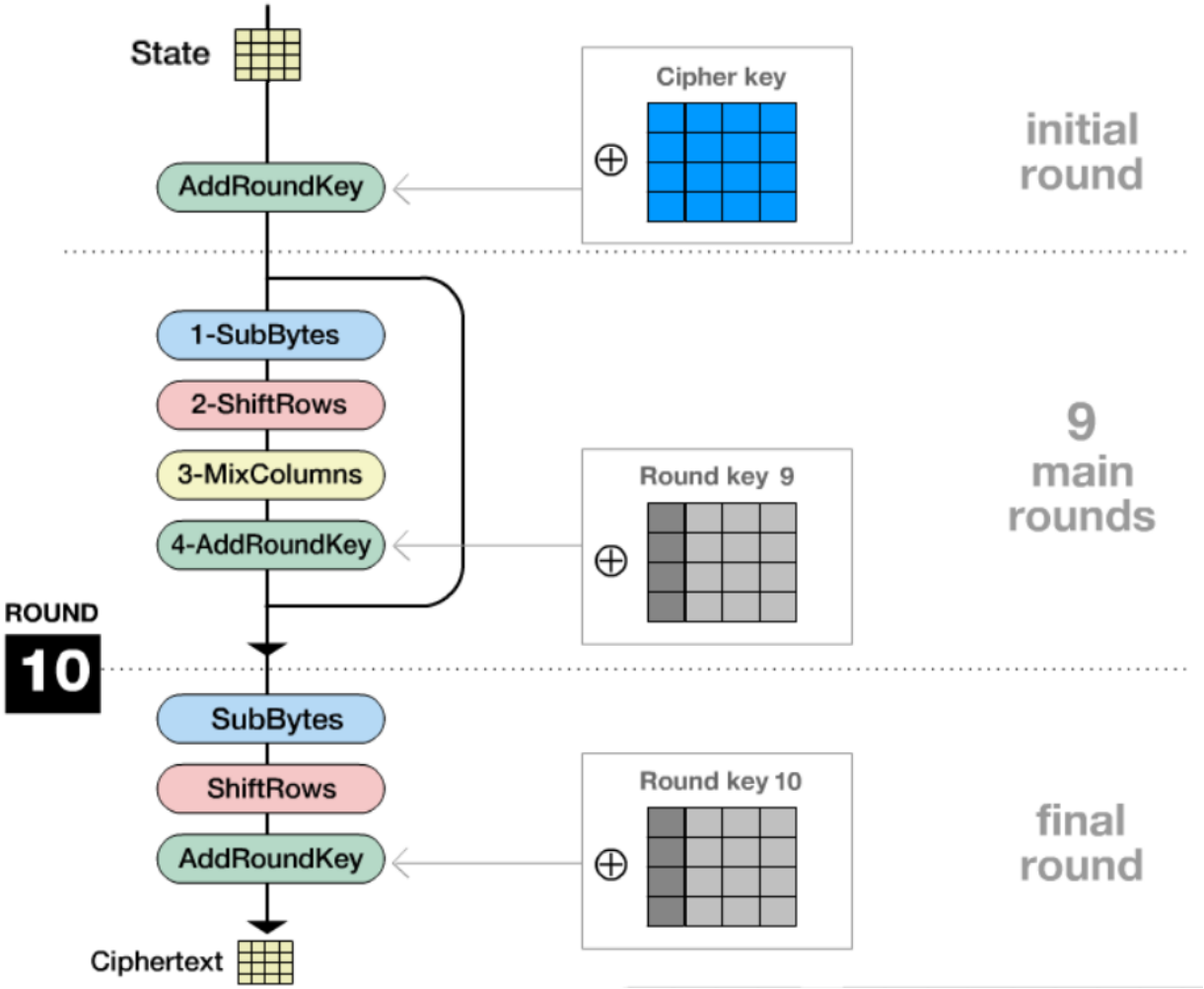
Algoritmi AES - Procesi i enkriptimit

AES është një specifikim për enkriptimin e të dhënave elektronike i krijuar nga Instituti Kombëtar i Standardeve dhe Teknologjisë në SHBA (NIST) në 2001.Si fitues për standartin AES në vjeshtën e vitit 2000 është zgjedhur algoritmi Rijndael, dizajnuesit e të cilit janë Johan Daemen dhe Vincet Rijmen. Rijndael është Block Cipher, që nuk është bazuar në dizajnin themelor të Feistel Cipher, megjithatë edhe te ky algoritëm vërehet ngjajshmëri e madhe me algoritmin DES. Te ai shfrytëzohet numri i raundeve të përsëritur me të cilën fitohet siguria më e madhe, por çdo raund përbëhet prej zëvendësimeve dhe permutacioneve, por edhe prej fazës së mbledhjes së çelësave. Përveç kësaj Rijndael ka strukturë të fortë matematikore, që rrjedh prej faktit se pjesa më e madhe prej operacioneve të tij bazohet në operacionet aritmetike të fushës F_2b. AES përdoret gjerësisht sot pasi është shumë më i fortë se DES dhe DES i trefishtë pavarësisht se është më i vështirë për të zbatuar. Madhësia kryesore mund të jetë 128/192/256 bit. Kripton të dhënat në blloqe me 128 bit secili. Kjo do të thotë se merr 128 bit si hyrje dhe nxjerr 128 bit tekst të koduar si dalje. Numri i raundeve varet nga gjatësia e çelësit. Çelësi 128 bit - 10 raunde, 192 bit - 12 raunde dhe 256 bit - 14 raunde.

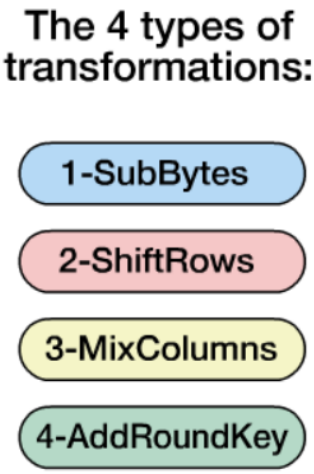
Algoritmi AES



AES e konsideron çdo bllok si një matric 16 bajt (4 bajt x 4 bajt = 128).

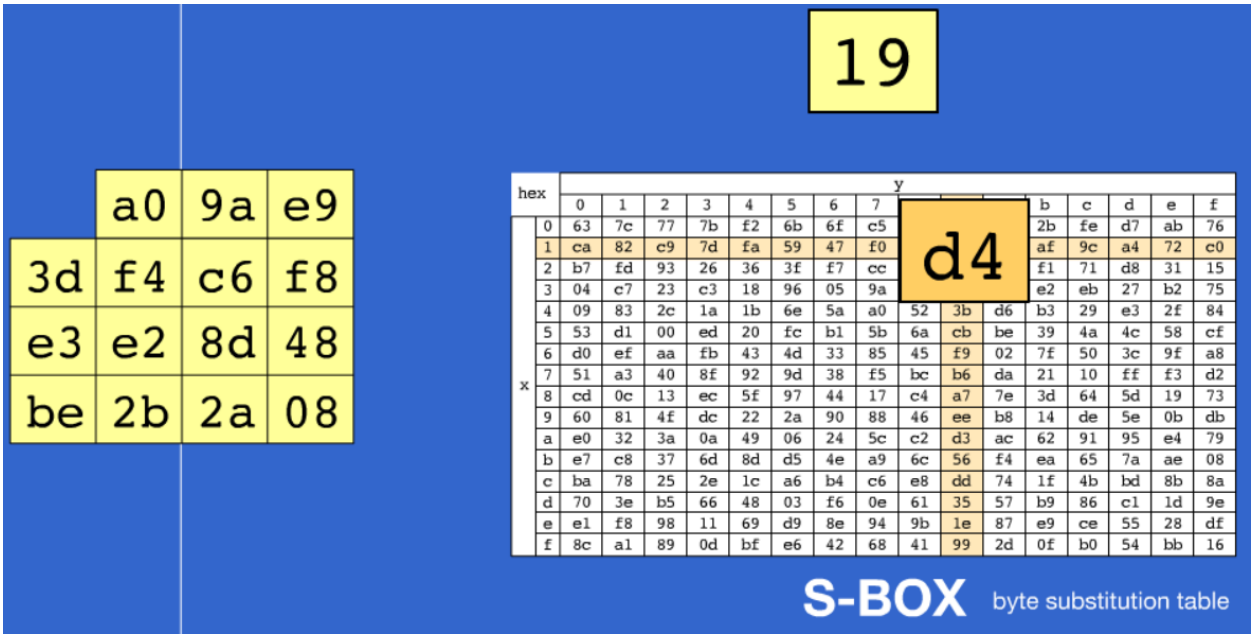
```
[ b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15 ]
```

Çdo raund përbëhet nga 4 hapa-transformime që duhet bëhen:



1- Transformimi Sub bytes

Ky hap zbaton zëvendësimin. Në këtë hap çdo bajt zëvendësohet me një bajt tjetër. Ajo kryhet duke përdorur një tabelë kërkimi të quajtur edhe S-box. Në këtë Në këtë rast vlera 19 në heksadecimal do të jetë d4 sepse tek tabela ne me prerjen e rreshtit 1 dhe kolonën 9 gjendet vlera d4. Njejt veprohet edhe me vlerat e tjera të matricës 4x4.



d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

hex	y															
	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

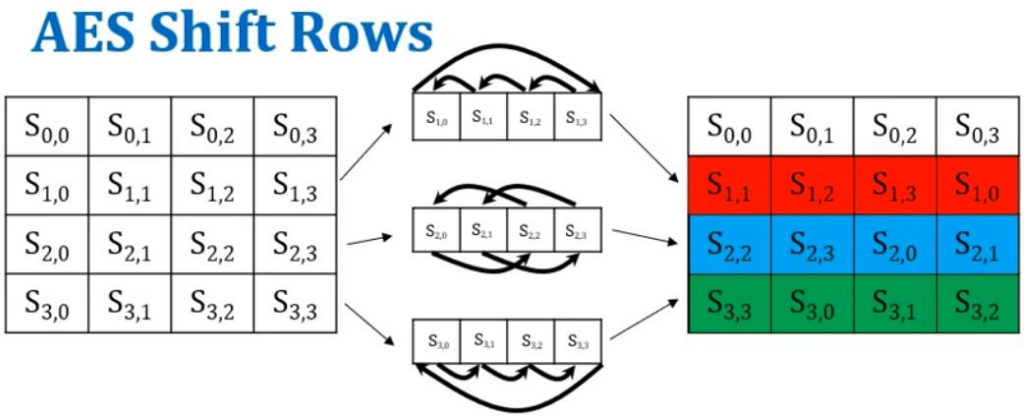
x

S-BOX byte substitution table

2- Transformimi ShiftRows

Në këtë hap çdo rresht zhvendoset në një numër të caktuar herësh.

- Rreshti i parë nuk duhet zhvendosur
- Rreshti i dytë zhvendoset një herë në të majtë.
- Rreshti i tretë zhvendoset dy herë në të majtë.
- Rreshti i katërt zhvendoset tri herë në të majtë.



Nga shembulli ynë kemi:

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

3. Transformimi MixColumns

Ky hap është një shumëzim matrice. Çdo kolonë shumëzohet me një matricë specifike dhe kështu pozicioni i secilit bajt në kolonë ndryshon.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

$*$

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

$=$

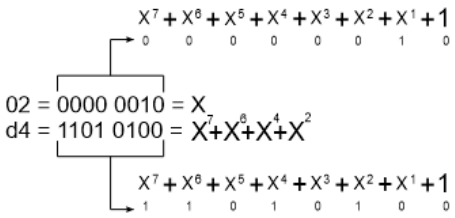
$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,0}$	$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$
$S'_{2,0}$	$S'_{2,1}$	$S'_{2,2}$	$S'_{2,3}$
$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$	$S'_{3,3}$

Nga shembulli ynë ne kemi:

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Meret kolona e parë nga matrica dhe shumëzohet me matricën e dhënë si më poshtë

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$



$\{02\}*\{d4\}=X*(X^7+X^6+X^4+X^2)$

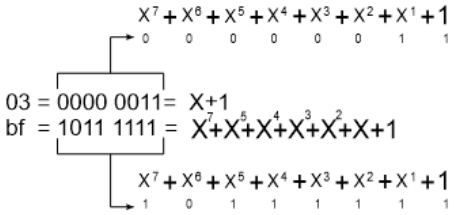
$=X^8+X^7+X^5+X^3$

$= X^4+X^3+X+1+X^7+X^5+X^3$

$= X^7+X^5+X^4+X+1$ $\quad X^7+X^6+X^5+X^4+X^3+X^2+X^1+1$ (1 0 1 1 0 0 1 1)

$= 10110011$

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



$\{03\}*\{d4\}=(X+1)*(X^7+X^5+X^4+X^3+X^2+X+1)$

$=X^8+X^6+X^5+X^4+X^3+X^2+X+X^7+X^5+X^4+X^3+X^2+X+1$

$= X^4+X^3+X+1+X^6+X^4+X^3+X^2+X+1+X^7+X^5+X^4+X^3+X^2+X+1$

$= X^7+X^6+X^4+X^3+X$ $\quad X^7+X^6+X^5+X^4+X^3+X^2+X^1+1$ (1 1 0 1 1 0 1 0)

$= 11011010$

$X^8 = X^4+X^3+X+1$

$\{02\}*\{d4\}=1\ 0\ 1\ 1\ 0\ 0\ 1\ 1$

$\{03\}*\{d4\}=1\ 1\ 0\ 1\ 1\ 0\ 1\ 0$ ⊗ XOR

$5d=0\ 1\ 0\ 1\ 1\ 1\ 0\ 1$

$30=0\ 0\ 1\ 1\ 0\ 0\ 0\ 0$

$0\ 0\ 0\ 0\ 0\ 1\ 0\ 0$

Vlera e $S_{0,0}$ = 00000100 = 04, në të njëjtën mënyrë veprojmë edhe me shtyllat e tjera dhe ne fund fitojmë matricën:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

=

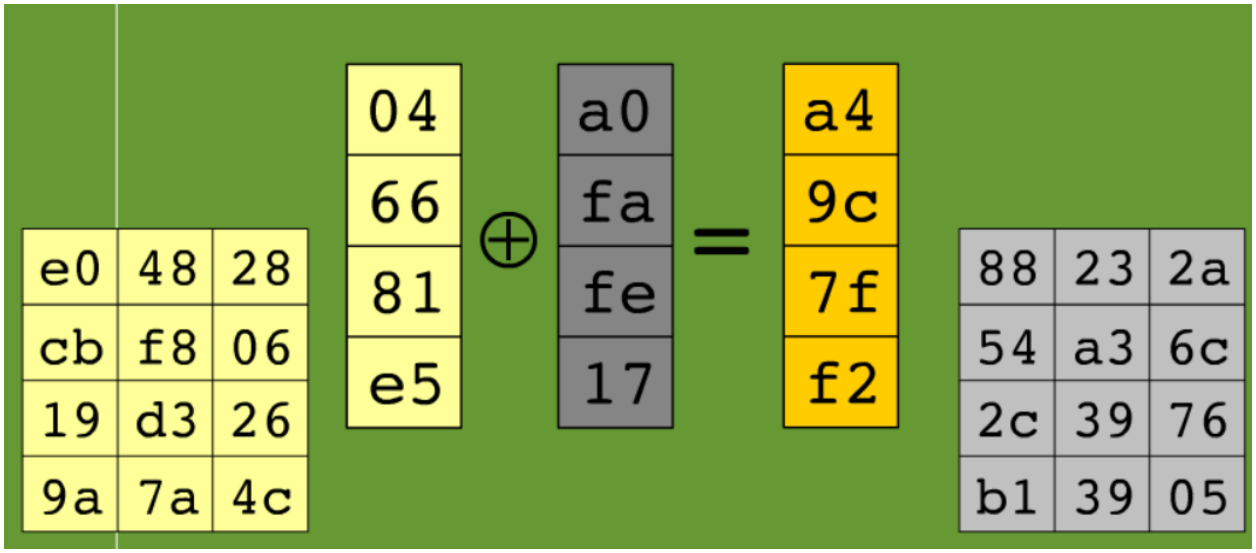
04	?	?	?
?	?	?	?
?	?	?	?
?	?	?	?

dhe ne fund fitohet kjo matricë

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

4. Add round Key

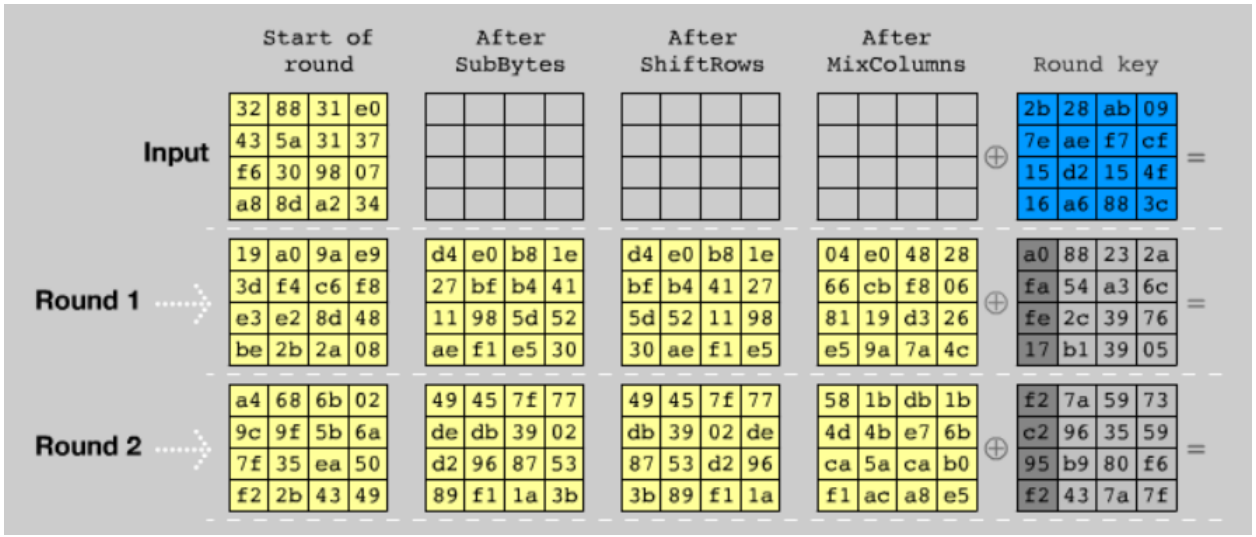
Tani rezultati i prodhimit të fazës së mëparshme është bërë XOR me çelësin e rrethit të përshtatshëm.



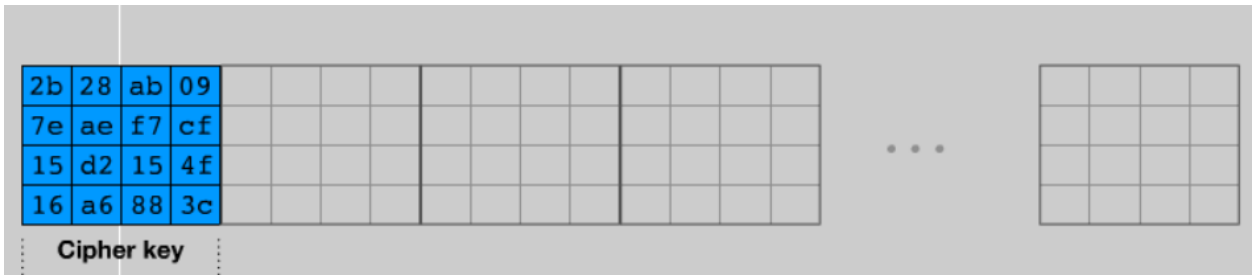
Njejtë veprohet edhe me kolonat e tjera kolona e dytë e state bëhet xor me kolonën e dytë të çelësit round key etj, dhe në dund fitojmë:

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

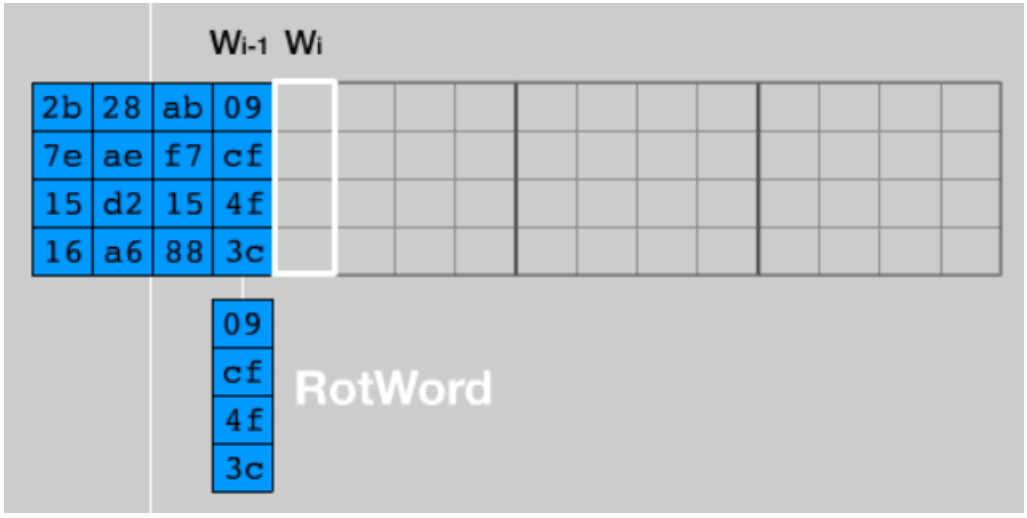
Këto transformime aplikohen në shtet edhe për 9 raunde të tjera. Raundi përfundimtar nuk përfshin transformimin MixColumns.



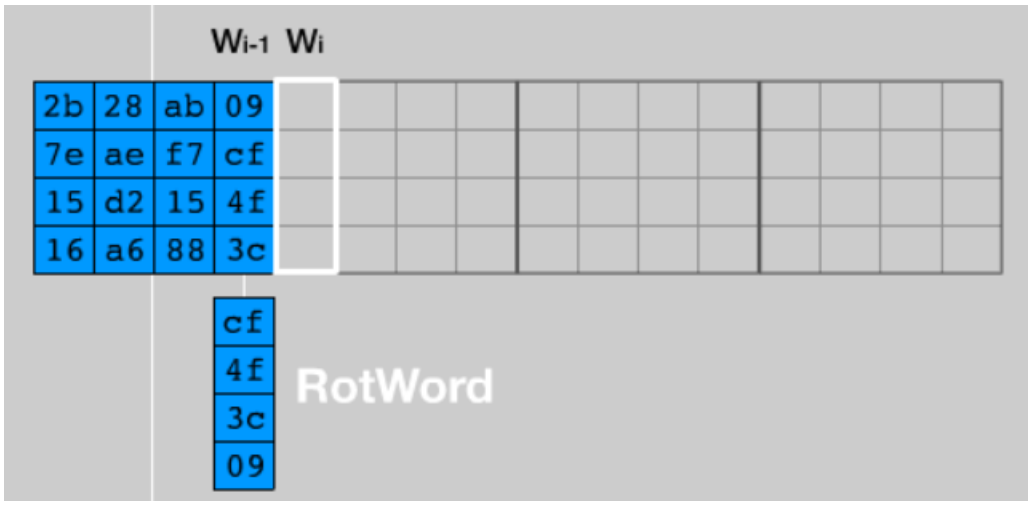
Çelësi i roundit të parë është fituar nga çelësi bazë i dhënë në fillim në këtë mënyrë:



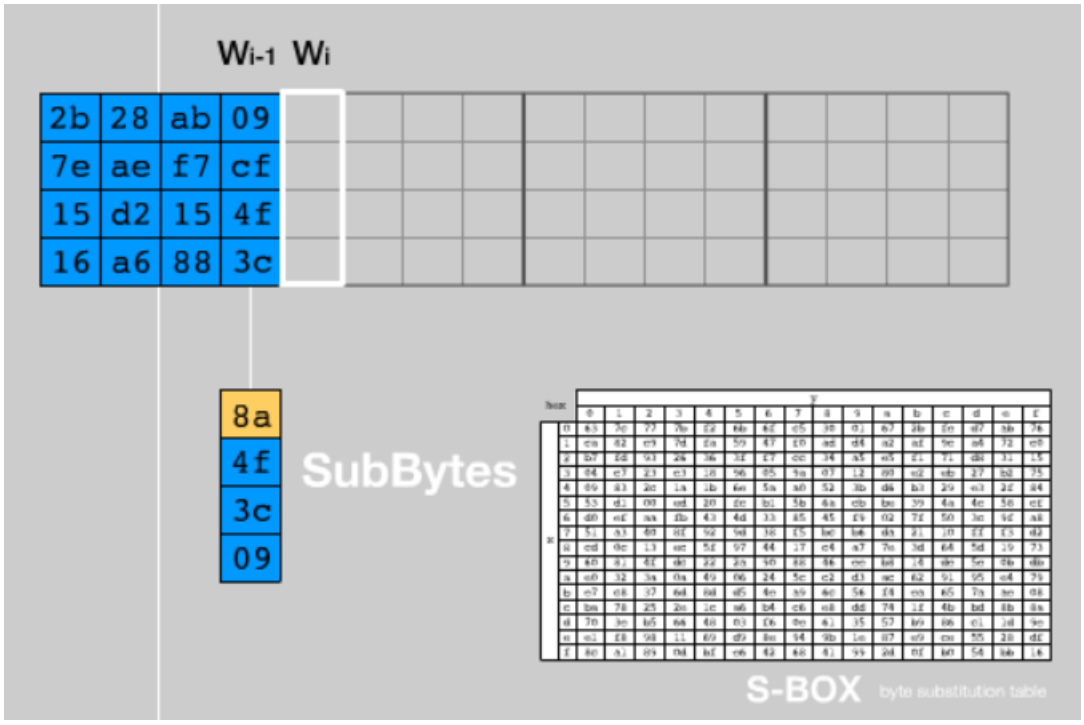
Nga çelësi bazë mirët kolona e fundit dhe lëvizet për1 vertikalisht



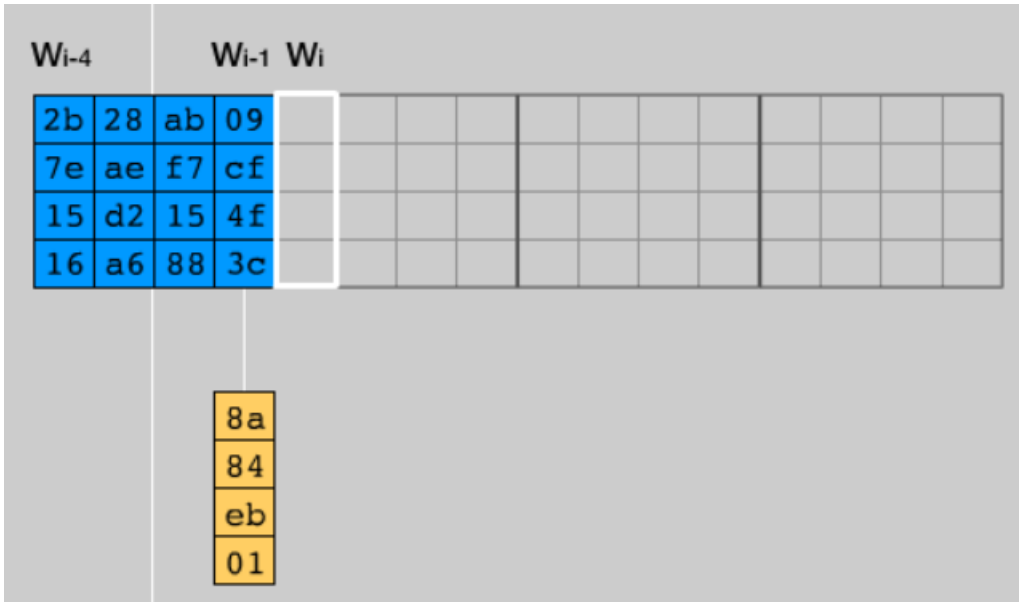
Dhe fitohet:



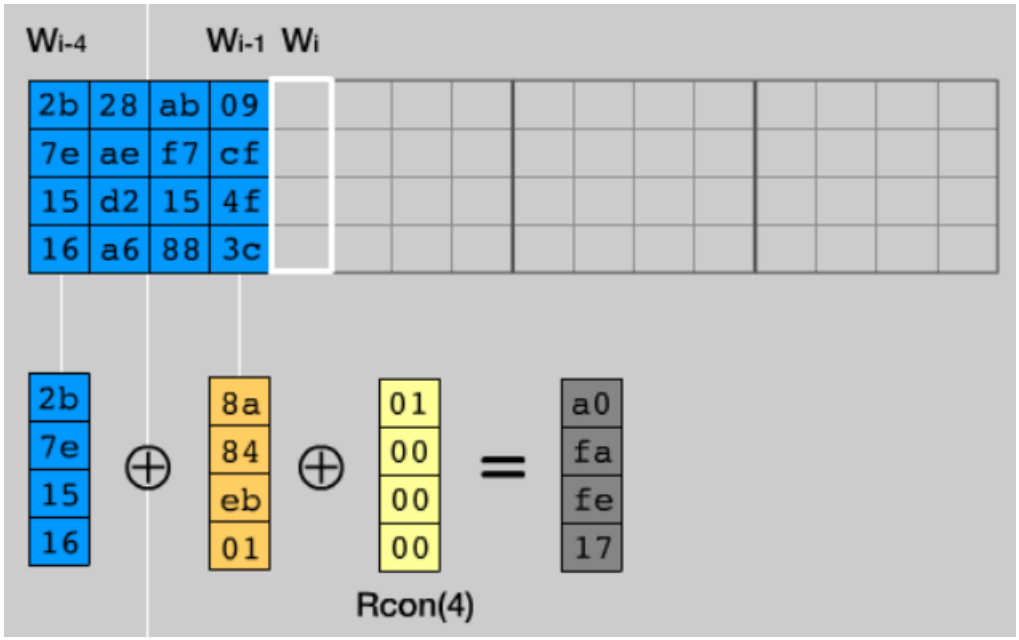
Pastaj numrat e kësaj kolone shikohen në tabelën S-BOX

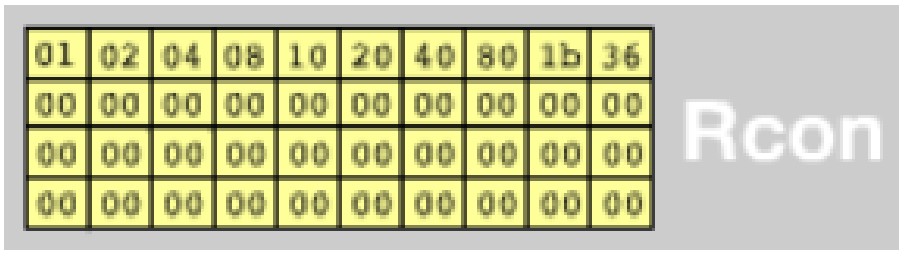


Dhe fitohet:

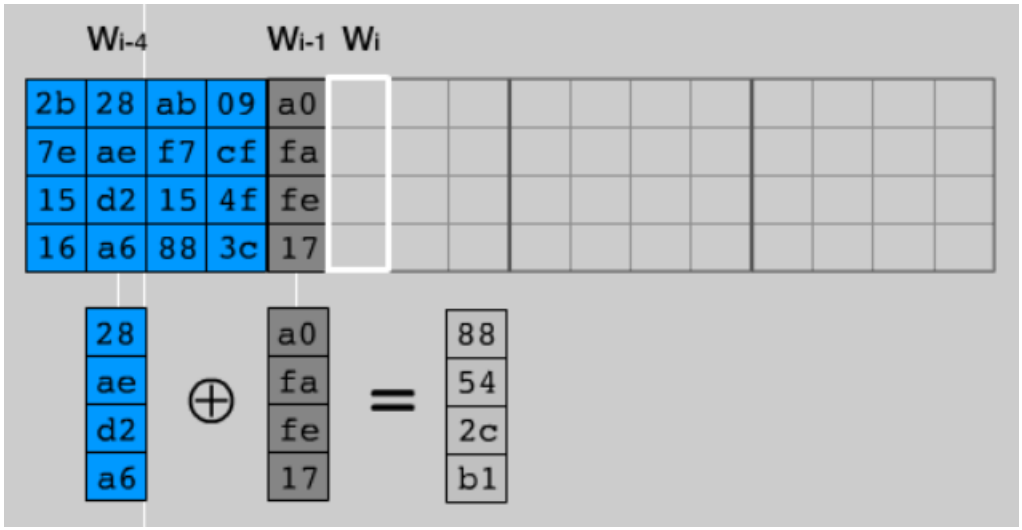


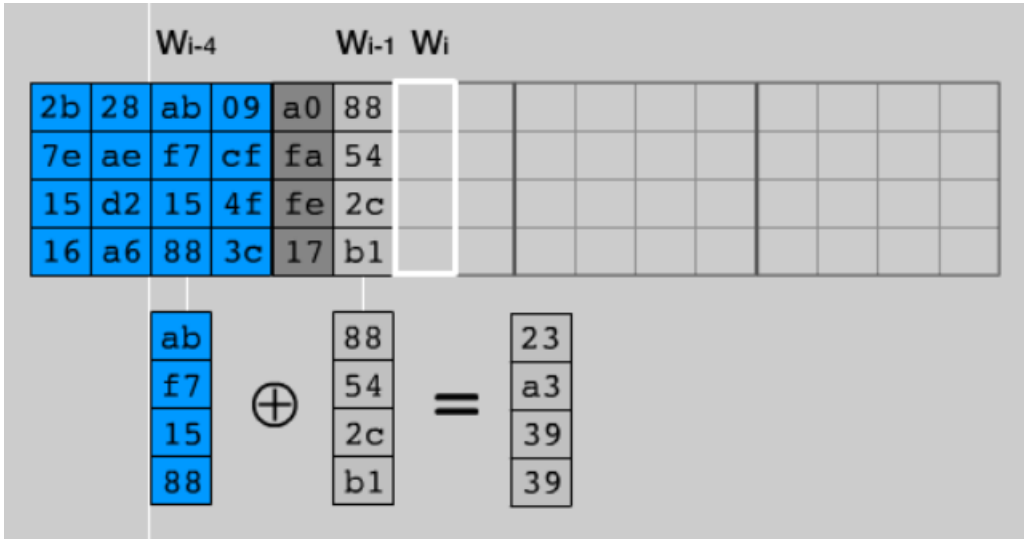
Pastaj kolona e parë bëhet xor me rezultatin e fituar më parë dhe round konstanten Rcon

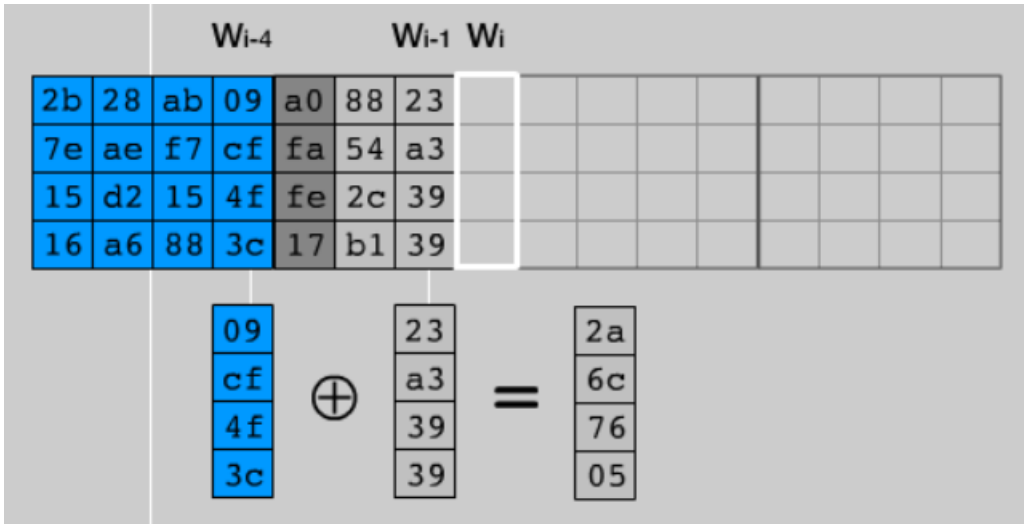




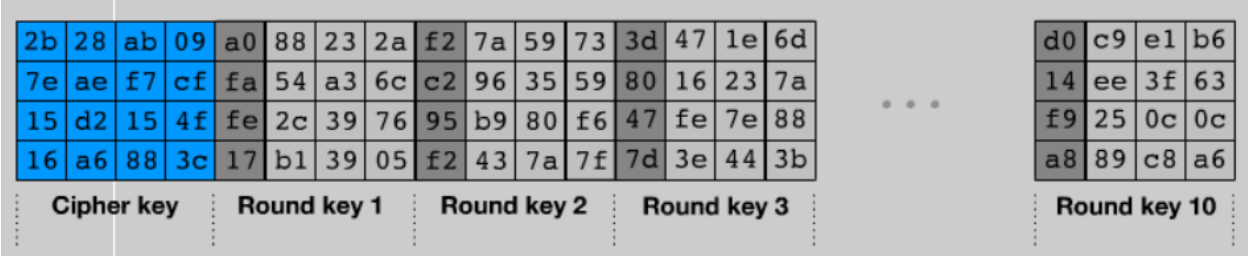
Pastaj rezultati i kolonës së fituar bëhet xor me kolonën e dytë të çelësit bazë

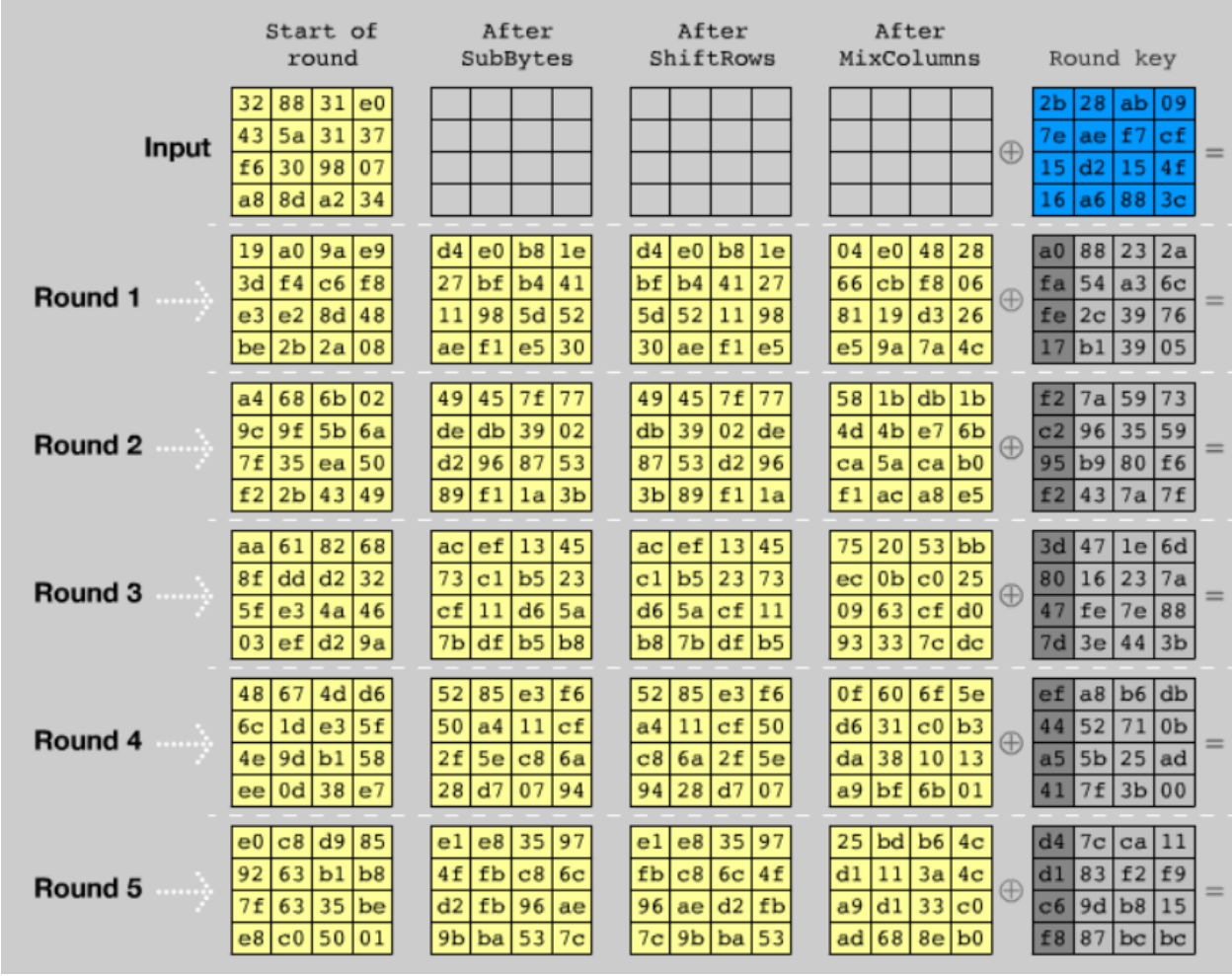


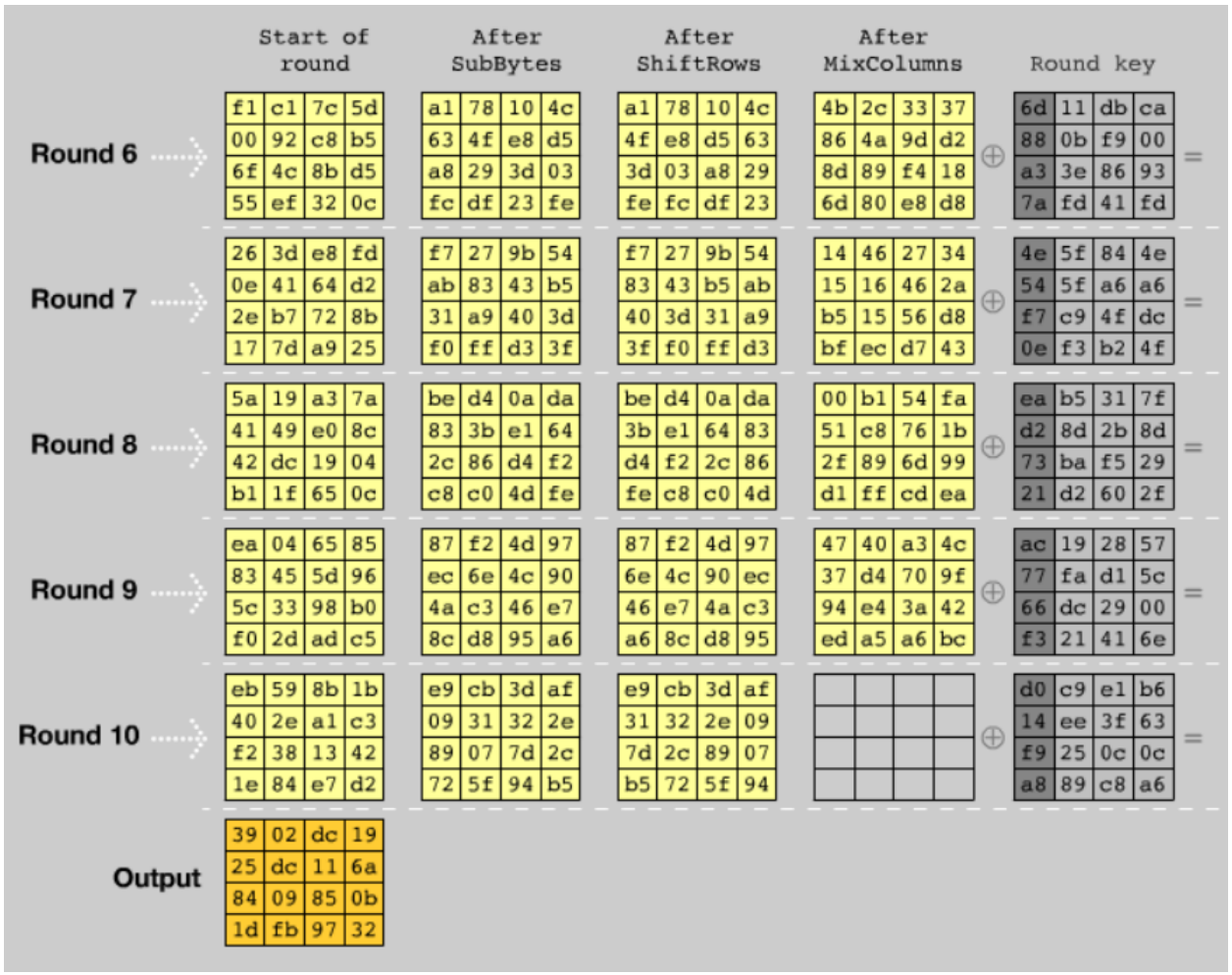




Njejt veprohet për ti fituar edhe çelësat e roundeve të tjera






Start of round
After SubBytes
After ShiftRows
After MixColumns
Round key
Round 6
f1 c1 7c 5d
00 92 c8 b5
6f 4c 8b d5
55 ef 32 0c
a1 78 10 4c
63 4f e8 d5
a8 29 3d 03
fc df 23 fe
a1 78 10 4c
4f e8 d5 63
3d 03 a8 29
fe fc df 23
4b 2c 33 37
86 4a 9d d2
8d 89 f4 18
6d 80 e8 d8
6d 11 db ca
88 0b f9 00
a3 3e 86 93
7a fd 41 fd
Round 7
26 3d e8 fd
0e 41 64 d2
2e b7 72 8b
17 7d a9 25
f7 27 9b 54
ab 83 43 b5
31 a9 40 3d
f0 ff d3 3f
f7 27 9b 54
83 43 b5 ab
40 3d 31 a9
3f f0 ff d3
14 46 27 34
15 16 46 2a
b5 15 56 d8
bf ec d7 43
4e 5f 84 4e
54 5f a6 a6
f7 c9 4f dc
0e f3 b2 4f
Round 8
5a 19 a3 7a
41 49 e0 8c
42 dc 19 04
b1 1f 65 0c
be d4 0a da
83 3b e1 64
2c 86 d4 f2
c8 c0 4d fe
be d4 0a da
3b e1 64 83
d4 f2 2c 86
fe c8 c0 4d
00 b1 54 fa
51 c8 76 1b
2f 89 6d 99
d1 ff cd ea
ea b5 31 7f
d2 8d 2b 8d
73 ba f5 29
21 d2 60 2f
Round 9
ea 04 65 85
83 45 5d 96
5c 33 98 b0
f0 2d ad c5
87 f2 4d 97
ec 6e 4c 90
4a c3 46 e7
8c d8 95 a6
87 f2 4d 97
6e 4c 90 ec
46 e7 4a c3
a6 8c d8 95
47 40 a3 4c
37 d4 70 9f
94 e4 3a 42
ed a5 a6 bc
ac 19 28 57
77 fa d1 5c
66 dc 29 00
f3 21 41 6e
Round 10
eb 59 8b 1b
40 2e a1 c3
f2 38 13 42
1e 84 e7 d2
e9 cb 3d af
09 31 32 2e
89 07 7d 2c
72 5f 94 b5
e9 cb 3d af
31 32 2e 09
7d 2c 89 07
b5 72 5f 94
d0 c9 e1 b6
14 ee 3f 63
f9 25 0c 0c
a8 89 c8 a6
Output
39 02 dc 19
25 dc 11 6a
84 09 85 0b
1d fb 97 32