Ασκηση: Υλοποιηση AES.
Εργασια Φοιτητη: Βασιλειος Ριζεακος

Υλοποίηση 1ου βήματος του AES (Advanced Encryption Standard)

Μας δίνεται το $plaintext = \begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix}$

με κλειδί κρυπτογράφησης $key = \begin{bmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{bmatrix}$.

Γνωρίζουμε το S-Box ότι είναι η μήτρα:

	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

Δημιουργία 1st RoundKey

Έχουμε: $w_{0-3} = \begin{bmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{bmatrix}$.

$$g(w[3]) = S\left(\begin{bmatrix} 01 \\ 01 \\ 01 \\ 01 \end{bmatrix}\right) \oplus \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 7C \\ 7C \\ 7C \\ 7C \end{bmatrix} \oplus \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 7D \\ 7C \\ 7C \\ 7C \end{bmatrix}.$$

Άρα έχουμε το πρώτο roundkey να ισούται με:

$$w_{4-7} = [\mathrm{w}[0] \oplus \mathrm{g}(\mathrm{w}[3]),\ \ \mathrm{w}[1] \oplus \mathrm{w}[4],\ \ \mathrm{w}[2] \oplus \mathrm{w}[5],\ \ \mathrm{w}[3] \oplus \mathrm{w}[6]] = \begin{bmatrix} 7C & 7D & 7C & 7D \\ 7D & 7C & 7D & 7C \\ 7D & 7C & 7D & 7C \\ 7D & 7C & 7D & 7C \end{bmatrix}.$$

State Matrix

Με την πράξη της XOR του plaintext και του roundkey παίρνουμε:

$$cypher = \begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix} \oplus \begin{bmatrix} 7C & 7D & 7C & 7D \\ 7D & 7C & 7D & 7C \\ 7D & 7C & 7D & 7C \\ 7D & 7C & 7D & 7C \end{bmatrix} = \begin{bmatrix} 7C & 79 & 74 & 71 \\ 7C & 79 & 74 & 71 \\ 7F & 7A & 77 & 72 \\ 7E & 7B & 76 & 73 \end{bmatrix}.$$

SubBytes

Τώρα μέσω του S-Box παίρνουμε τη state matrix:

$$SM = \begin{bmatrix} 10 & B6 & 92 & A3 \\ 10 & B6 & 92 & A3 \\ D2 & DA & F5 & 40 \\ F3 & 21 & 38 & 8F \end{bmatrix}.$$

ShiftRows

Τώρα, μετατοπίζουμε την κάθε σειρά της state matrix κατά 0, 1, 2 και 3 αντίστοιχα:

$$SM = \begin{bmatrix} 10 & B6 & 92 & A3 \\ B6 & 92 & A3 & 10 \\ F5 & 40 & D2 & D2 \\ 8F & FE & 21 & 38 \end{bmatrix}.$$

MixColumns

Τελευταίο βήμα του πρώτου σταδίου είναι ο υπολογισμός του γινόμενου πινάκων:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 10 & B6 & 92 & A3 \\ B6 & 92 & A3 & 10 \\ F5 & 40 & D2 & D2 \\ 8F & FE & 21 & 38 \end{bmatrix}$$

Η πράξη που επιτελείται εδώ είναι η εξής. Π.χ. το γινόμενο στην θέση (1,1) υπολογίζεται ως:

$S_{1,1} = (02 \cdot 10) \oplus (03 \cdot B6) \oplus (01 \cdot F5) \oplus (01 \cdot 8F) = (00100000) \oplus (11011010) \oplus (11110101) \oplus (10001111) = 1000000 = 80.$

Πράττοντας παρομοίως για τα υπόλοιπα 15 στοιχεία του πίνακα, παίρνουμε το τελικό αποτέλεσμα, τη τελική state matrix του 1ου σταδίου:

$$SM = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 10 & B6 & 92 & A3 \\ B6 & 92 & A3 & 10 \\ F5 & 40 & D2 & D2 \\ 8F & FE & 21 & 38 \end{bmatrix} = \begin{bmatrix} 80 & 29 & 32 & 9C \\ EC & 7B & 83 & CD \\ DD & D1 & F6 & 5F \\ 6D & EE & 85 & 57 \end{bmatrix}.$$