3장 : Advanced Encryption Standard (AES)

정보보호이론

Spring 2015

고려대학교
KOREA UNIVERSITY

3.1 AES소개

- 배경
  - DES의 2^{56}개의 키에 대한 전사적 공격이 가능
    - 1999년 distributed.net 과 Electronic Frontier Foundation이 협력한 공격에서 DES의 비밀키를 22시간 15분만에 찾아냄
  - TDES가 있지만 다음 이유로 NIST에서는 AES 공모
    1. TDES는 DES를 세 번 사용하기 때문에 속도가 느림
    2. DES의 블록 크기인 64 비트는 여러 가지 응용분야에 적합하지 않다. 예로 블록 암호를 이용하여 설계한 해쉬 함수(8장에서 소개)의 경우 64비트의 블록 크기는 해쉬 함수의 안전성에 문제
    3. 가까운 미래에 양자컴퓨터가 현실화 될 수 있으며, 양자컴퓨터를 이용하여 공격할 경우 적어도 256 비트 크기의 키가 바람직

3.1 AES소개

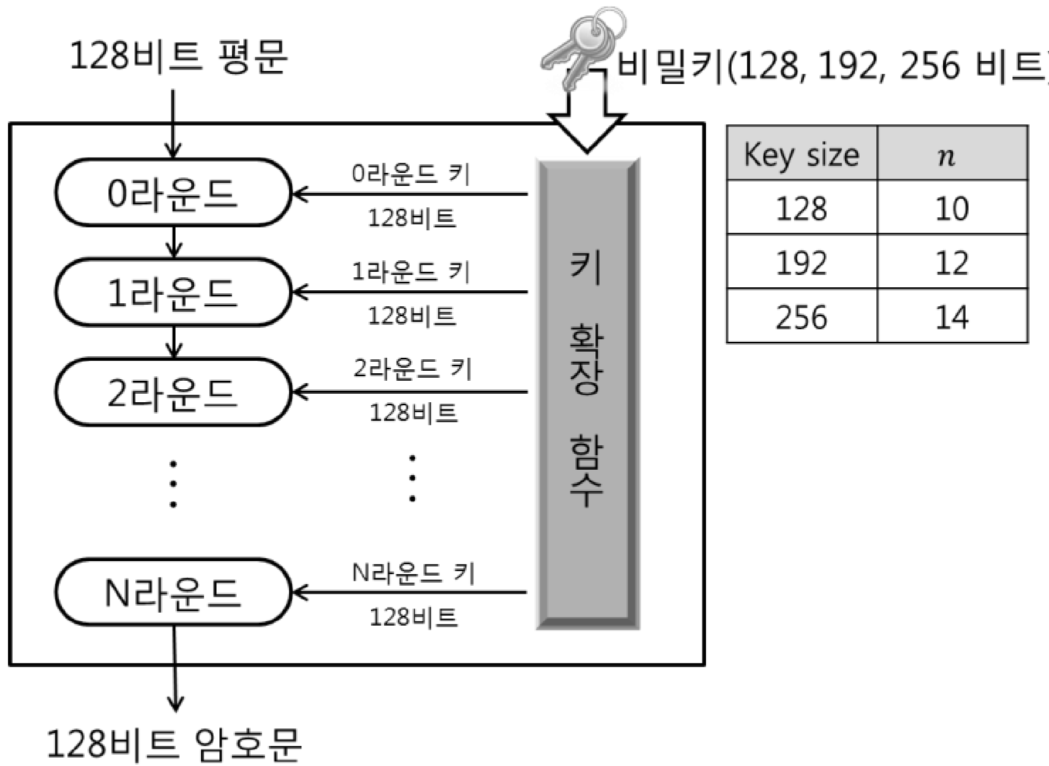
- History
  - US NIST issued call for ciphers in 1997
    - 15 candidates accepted in Jun 98
    - 5 were shortlisted in Aug-99
    - Rijndael was selected as the AES in Oct-2000
    - issued as FIPS PUB 197 standard in Nov-2001
  - AES의 공모 시 요구사항
    - 블록의 크기는 128 비트
    - 대칭키 암호이며 세 종류의 키(128 비트, 192 비트, 256 비트)를 사용할 수 있어야 함
    - 소프트웨어와 하드웨어로 구현될 경우 모두 효율적
    - 모든 키를 다 찾는 전수 키 조사 이외에 현재 알려진 다른 암호 분석 공격에 강해야 함

3.1 AES소개

- 당시 벨기에 루벤대학의 대학원생인 Rijmen과 Daemen이 설계
- AES 공모의 모든 요구사항을 만족시킴
  - 128/192/256 bit keys, 128 bit data
  - an **iterative** rather than **feistel** cipher
  - 설계:
    - 하드웨어나 소프트웨어로 구현할 때 속도나 코드 간결성(Compactness) 면에서 효율적
    - 알려진 블록 암호 알고리즘에 대한 공격들에 안전
    - 현재 AES에 대한 가장 실질적인 공격은 전수 키 조사
    - 최악의 경우(in the worst case) 2^{128} 번의 계산이 필요 (이러한 계산량은 현재 가장 빠른 슈퍼컴퓨터가 계산을 수행해도 태양계의 수명보다 긴 시간이 필요)

3.2 AES 개요

- AES 구조
  - 한 블록 : 128 비트
  - 128, 192, 256 비트의 비밀키에 대해 라운드의 수는 각각 10, 12, 14 라운드가 실행

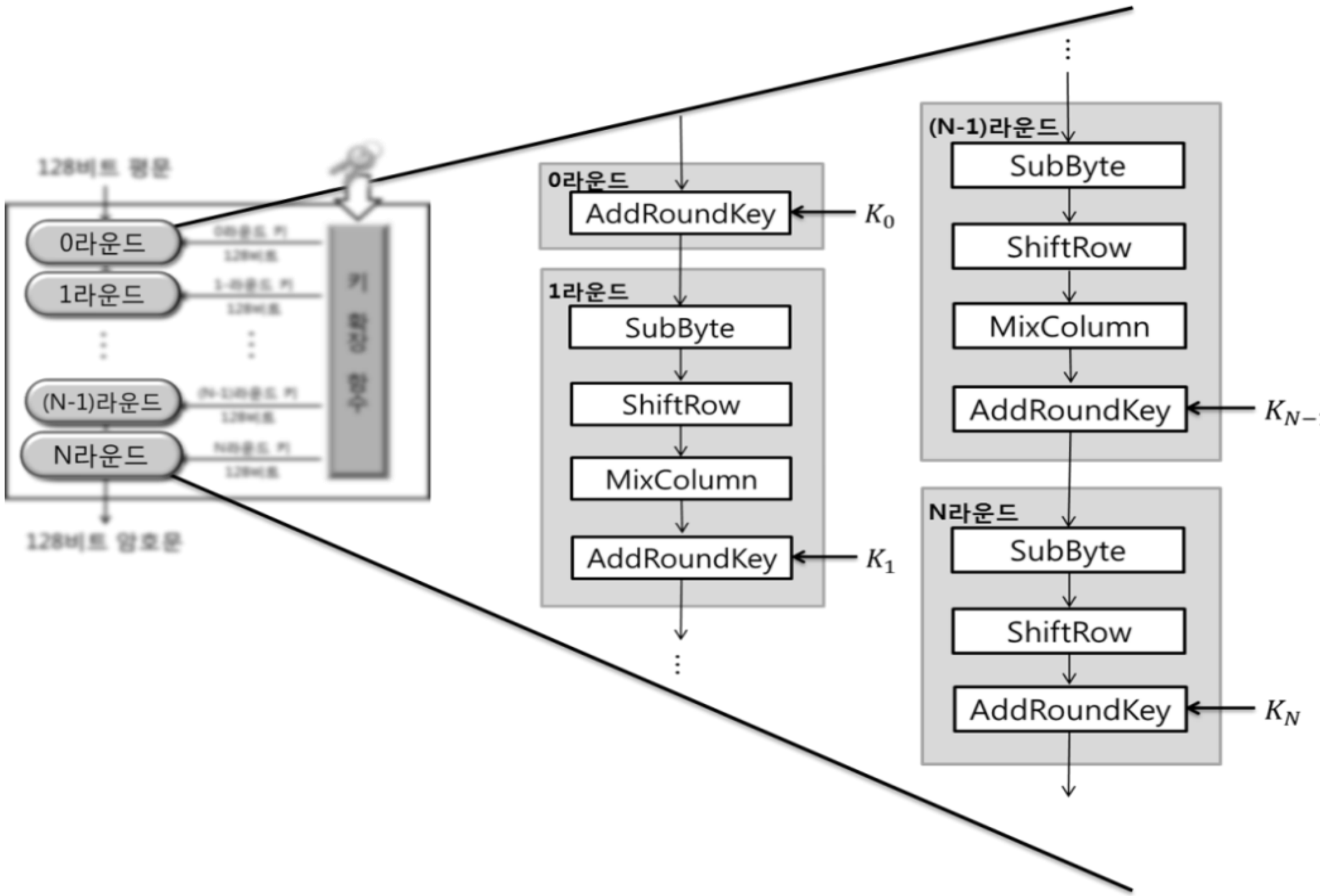


Key size	n
128	10
192	12
256	14

3.2 AES 개요

- 한 블록인 16 바이트(=128 비트)는 원소가 한 바이트인 4x4 행렬로 변환됨
  - 이 행렬을 **상태**(state)라 부름
- 한 라운드는 네 가지 계층(Layer)으로 구성
  - SubBytes : DES의 S-Box에 해당하며 한 바이트 단위로 치환을 수행.
    - 상태(state)의 한 바이트를 대응되는 S-Box의 한 바이트로 치환한다. 이 계층은 혼돈의 원리를 구현한다.
  - ShiftRows : 상태의 한 행안에서 바이트 단위로 자리바꿈이 수행
  - MixColumns : 상태가 한 열안에서 혼합이 수행. ShiftRows와 함께 분산의 원리를 구현
  - AddRoundKey : 비밀키(128/192/256 비트)에서 생성된 128 비트의 라운드 키와 상태가 XOR됨

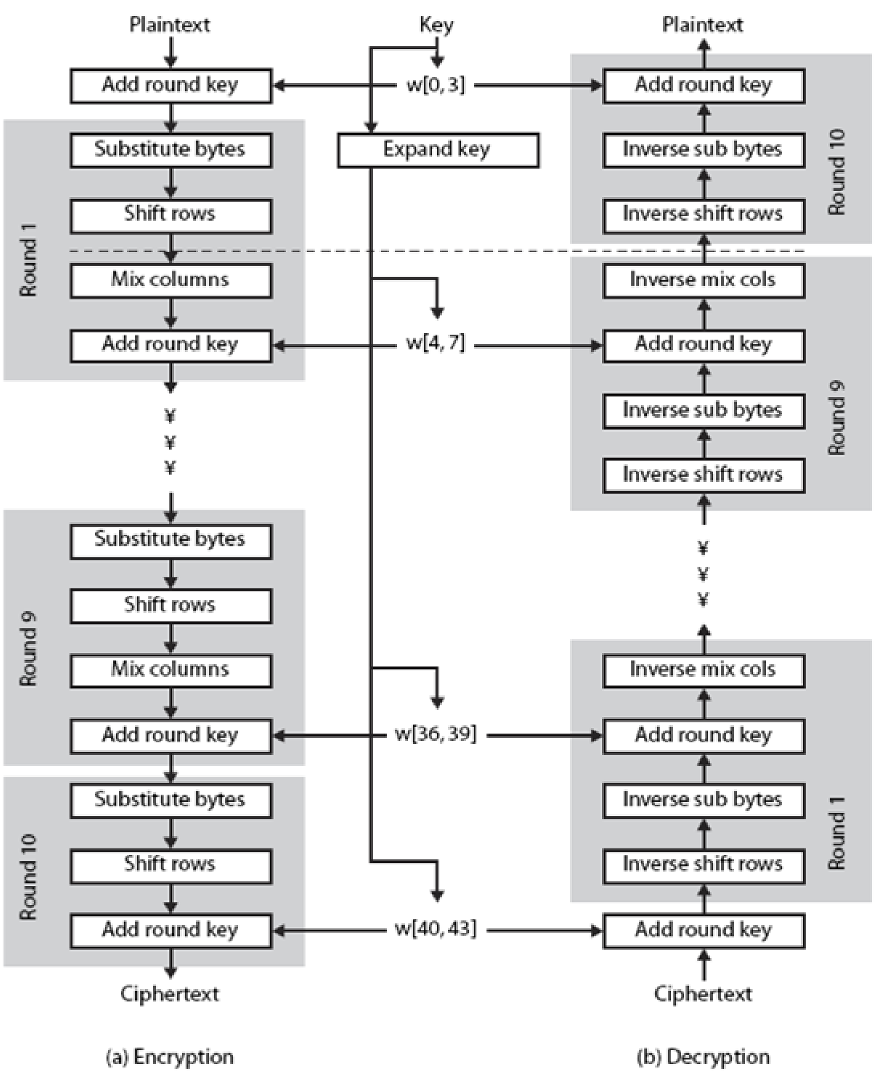
3.2 AES 개요



128비트 평문
0라운드
1라운드
(N-1)라운드
N라운드
128비트 암호문
0라운드
AddRoundKey
K_0
1라운드
SubByte
ShiftRow
MixColumn
AddRoundKey
K_1
(N-1)라운드
SubByte
ShiftRow
MixColumn
AddRoundKey
K_{N-1}
N라운드
SubByte
ShiftRow
AddRoundKey
K_N

3.2 AES 개요

- Encryption and Decryption
  - Iterative이기 때문에 모든 component가 invertible해야 함
  - Round key는 DES와 동일하게 역순임



3.3 AES의 수학적 배경

- **정의 3.1 군** : 집합 G와 이항 연산 ■이 조건 1~4를 만족할 때, (G, ■)을 군(group)이라 함.
  1. **닫혀있음(Closure) :** 집합 G의 임의의 두 원소 a와 b에 대해, c=a ■b도 G의 원소
  2. **결합법칙(Associativity) :** G의 임의의 원소 a, b, c에 대해 (a ■ b) ■ c = a ■(b ■c)
  3. **항등원 존재(Existence of Identity) :** G의 임의의 원소 a에 대해 e ■a = a ■e = a를 만족하는 항등원 e가 존재
  4. **역원 존재(Existence of Inverse) :** G의 임의의 원소 a에 대해 a ■ a′ = a′ ■a = e 를 만족하는 역원이 존재.
  5. **교환법칙(Commutativity) :** G의 임의의 원소 a와 에 대해 a ■b= b ■a 를 만족한다. 이 조건을 만족하는 군을 가환군(Commutative group) 또는 아벨군(Abelian Group)이라 함

3.3 AES의 수학적 배경

- **예제 3.1** : $(\mathbb{Z}_3, +)$이 군임을 보이시오
  - 풀이) : $\mathbb{Z}_3$ $=\{0,1,2\} \rightarrow$ " + "는 모듈로 3에서의 덧셈 연산
    - 닫혀있음 : $\mathbb{Z}_3$의 임의의 두 원소와 +연산을 수행하여 얻은 결과값은 다시 $\mathbb{Z}_3$의 원소가 되므로 $\mathbb{Z}_3$은 +연산에 대하여 닫혀있다.
      - $0+0 \equiv 0(mod\ 3),\ 0+1 \equiv 1(mod\ 3),\ 0+2 \equiv 2(mod\ 3)$
      - $1+0 \equiv 1(mod\ 3),\ 1+1 \equiv 2(mod\ 3),\ 1+2 \equiv 0(mod\ 3)$
      - $2+0 \equiv 2(mod\ 3),\ 2+1 \equiv 0(mod\ 3),\ 2+2 \equiv 1(mod\ 3)$
    - 결합법칙 : $\mathbb{Z}_3$의 임의의 세 원소 $a, b, c \in \mathbb{Z}_3$에 대하여
      - $(a+b)+c \equiv a+b+c \equiv a+(b+c)\ (mod\ 3)$
    - 항등원
      - $\mathbb{Z}_3$의 임의의 원소 a에 대하여 $a+0 \equiv a \equiv 0+a\ (mod\ 3)$ 을 만족하므로, 항등원 0이 존재
    - 역원
      - $\mathbb{Z}_3$의 임의의 원소 a에 대하여, $a+(-a) \equiv 0\ (mod\ 3)$이므로 a 의 역원 $-a$이 존재

3.3 AES의 수학적 배경

- **위수(Order) :**
  - 군의 위수 : 군의 원소의 개수
  - 원소의 위수 : 원소 a에 대하여 $a^m = e$가 되는 최소 정수 m
    - G = $<Z_6, +>$: the orders of the elements are

      ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.
    - G = $<Z_{10}{}^*, \times>$: the orders of the elements are

      ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

3.3 AES의 수학적 배경

- **순환 군**
  - 군의 모든 원소가 군의 한 원소의 지수승으로 표현됨
    - a = g^k for some g and every a in group (g^k means applying a group operation k times. g^0 is e.)
    - i.e., {e, g, g^1, . . . , g^{n-1} }, and g^{n-1} = e
    - "a"는 군을 생성하므로 군의 "생성자(generator)" 혹은 "원시 원소(primitive element)"라 불림
  - **(**Z^*_7 = {1, 2, ..., 6},x) is a cyclic group.
    - 3 mod 7 = 3, 9 mod 7 = 2, 27 mod 7 = 6, 81 mod 7 =4, 243 mod 7 = 5, 729 mod 7 = 1.

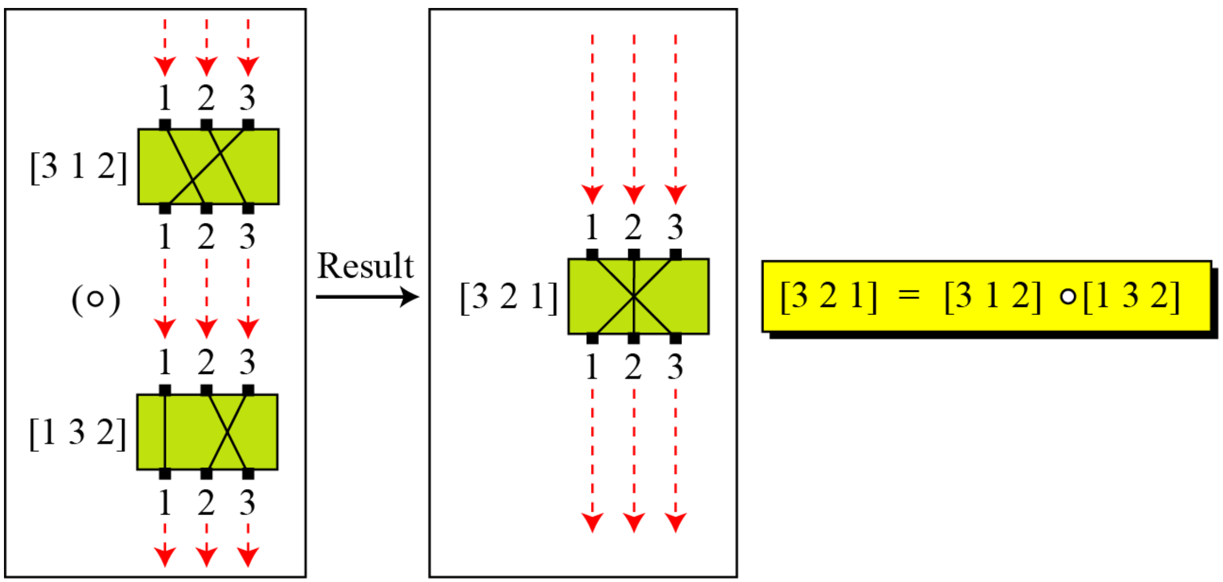
    So 3 is a generator
    - 2 mod 7 = 2, 4 mod 7 = 4, 8 mod 7 = 1.

    So 2 is not a generator

3.3 AES의 수학적 배경

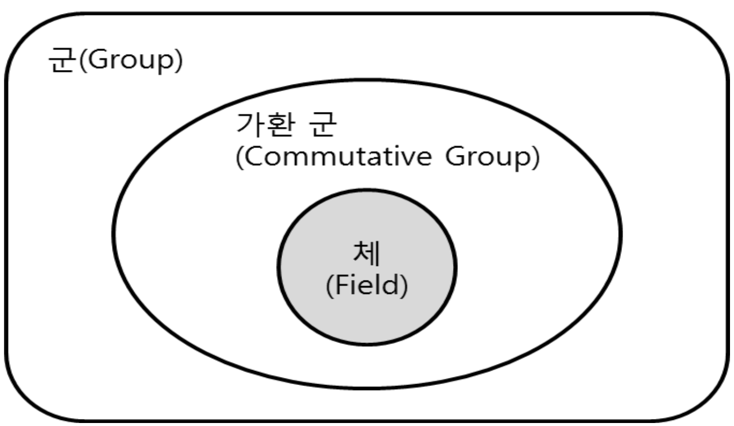
the permutation group

- using two permutations one after another cannot strengthen the security of a cipher



3.3 AES의 수학적 배경

- **정의 3.2 체** : 집합 F 위에 덧셈 연산 +와 곱셈 연산 × 이 정의되어 있고 다음 조건을 만족할 때, $(F,+,\times)$를 체(Field)라 함
  1. $(F,+)$는 가환군
  2. $(F,\times)$는 가환군 (단, 덧셈 연산의 항등원의 경우 곱셈 연산에 대한 역원이 존재하지 않는다.)
  3. 덧셈 연산에 대한 곱셈 연산의 분배 법칙이 성립
     – F의 임의의 원소 a, b, c에 대해 $a \times (b + c) = a \times b + a \times c$가 성립



3.3 AES의 수학적 배경

- **유한체 :** 원소의 개수가 유한
  - 암호학에서는 유한체만을 다룸
  - **갈루아(Galois)** : 위수 m을 갖는 체의 경우 m은 반드시 소수의 지수승으로 표현됨
    - 양수 n과 소수 p에 대하여 $m = p^n$
    - p^n 의 원소를 갖는 체를 $GF(p^n)$
  - 예제 : $(\mathbb{Z}_7, +, \times)$: $(\mathbb{Z}_7, +)$는 덧셈군, $(\mathbb{Z}_7, \times)$는 곱셈군
    - 역원

a	0	1	2	3	4	5	6
$-a$	0	6	5	4	3	2	1
$a+(-a)$	0	0	0	0	0	0	0

a	0	1	2	3	4	5	6
a^{-1}	.	1	4	5	2	3	6
$a \times a^{-1}$	.	1	1	1	1	1	1

3.3 AES의 수학적 배경

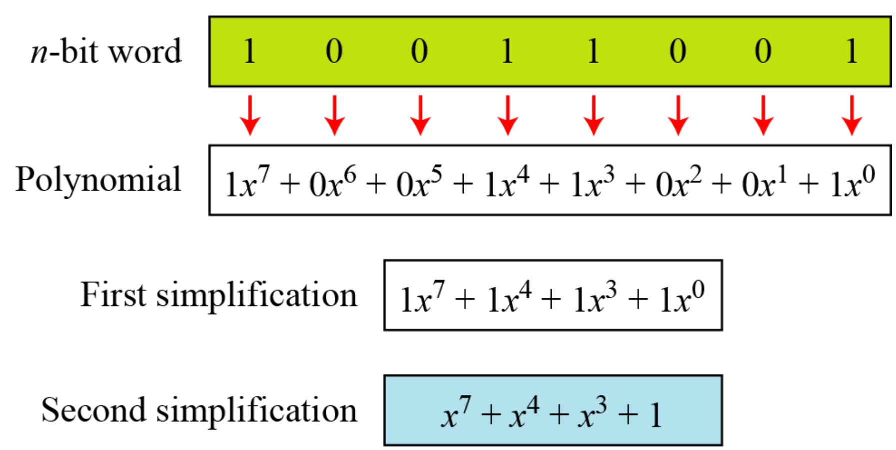
- 소수 체(Prime Field)
  - 유한 체 $GF(p^n)$중에 $n = 1$인 유한 체를 소수 체라 하며 그 원소는 $\{0, 1, \ldots, p - 1\}$
  - AES에서 중요한 소수체는 $GF(2) = \{0,1\}$
    - $GF(2)$에서 덧셈은 XOR연산과 동일하며 곱셈은 논리적 AND 연산과 동일

3.3 AES의 수학적 배경

- 확장 체(Extension Field) $GF(2^n)$
  - 암호에서는 (+, -, x, /) 필요 → 즉 체 필요
  - 컴퓨터에서 양수는 n bit가 배정, 즉 0~$2^n - 1$
  - 2^n 은 소수가 아님 → 4칙 연산 불가 → 새로운 연산 정의필요
  - $GF(2^n)$, n>1, 은 확장 체라 불림
    - 원소에 대한 새로운 개념 → 다항식
    - 각 원소에 대한 연산을 새롭게 정의 → 다항 연산

3.3 AES의 수학적 배경

- **$GF(2^n)$의 원소**
  - 최고차항이 $n-1$이며, 최고 n개의 항을 갖는 다항식
  - 계수(coefficient)는 $GF(2)$ 의 원소(즉, 0이나 1)
    - $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0,\ a_i \in GF(2) = \{0,1\}$
  - AES에서는 $GF(2^8)$
    - $a_7x^7 + a_6x^6 + \cdots + a_1x^1 + a_0x^0$
    - 8 비트인 $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$만 저장



3.3 AES의 수학적 배경

- $\boldsymbol{GF(2^n)}$의 덧셈 연산
  - $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$
  - $g(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x^1 + b_0x^0$

  - $f(x) + g(x) = \ (a_{n-1} + b_{n-1} \bmod 2)x^{n-1} + (a_{n-2}+b_{n-2} \bmod 2)x^{n-2} + \cdots + (a_1+b_1 \bmod 2)x^1 + (a_0+b_0 \bmod 2)x^0$

3.3 AES의 수학적 배경

- $GF(2^n)$의 곱셈 연산
  - 계수 계산은 $GF(2)$에서
  - $x^i \times x^j$ 는 x^{i+j}
    - i+j > n -1일 경우, 집합 $GF(2^n)$이 곱셈에 대하여 닫혀 있기 위해서는 n차 기약 다항식을 이용한 모듈로 연산으로 곱셈의 결과가 $(n-1)$차 이하인 다항식이 되도록 해야 함
    - 기약 다항식 : 1과 그 자신만을 인수로 갖는 다항식
      - $(X^2 + 1) = (X+1)(X+1)$ → 기약 다항식이 아님

Degree	*Irreducible Polynomials*
1	$(x+1), (x)$
2	(x^2+x+1)
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+1), (x^4+x+1)$
5	$(x^5+x^2+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1),$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

3.3 AES의 수학적 배경

- **$\mathbf{GF(2^n)}$의 곱셈 연산**
  - $(x^5 + x^2 + x) \times (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$

$$P_1 \otimes P_2 = \boxed{(x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1)} = x^5 + x^3 + x^2 + x + 1$$

3.3 AES의 수학적 배경

$$
\begin{array}{r|l}
 & x^4 + 1 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{12} + x^7 + x^2 \\
 & x^{12} + x^8 + x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^8 + x^5 + x^4 + x^2 \\
 & x^8 + x^4 + x^3 + x + 1 \\
\cline{2-2}
\text{Remainder} & \boxed{x^5 + x^3 + x^2 + x + 1}
\end{array}
$$

3.3 AES의 수학적 배경

- **$GF(2^n)$의 역 연산**
  - 덧셈 $f(x)$ XOR $f(x)$ = 0 → 역원은 $f(x)$
  - 곱셈 역원은 $f(x)$ x $f(x)^{-1}$ mod (irreducible poly) = 1
    - 정수와 동일하게 확장 유클리드 알고리즘을 이용

  - 예제 : $GF(2^4)$에서 modulo $(x^4 + x + 1)$에서 $(x^2 + 1)$의 역은?

q	r_1	r_2	r	t_1	t_2	t
$(x^2 + 1)$	$(x^4 + x + 1)$	$(x^2 + 1)$	(x)	(0)	(1)	$(x^2 + 1)$
(x)	$(x^2 + 1)$	(x)	(1)	(1)	$(x^2 + 1)$	$(x^3 + x + 1)$
(x)	(x)	(1)	(0)	$(x^2 + 1)$	$(x^3 + x + 1)$	(0)
	(1)	(0)		$(x^3 + x + 1)$	(0)	

3.3 AES의 수학적 배경

컴퓨터 구현

- multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(28)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes \mathrm{P}_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes \mathrm{P}_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1 \times P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

3.3 AES의 수학적 배경

- P1 = 000100110, P2 = 10011110, modulus = 100011010 (nine bits).

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) $\oplus$ (00011011) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) $\oplus$ (00011011) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$\mathbf{P_1 \otimes P_2}$ **= (00100111)** $\oplus$ **(01001110)** $\oplus$ **(01000110) = 00101111**		

- Multiplication of poly.'s in $GF(2^n)$ is done using Shift-left and $\oplus$.

3.4 AES의 내부 구조

- 블록이 상태(State)의 형태로 표현
  - 상태는 원소가 한 바이트인 4 × 4행렬
  - AES의 한 블록이 “EASYCRYPTOGRAPHY”인 경우

16 바이트

E	A	S	Y	C	R	Y	P	T	O	G	R	A	P	H	Y
04	00	12	18	02	11	18	0F	13	0E	06	11	00	0F	07	18

(텍스트를 16진수로 표현)

상태(State) 4×4

04	02	13	00
00	11	0E	0F
12	18	06	07
18	0F	11	18

3.4 AES의 내부 구조

- Substitute Bytes(SubBytes) 계층
  - 한 원소가 16진수로 (xy)인 경우 상위 4 비트 값인 x가 S-Box의 행을 결정하고 하위 4 비트 값인 y가 열을 결정

	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	CB	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

19	11	00	14
19	13	C6	12
04	04	00	23
00	12	0C	08

상태 (State)

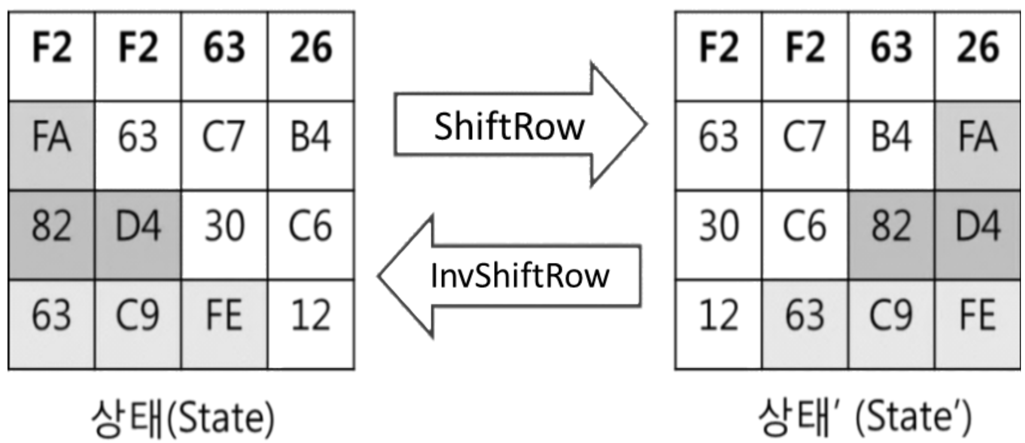
SubByte

D4	82	63	FA
D4	7D	B4	C9
F2	F2	63	26
63	C9	FE	30

상태' (State')

3.4 AES의 내부 구조

- ShiftRows 계층



3.4 AES의 내부 구조

- MixColumns 계층
  - SubBytes 계층과 ShiftRows 계층은 바이트 단위로 처리
  - 충분한 분산 효과를 발생시키기 위하여, MixColumns 계층에서는 상태의 각 열을 비트 단위로 섞어 줌

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

$$s'_{0,0} = (02 \cdot s_{0,0}) \oplus (03 \cdot s_{1,0}) \oplus (01 \cdot s_{2,0}) \oplus (03 \cdot s_{3,0})$$
$$s'_{1,0} = (01 \cdot s_{0,0}) \oplus (02 \cdot s_{1,0}) \oplus (03 \cdot s_{2,0}) \oplus (01 \cdot s_{3,0})$$

.

.

.

$$s'_{3,3} = (03 \cdot s_{0,3}) \oplus (01 \cdot s_{1,3}) \oplus (01 \cdot s_{2,3}) \oplus (02 \cdot s_{3,3})$$

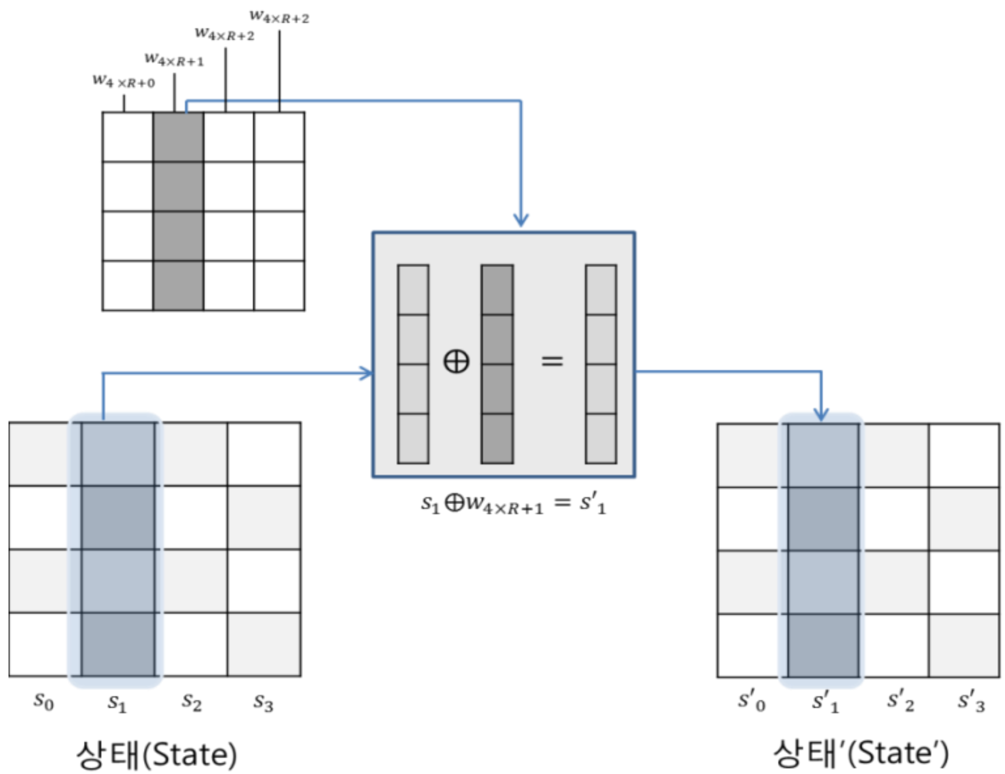
3.4 AES의 내부 구조

- Inverse MixColumns 계층

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}^{-1} = \begin{bmatrix} 0\mathrm{E} & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

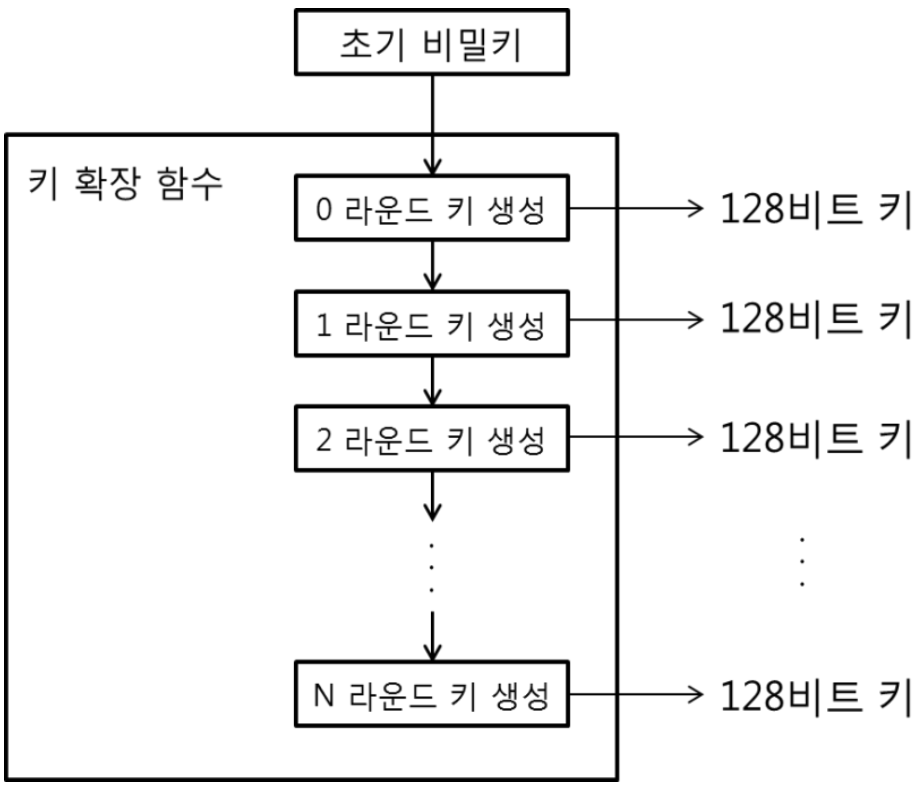
3.4 AES의 내부 구조

- AddRoundKey



3.4 AES의 내부 구조

- 키 확장(Key Expansion)



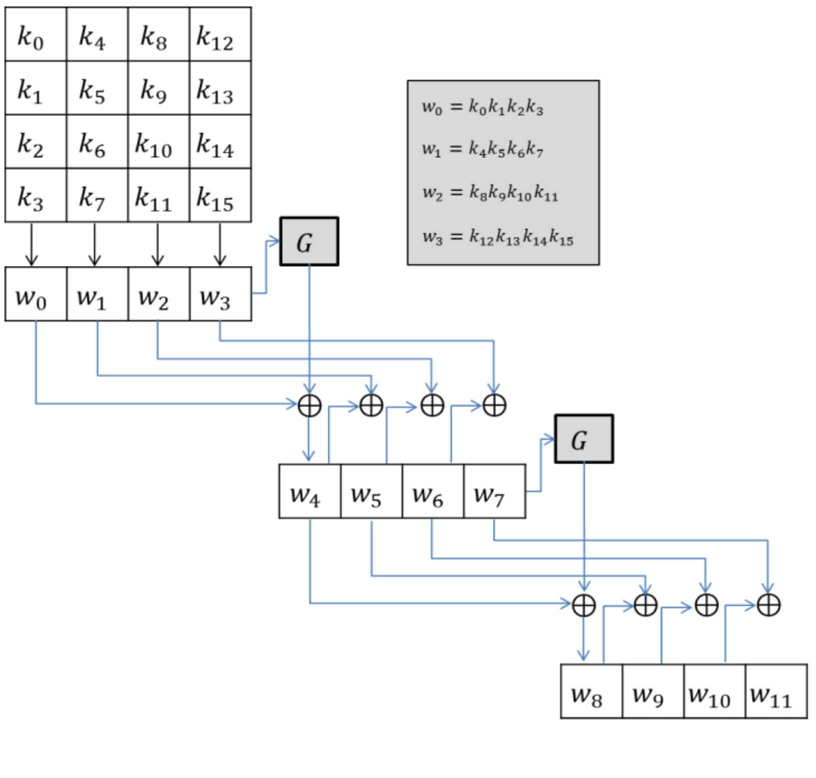
3.4 AES의 내부 구조

- 키 확장 (Key Expansion)

라운드	워 드
0라운드	w_0, w_1, w_2, w_3
1라운드	w_4, w_5, w_6, w_7
2라운드	w_8, w_9, w_{10}, w_{11}
…	…
N라운드	w_{4N}, w_{4N+1}, w_{4N+2}, w_{4N+3}

3.4 AES의 내부 구조

- Key Expansion
  - $G(w_{4i-1}) = \text{SubWord}(\text{RotWord}(w_{4i-1})) \oplus RCons,$



Nonlinearity
→ DES의 보수 특성과 취약키 존재하지 않음

- Animation of AES

3.5 AES의 분석

- 안전성
  - 취약키(Weak Keys)와 차분 분석 방법(Differential Cryptanalysis), 선형 분석 방법 (Linear Cryptanalysis) 등을 이용한 공격에 대해 안전
  - 2011년 “Biclique 암호분석”? →
    - 소요시간 : 2^{126}
    - AES에 대한 가장 최선의 공격이라고 믿었던 전사적 공격(2^{128}의 연산이 필요)보다 4배정도 효율적인 공격
      - 2^{88} bits data 사용 >지구에 존재하는 모든 컴퓨터의 저장 data
    - 이는 키 길이가 56비트인 DES 암호 알고리즘에 대한 전수 조사 공격을 2^{70}번을 실시하는 것과 동일
    - Bruce Shneier : “공격 수법은 언제나 진화한다”
    - 현재 AES을 대체할 다른 암호가 필요한 것은 아니며 향후 새로운 공격에 대비하여 AES의 라운드 수를 증가시켜야 한다고 주장

3.6 AES 구현

- DES와는 다르게 AES는 소프트웨어로도 효율적으로 구현되도록 설계
  - 바이트 단위의 연산을 주로 수행
  - 스마트카드와 같은 8 비트 프로세서에 효율적으로 설계
  - BUT 현재 PC에 주로 사용되는 32 비트나 64 비트 프로세서에서는 비효율적
    - Rijndael의 설계자들은 효율적인 소프트웨어 구현방법을 제시
      - 한 라운드의 입력 값에 대응되는 출력 값을 표를 통해서 찾으면 되며, 모두 4개의 표가 존재
      - 표의 입력 값은 32 비트이며 이러한 표를 특별히 T−Box라 부름
      - 1.2−GHz 인텔 프로세서를 사용하며 초당 50MB 정도를 처리.
  - AES는 DES보다 더 많은 하드웨어 자원을 요구
    - 집적 회로의 집적도(Integration Density)가 매우 높아지고 있으며 현재 상용 AES ASIC의 경우 초당 10−Ghz이상의 처리능력