การเข้ารหัสลับแบบ Advance Encryption Standard

เป็นการเข้ารหัสลับแบบบล็อกที่ Nationation Institute of Standard and Technology ประเทศสหรัฐอเมริการับเป็นมาตรฐาน การเข้ารหัสลับแบบ Advance Encryption Standard: AESเสนอโดย J. Daemen และ V.Rijmen เพื่อรับการคัดเลือกเป็นการเข้ารหัสลับมาตรฐานแทนการเข้ารหัสลับแบบ Data Encryption Standard ที่ใช้มากว่า 30 ปี โดย AES เป็นการรหัสลับแบบบล็อกขนาด 128 บิตโดยสามารถใช้กุญแจได้ขนาด 128 บิต 196 บิตและ 256 บิตโดยมีรอบการทำงานคือ 10,12,14 รอบตามลำดับ สำหรับขั้นตอนวิธีเริ่มต้นค่าอินพุตขนาด 128 บิตหรือ 16 ไบต์จะถูกจัดให้เป็นเมตริกซ์ขนาดสถานะ S ขนาด 4×4 ไบต์ดังรูป

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

สำหรับการทำงานในแต่ละรอบประกอบด้วย

1.การแทนค่าด้วย S-Box

ข้อมูลในเมตริกซ์สถานะ S แทนค่าด้วย S-box ที่กำหนดไว้เพื่อให้ข้อมูลเกิด confusion

2.การเลื่อนแถว ShiftRows

เป็นการเลื่อนแถว(row: r_i) ของเมตริกซ์ S ไปทางซ้าย i ตำแหน่งโดย $i = 0,1,2,3$

3.การผสมหลัก MixColumns

หลังจากทำการเลื่อนแถวแล้ว ในขั้นนี้ค่าในหลักในเมตริกซ์สถานะ S ถูกผสมเข้าด้วยกันในขั้นตอน 2-3 เป็นการทำให้ข้อมูลที่เข้ารหัสเกิด diffusion

4.การบวกกุญแจย่อย AddRoundKey

ค่าของเมตริกซ์สถานะบวกแบบมอดุโล 2 เข้ากับกุญแจโดยแต่รอบค่ากุญแจจะถูกขยายให้เป็นกุญแจใหม่ทุกรอบ

แสดงขั้นตอนวิธีการเข้ารหัสลับแบบ AES

```
AddRoundKey(S,K0)
For i to 9 do
    SubBytes(S)
    ShiftRows(S)
    MixColumns(S)
   AddRoundKey(S,K i)
End
SubBytes(S)
ShiftRows(S)
AddRoundKey(S, K10)
```

การแทนค่าด้วย S-Box (SubBytes)

ค่าอินพุตของการแทนค่ามีขนาด 8 บิตแทนด้วยพหุนามได้

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0x^0 = \sum_{i=0}^{7} b_i x^{i+1}$$

โดย b_i เป็นสัมประสิทธิ์ที่เกิดค่าจากไบนารี

การแทนค่าด้วย S-Box มีขั้นตอนดังนี้

1.ทำการหาค่าผกผันการคูณของค่าอินพุต 8 บิตภายใต้มอดุโล

$$P(x) = x^8 + x^4 + x^3 + x + 1$$

2.จากข้อ 1 ทำการแปลง Affine ถ้า b_i' เป็นเอาท์พุตของข้อที่ 1 ขนาด 8 บิต แสดงสมการของการแปลง Affine ได้

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} mod2 \qquad (5)$$

ตัวอย่าง ให้อินพุตของ S-Box มีค่าเท่ากับ 3D หาค่าเอาท์พุต

จาก $3D = b(x) = x^5 + x^4 + x^3 + x + 1$

หา $\gcd(b(x), P(x))$

$x^8 + x^4 + x^3 + x + 1 = (x^3 + x^2)(x^5 + x^4 + x^3 + x^2 + 1) + (x^2 + x + 1)$

$(x^5 + x^4 + x^3 + x^2 + 1) = (x^3 + 1)(x^2 + x + 1) + x$

$(x^2 + x + 1) = (x + 1)(x) + 1$

ขยาย Euclidean

$1 = (x^2 + x + 1) + (x + 1)(x)$

$1 = (x^2 + x + 1) + (x + 1)\{(x^5 + x^4 + x^3 + x^2 + 1) + (x^3 + 1)(x^2 + x + 1)\}$

$1 = (x^4 + x^3 + x)(x^2 + x + 1) + (x + 1)(x^5 + x^4 + x^3 + x^2 + 1)$

$1 = (x^4 + x^3 + x)\{(x^8 + x^4 + x^3 + x + 1) + (x^3 + x^2)(x^5 + x^4 + x^3 + x^2 + 1)\} + (x + 1)(x^5 + x^4 + x^3 + x^2 + 1)$

$$1 = (x^4 + x^3 + x)(x^8 + x^4 + x^3 + x + 1) + (x^7 + x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1)$$

ค่าผกผันภายใต้ $x^8 + x^4 + x^3 + x + 1 = x^7 + x^5 + x^4 + x^3 + x + 1$

หรือเป็นค่าไบนารี =10111011 จากสมการ (1)

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} mod 2$$

เอาท์พุตแสดงได้ $b'_i = 00100111 = 27H$

ผลของการแทนค่าด้วย S-box เมื่ออินพุตเป็น $S_{r,c}$ โดย r,c เป็นค่าของบิต 7-4 และบิต 3-0 ตามลำดับ

	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	FC	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	CC	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	C7	C8	37	6D	8D	D5	4C	A9	6C	56	F4	CA	65	7A	AC	08
C	BA	78	25	2C	1C	AB	B4	C6	C8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	89	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

การเลื่อนแถว ShiftRows

เป็นการกระทำในแถวของแต่ละเมทริกซ์สถานะของข้อมูล จากบล็อกขนาด 128 บิต การแทนค่าด้วย S-box จำนวน 16 ไบต์แสดงได้

$$\begin{bmatrix} S_{0,0}S_{0,1}S_{0,2}S_{0,3} \\ S_{1,0}S_{1,1}S_{1,2}S_{1,3} \\ S_{2,0}S_{2,1}S_{2,2}S_{2,3} \\ S_{3,0}S_{3,1}S_{3,2}S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S_{0,0}S_{0,1}S_{0,2}S_{0,3} \\ S_{1,1}S_{1,2}S_{1,3}S_{1,0} \\ S_{2,2}S_{2,3}S_{2,0}S_{2,1} \\ S_{3,3}S_{3,0}S_{3,1}S_{3,2} \end{bmatrix} \qquad (6)$$

การเลื่อนแถวของเมทริกซ์ แถวที่ 2 เลื่อนซ้าย 1 ตำแหน่ง แถวที่ 3 เลื่อนซ้าย 2 ตำแหน่ง แถวที่ 3 เลื่อนซ้าย 3 ตำแหน่ง

การผสมหลัก MixColumns

ในขั้นตอนนี้เป็นกระทำในแต่ละหลักของเมทริกซ์สถานะจำนวน 4 ไบต์หรือขนาด 1 คำของจำนวน 32 บิต จากสมการ (2) แสดงเมตริกซ์จำนวน 1 หลักได้

$$\begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \qquad (7)$$

หลักของเมตริกซ์สามารถแทนได้ด้วยพหุนามลำดับ 3 ได้

$$s(x) = s_{3,c}x^3 + s_{2,c}x^2 + s_{1,c}x + s_{0,c} \qquad (8)$$

หลักที่ผสม $s'(x)$ ประสิทธิ์ของพหุนามจะเป็นค่าของแต่ละไบต์การกระทำการผสมหลักกระทำบนข้อมูล 4 ไบต์หรือเป็นการคูณพหุนามลำดับ 3 ภายใต้การมอดุโล $x^4 + 1$

$$s'(x) = c(x) \times s(x) mod(x^4 + 1) \qquad (9)$$

โดยพหุนาม $c(x)$ ที่ใช้ในทำการผสมหลักแสดงได้คือ

$$c(x) = c_3x^3 + c_2x^2 + c_1x + c_0 = '03'x^3 + '01'x^2 + '01'x + '02' \qquad (10)$$

จากการดำเนินการภายใต้ $x^4 + 1$ ผลของการคูณในสมการที่ (5) ที่มีค่าอันดับเกิน 3 ค่าสัมประสิทธิ์จะถูกนำมาบวกเข้ากับสัมประสิทธิ์ที่อยู่ในอันดับ 0-3 หรือแสดงได้คือ

$$x^i mod(x^4 + 1) = x^{i(mod4)} \qquad (11)$$

ดังนั้น

$$s'(x) = c(x) \times s(x) mod(x^4 + 1) = s'_{3,c}x^3 + s'_{2,c}x^2 + s'_{1,c}x + s'_{0,c} \qquad (12)$$

แสดงการกระทำการผสมหลักในรูปของเมทริกซ์

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 02\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \qquad (13)$$

หรือแสดงผลคูณเมทริกซ์ในรูป

$$\begin{aligned} s'_{0,c} &= ([02] \times s_{0,c}) \oplus ([03] \times s_{1,c}) \oplus s_{2,c} \oplus s_{3,c} \\ s'_{1,c} &= s_{0,c} \oplus ([02] \times s_{1,c}) \oplus ([03] \times s_{2,c}) \oplus s_{3,c} \\ s'_{2,c} &= s_{0,c} \oplus s_{1,c} \oplus ([02] \times s_{2,c}) \oplus ([03] \times s_{3,c}) \\ s'_{3,c} &= ([03] \times s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus ([02] \times s_{3,c}) \end{aligned} \qquad (14)$$

สำหรับสังเกตุเพื่อให้สะดวกในการกระทำทางฮาร์ดแวร์การคูณของเมทริกซ์กระทำเพียงเลื่อน 1 บิตและ 2 บิตและบวกเท่านั้น

ตัวอย่าง เมทริกซ์สถานะของข้อมูล ก่อนผสมหลักแสดงการผสมของหลักที่ 1

$$S = \begin{bmatrix} D4 & E0 & B8 & 1E \\ EO & B4 & 41 & 27 \\ 5D & 52 & 11 & 98 \\ 30 & AE & F1 & E5 \end{bmatrix} \qquad (15)$$

จากสมการ (10) แสดง $s'_{0,c}$ที่เกิดจากการผสมกันของหลักทั้งหมดขนาด 4 ไบต์หรือ 32 บิตคำ

$$s'_{0,c} = ([02] \times [D4]) \oplus ([03] \times [E0]) \oplus [5D] \oplus [30]) = 04$$

จากการคูณของสัมประสิทธิ์แต่ละไบต์เป็นการคูณภายใต้พหุนามที่เป็นตัวกำเนิด $x^8 + x^4 + x^3 + x + 1$ หรือแสดงการคูณแต่ละไบต์ในรูปพหุนาม

$s'_{0,c} = x(x^7 + x^6 + x^4 + x^2) \oplus (x + 1)(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) \oplus 1(x^6 + x^4 + x^3 + x^2 + 1) \oplus (x^5 + x^4) = x^2$

แสดงผลของหลักทั้งหมด

$$s' = \begin{bmatrix} 04 & E0 & 48 & 28 \\ 66 & CB & F8 & 06 \\ 81 & 19 & D3 & 26 \\ E5 & 94 & 7A & 4C \end{bmatrix}$$