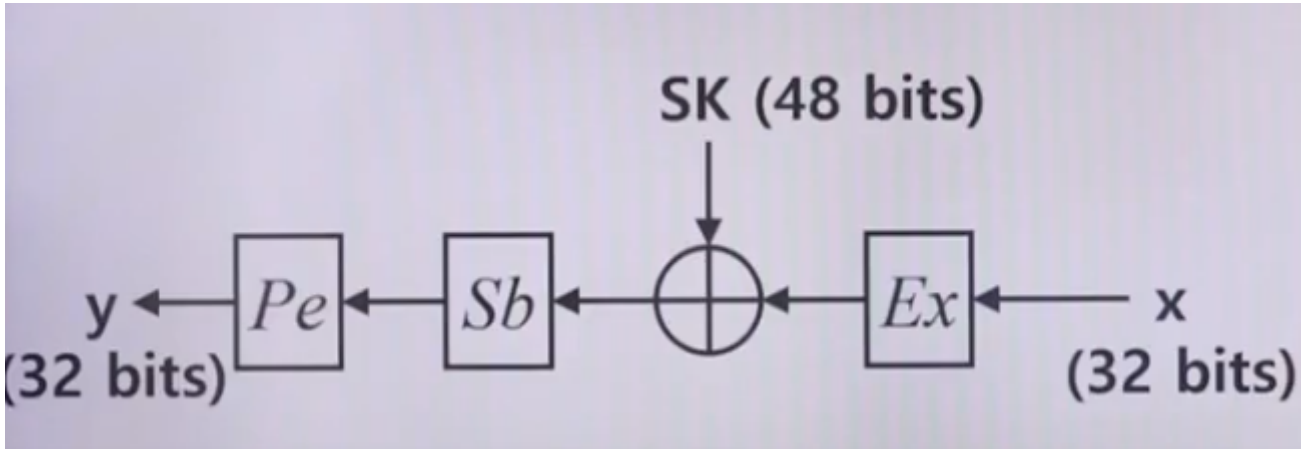
암호화로써의 기능은 없다. (하드웨어적인 역할)

IP^{-1} 함수는 IP함수의 역함수 (복호화시에 필요)



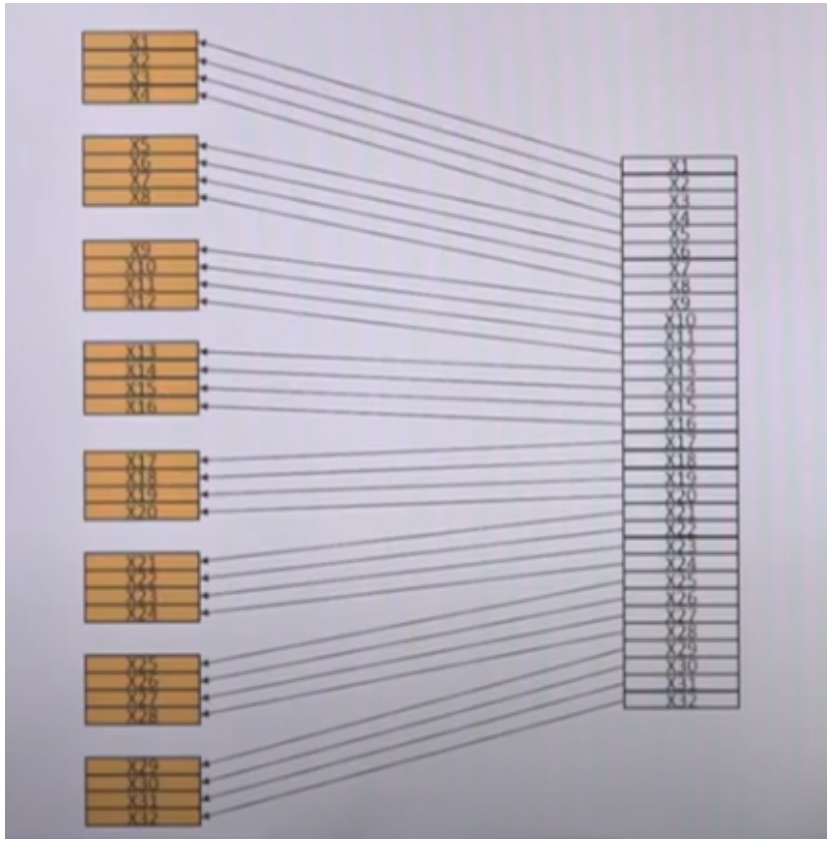
DES

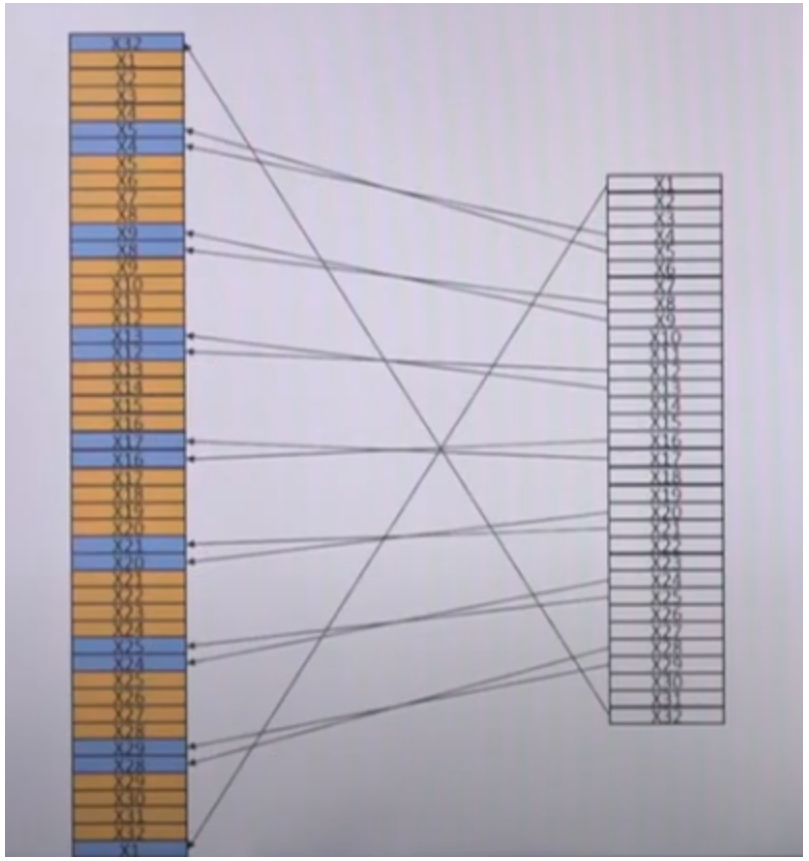
2-2. F함수



DES

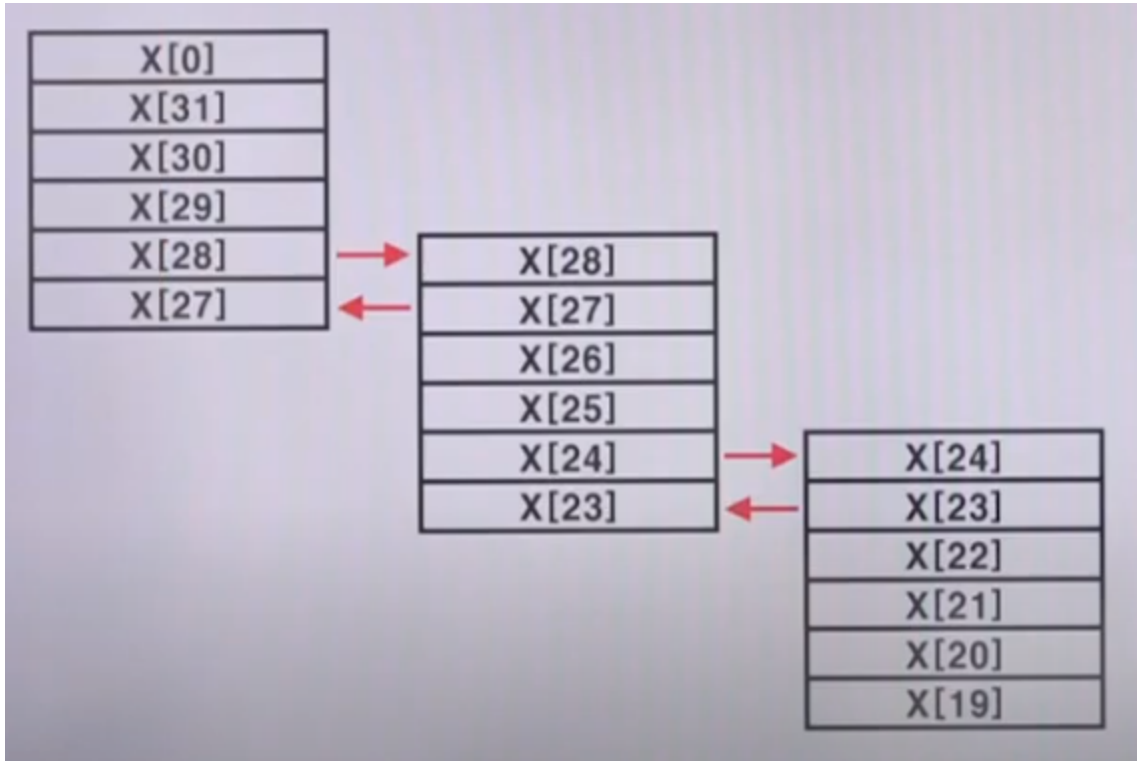
2-2-1. Ex함수 (Expansion)





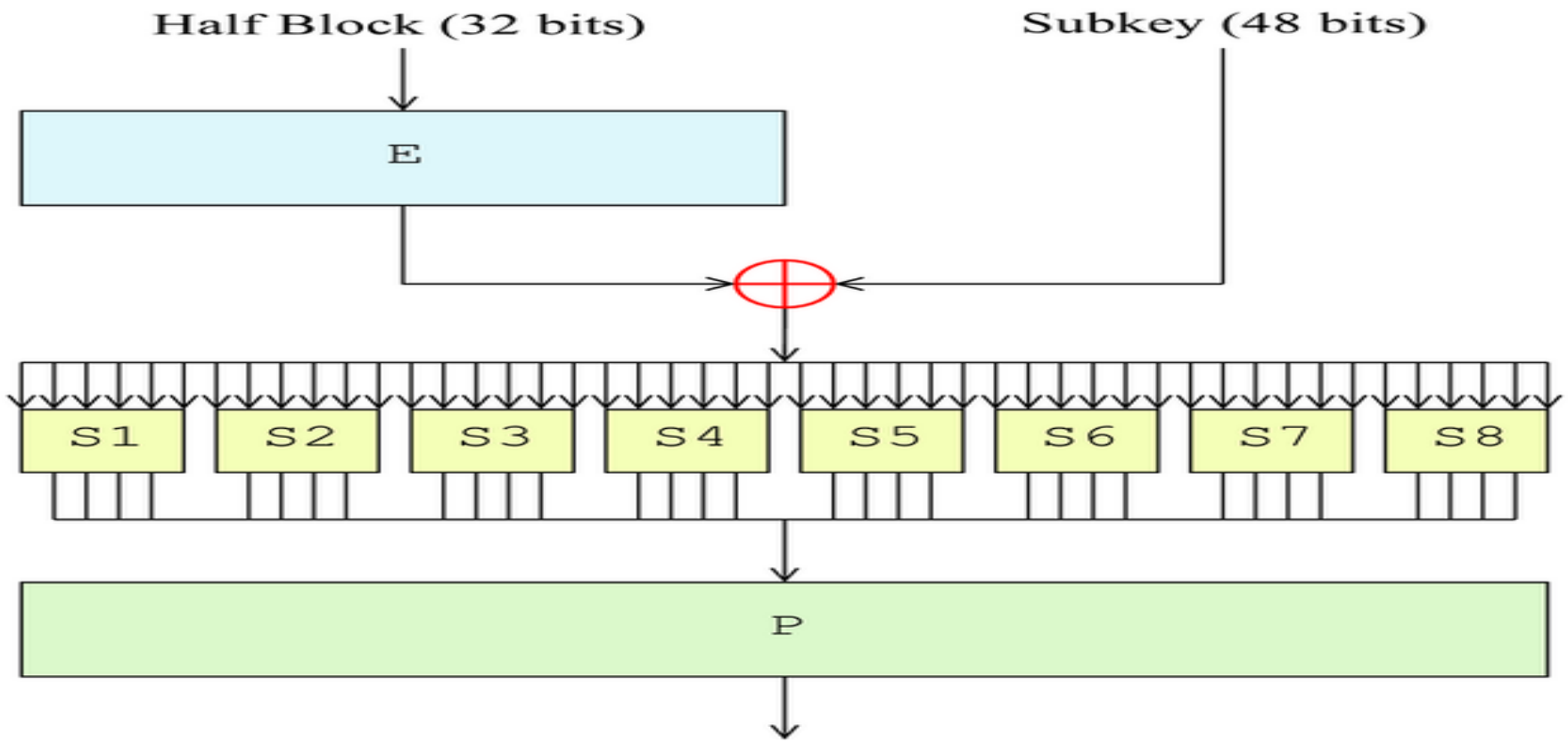
DES

2-2-2. Ex함수 (Expansion)



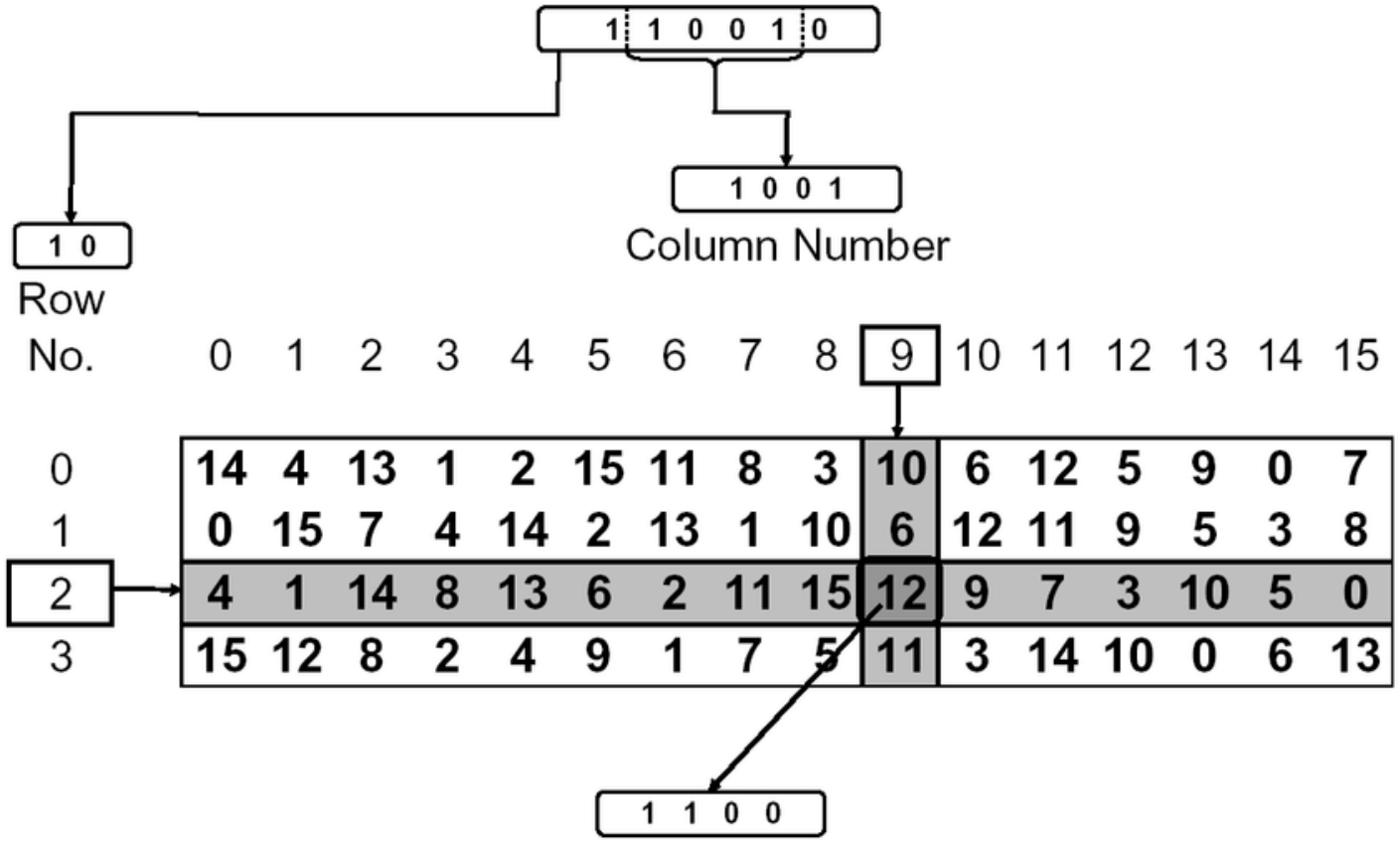
DES

2-2-2. Sb함수 (Substitution)



DES

2-2-2. Sb함수 (Substitution)



2-2-3. Pe함수 (Permutation)

비트의 순서를 섞는 함수

Key schedule의 PC-1, PC-2 함수와 유사

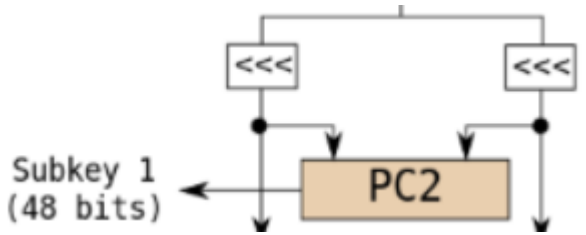
DES

3. 키 스케쥴

에러를 확인하기 위한 패리티비트(8bits)

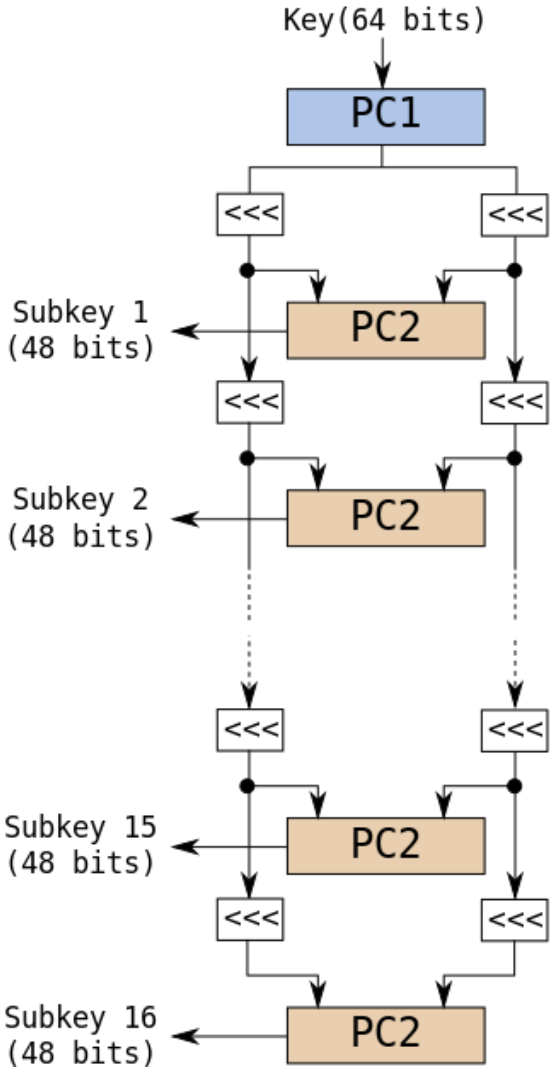
PC−1

57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4



PC−2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32



AES

현 국제표준

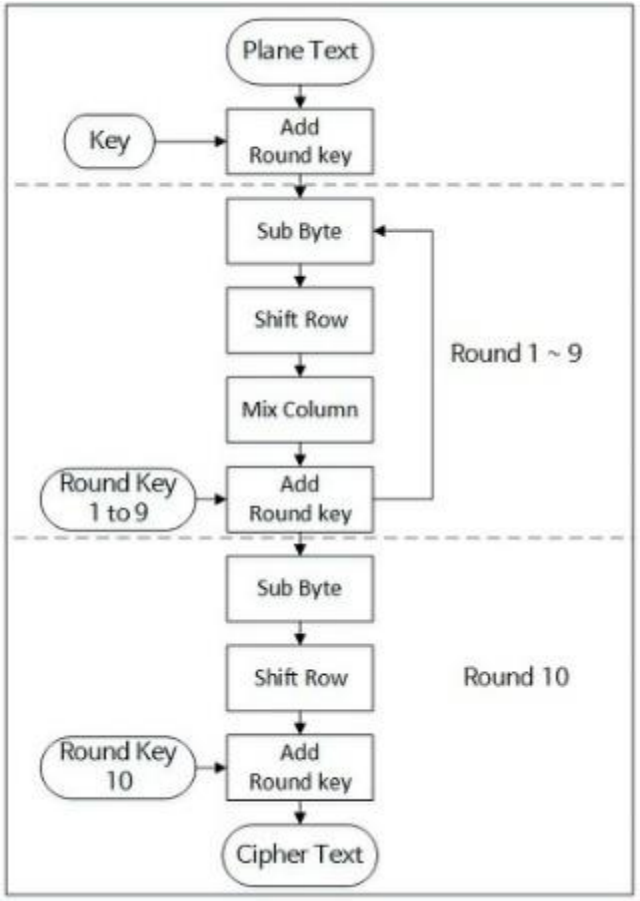
2001년 표준화

블록 길이 : 128bits

키 길이 : 128bits(10라운드), 192bits(12라운드), 256bits(14라운드)

AES

1. 간단한 구조

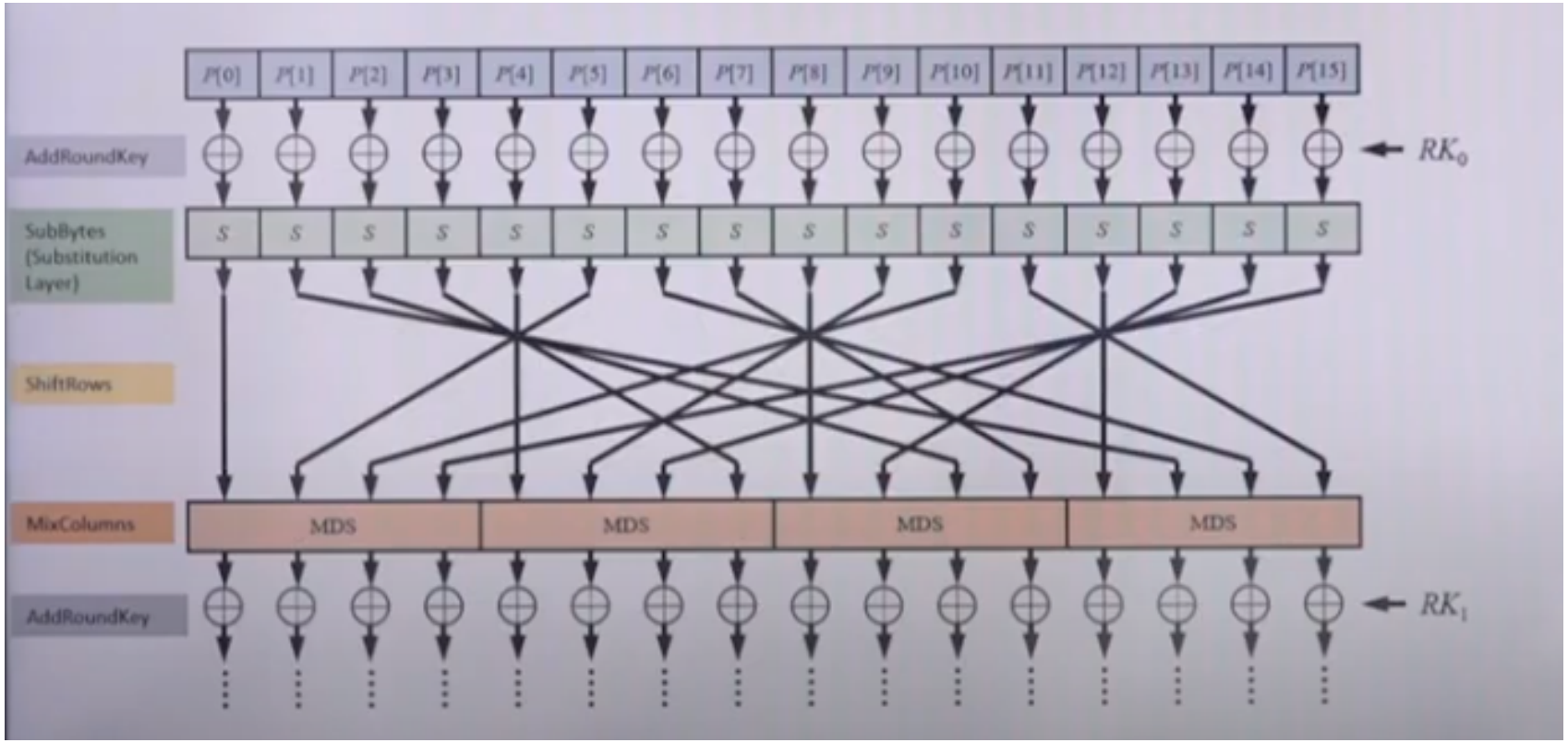

Plane Text
Key
Add
Round key
Sub Byte
Shift Row
Mix Column
Round Key
1 to 9
Add
Round key
Round 1 ~ 9
Sub Byte
Shift Row
Round Key
10
Add
Round key
Round 10
Cipher Text

AES

2. 평문 암호화

SPN 구조

(Substitution Permutation Network)



AES

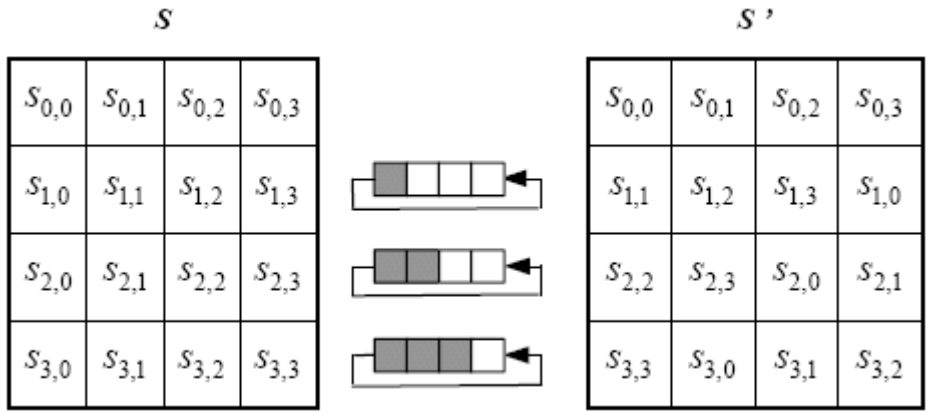
2-1. SubBytes

0x53 -> 0xed

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES

2-2. ShiftRows



AES

2-3. MixColumns

$$[S'] = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * [S]$$

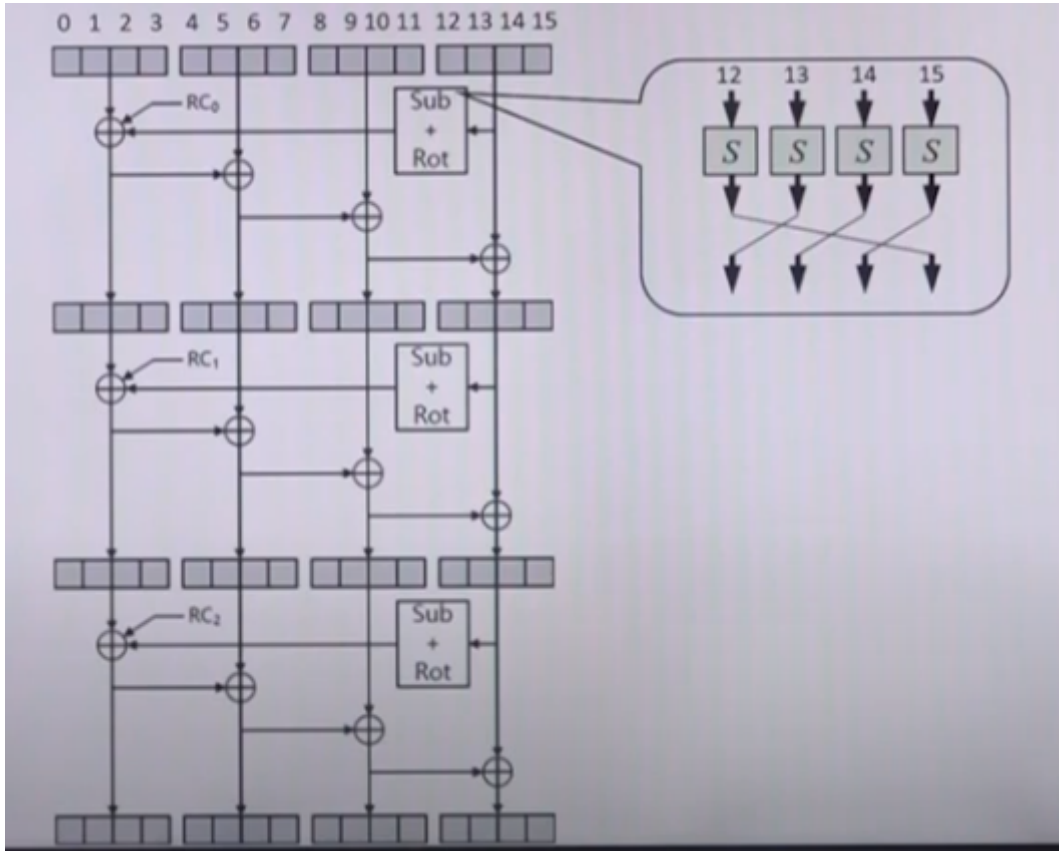
States bytes

States' bytes

AES

3. Key Schedule (128bits)

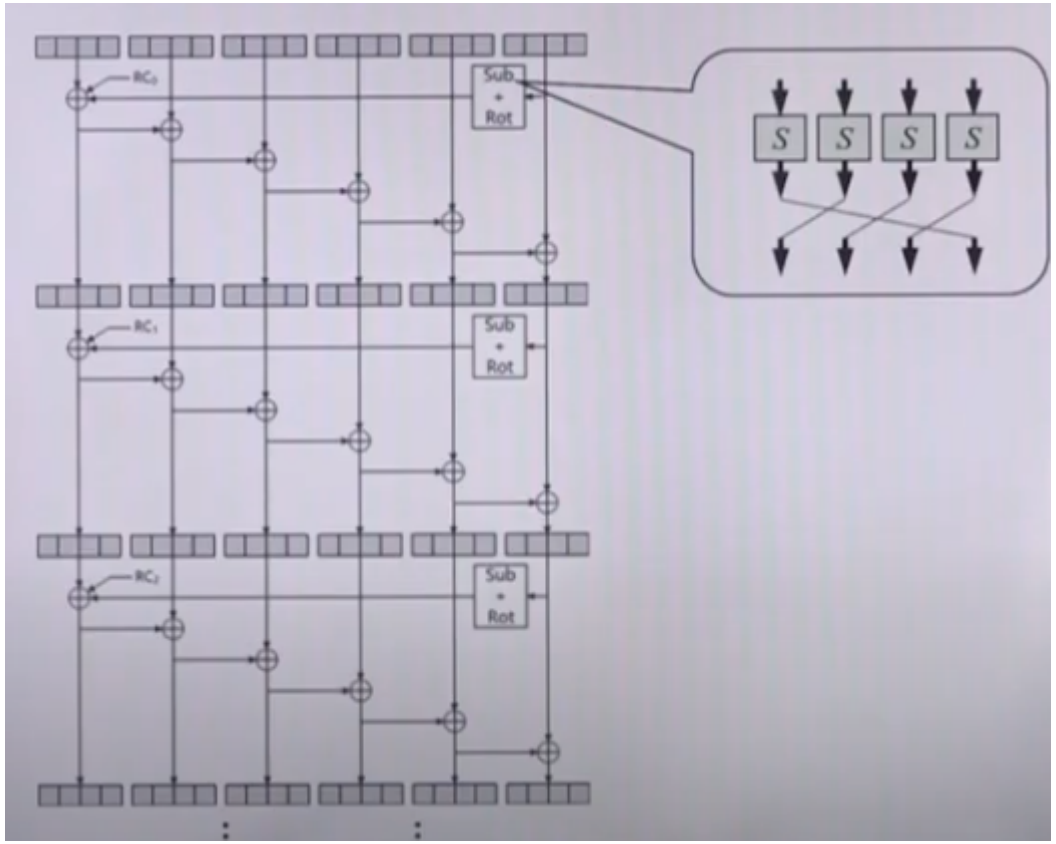
총 10개의 키 생성



AES

4. Key Schedule (192bits)

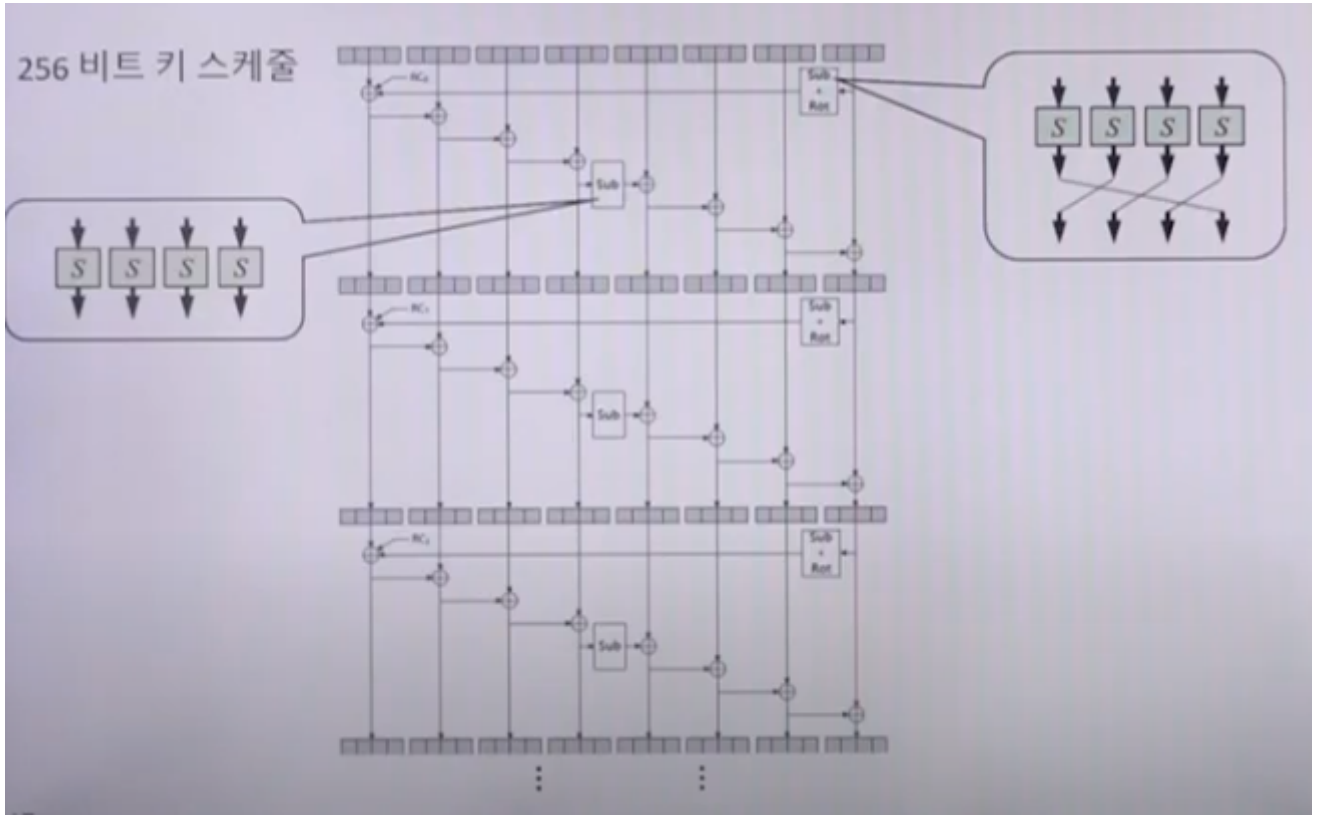
총 12개의 키 생성



AES

4. Key Schedule (256bits)

총 14개의 키 생성



Q & A