AES
(Advanced Encryption Standard)

컴퓨터공학부 김상원

https://youtu.be/uoURZyjjqes

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

AES 역사

AES 주요 특징

AES 알고리즘

Q & A

AES 역사

1997년 NIST는 새로운 블록 암호(Advanced Encryption Standard)에 대한 제안을 공고
DES와 다르게 모든 것을 공개적으로 하고 NSA도 공개적으로 관여함
DES와 다르게 전문가들도 적극적으로 참여

AES 후보에 대한 요구사항
128비트 블록 길이
3종류 키 길이 : 128, 192, 256 bits
알려진 알고리즘에 비해 우수한 안정성
효율적인 S/W와 H/W구현

2001년 NIST는 Rijndael(“rain doll”로 발음)을 새로운 AES 표준으로 발표

AES 주요 특징

반복 구조(Iterated Block Cipher)
대입-치환 네트워크(Substitution-Permutation Network; SPN)
블록 크기 : 128 bits
키 길이 : 128, 192, 256 bits (블록 크기와 상관없음)
반복(round)은 가변 (키 길이에 따라 결정)
10 if K = 128 bits
12 if K = 192 bits
14 if K = 256 bits
각 round에서 4가지 함수 사용
1. ByteSub (nonlinear layer)
2. ShiftRow (linear mixing layer)
3. MixColumn (nonlinear layer)
4. AddRoundKey (key addition layer)

128비트 블록을 4 x 4 byte array로 취급

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

AES 알고리즘

State = X
AddRoundKey(State, Key_0) (op1)
for i = 1 to r – 1
    ByteSub(State, S-box) (op2)
    ShiftRows(Stae) (op3)
    MixColumns(State) (op4)
    AddRoundKey(State, Key_i)
ByteSub(State, S-box)
ShitRows(State)
AddRoundKey(State, Key_r)
Y = State

AES 알고리즘

State = X
AddRoundKey(State, Key_0) (op1)
For I = 1 to r – 1
ByteSub(State, S-box) (op2)
ShiftRows(Stae) (op3)
MixColumns(State) (op4)
AddRoundKey(State, Key_i)
ByteSub(State, S-box)
ShitRows(State)
AddRoundKey(State, Key_r)
Y = State

AddRoundKey

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \oplus \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix}$$

$$= \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}.$$

AES 알고리즘

State = X
AddRoundKey(State, Key_0) (op1)
For I = 1 to r – 1
ByteSub(State, S-box) (op2)
ShiftRows(Stae) (op3)
MixColumns(State) (op4)
AddRoundKey(State, Key_i)
ByteSub(State, S-box)
ShitRows(State)
AddRoundKey(State, Key_r)
Y = State

ByteSub

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \longrightarrow \texttt{ByteSub} \longrightarrow \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}.$$

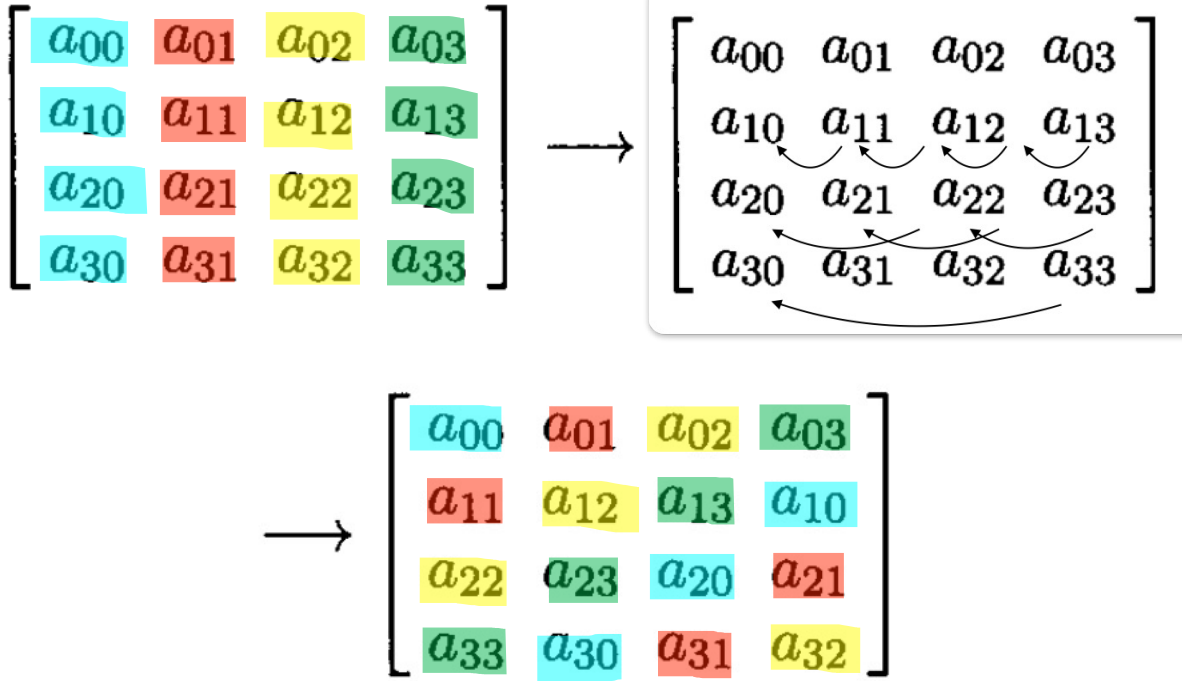
Table 3.5: AES ByteSub

	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

AES 알고리즘

State = X
AddRoundKey(State, Key_0) (op1)
For I = 1 to r – 1
ByteSub(State, S-box) (op2)
ShiftRows(Stae) (op3)
MixColumns(State) (op4)
AddRoundKey(State, Key_i)
ByteSub(State, S-box)
ShitRows(State)
AddRoundKey(State, Key_r)
Y = State

ShiftRows



AES 알고리즘

State = X
AddRoundKey(State, Key_0) (op1)
For I = 1 to r – 1
ByteSub(State, S-box) (op2)
ShiftRows(Stae) (op3)
MixColumns(State) (op4)
AddRoundKey(State, Key_i)
ByteSub(State, S-box)
ShitRows(State)
AddRoundKey(State, Key_r)
Y = State

MixColumns

$$\begin{bmatrix} a_{0i} \\ a_{1i} \\ a_{2i} \\ a_{3i} \end{bmatrix} \text{X} \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} b_{0i} \\ b_{1i} \\ b_{2i} \\ b_{3i} \end{bmatrix} \quad \text{for } i = 0, 1, 2, 3.$$

AES 알고리즘

MixColumns

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & ED \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

{02} * {87} ⊕ {03} * {6E} ⊕ {01} * {46} ⊕ {01} * {A6}

02 = 0000 0010 = X
87 = 1000 0111 = $X^7 + X^2 + X + 1$

{02} * {87} = X * ($X^7 + X^2 + X + 1$)
= $X^8 + X^3 + X^2 + X$
= $X^4 + X^3 + X + 1 + X^3 + X^2 + X$
= $X^4 + X^2 + 1$
= 0001 0101

Use irreducible Polynomial Theoreom, GF (2^3)
$X^8 = X^4 + X^3 + X + 1$

Q & A