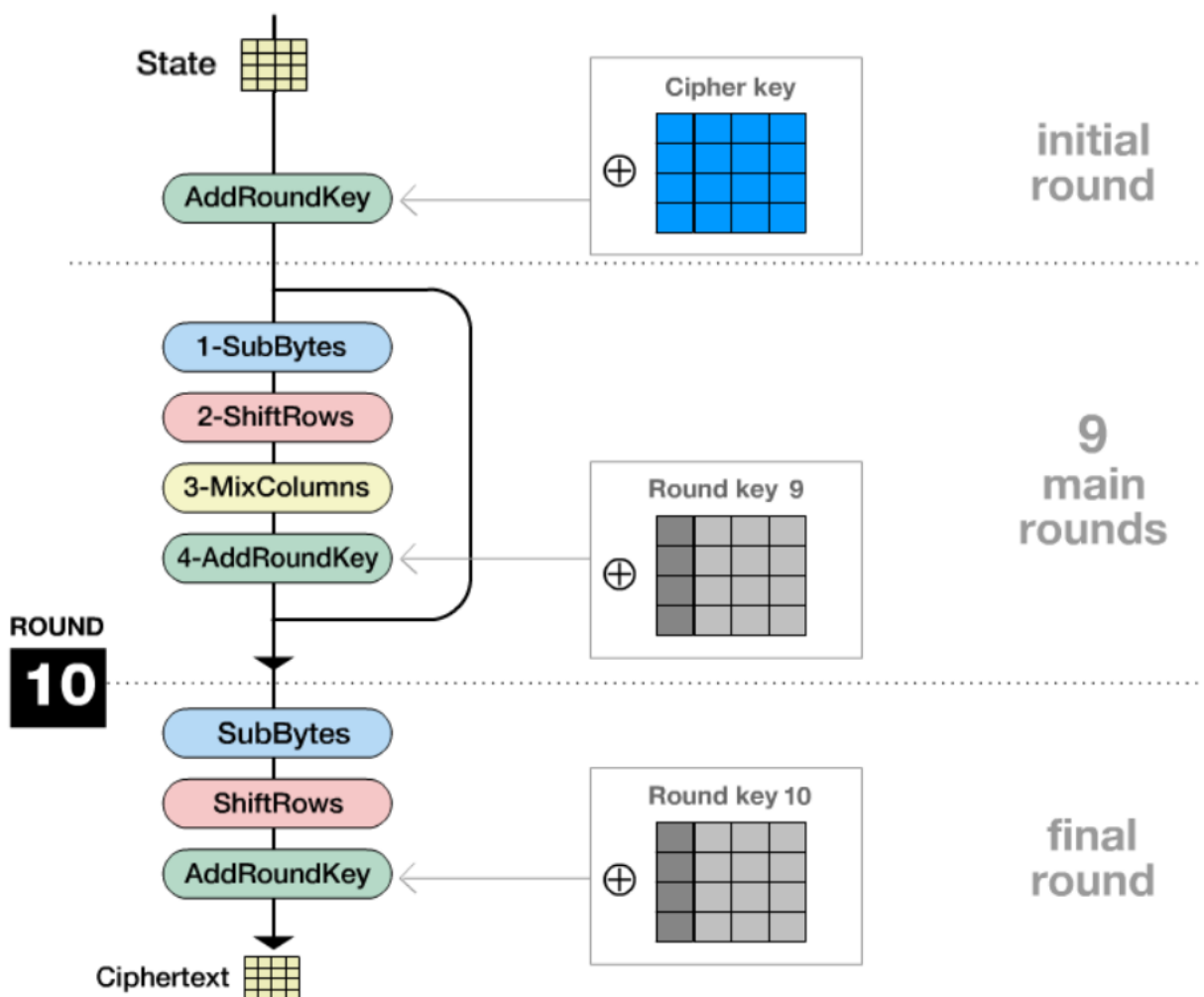


Algoritmi AES - Procesi i enkriptimit

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 standardin 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_2 . 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:

The 4 types of transformations:

1-SubBytes

2-ShiftRows

3-MixColumns

4-AddRoundKey

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 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.

19

	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

hex		y																				
		0	1	2	3	4	5	6	7								b	c	d	e	f	
x	0	63	7c	77	7b	f2	6b	6f	c5								2b	fe	d7	ab	76	
	1	ca	82	c9	7d	fa	59	47	f0	d4								af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc								f1	71	d8	31	15	
	3	04	c7	23	c3	18	96	05	9a								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					

S-BOX byte substitution table

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	e9	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

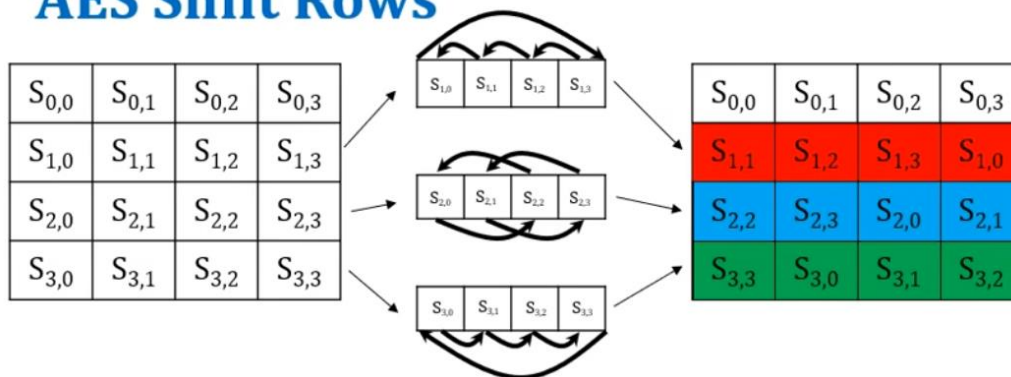
S-BOX byte substitution table

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.

AES Shift Rows



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.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

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

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

$$\begin{array}{r}
 X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^1 + 1 \\
 \begin{array}{cccccccc}
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
 \end{array} \\
 02 = 0000\ 0010 = X \\
 d4 = 1101\ 0100 = X^7 + X^6 + X^4 + X^2 \\
 \begin{array}{cccccccc}
 X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^1 + 1 \\
 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0
 \end{array}
 \end{array}$$

$$\begin{aligned}
 \{02\} * \{d4\} &= X * (X^7 + X^6 + X^4 + X^2) \\
 &= X^8 + X^7 + X^5 + X^3 \\
 &= X^4 + X + 1 + X^7 + X^5 + X^3 \\
 &= X^7 + X^5 + X^4 + X + 1 \\
 &= 10110011
 \end{aligned}$$

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

$$\begin{array}{r}
 X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^1 + 1 \\
 \begin{array}{cccccccc}
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
 \end{array} \\
 03 = 0000\ 0011 = X + 1 \\
 bf = 1011\ 1111 = X^7 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
 \begin{array}{cccccccc}
 X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^1 + 1 \\
 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1
 \end{array}
 \end{array}$$

$$\begin{aligned}
 \{03\} * \{d4\} &= (X + 1) * (X^7 + X^5 + X^4 + X^3 + X^2 + X + 1) \\
 &= X^8 + X^6 + X^5 + X^4 + X^3 + X^2 + X + X^7 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
 &= X^4 + X^3 + X + 1 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 + X^7 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
 &= X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
 &= 11011010
 \end{aligned}$$

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

$$\begin{array}{r}
 \{02\} * \{d4\} = 101110011 \\
 \{03\} * \{d4\} = 11011010 \\
 5d = 01011101 \\
 30 = 00110000 \\
 \hline
 00000100
 \end{array}
 \quad \otimes \text{ XOR}$$

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

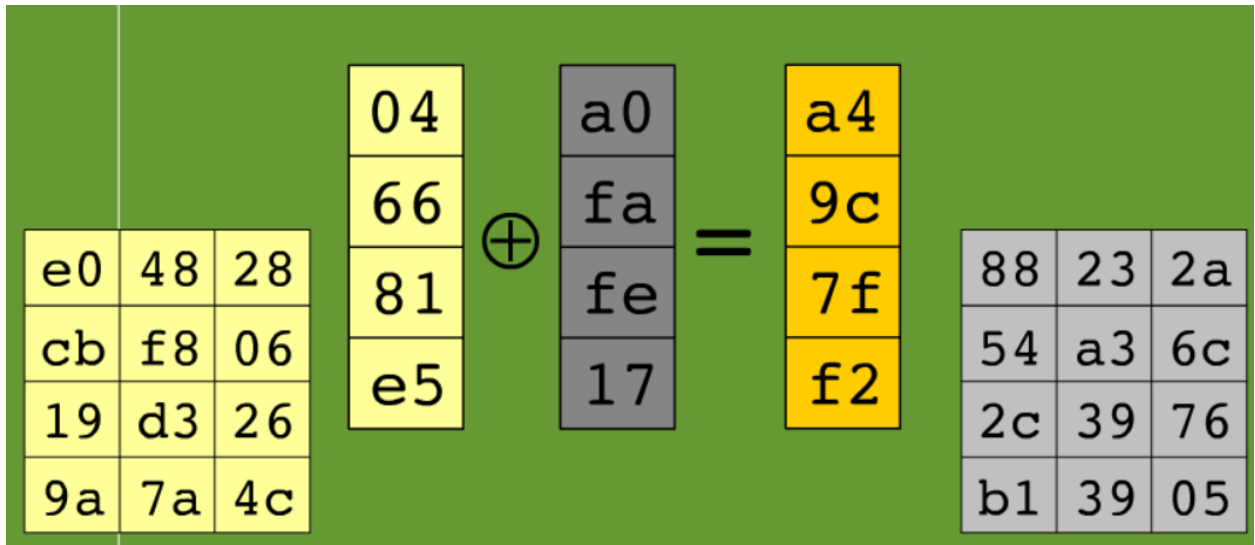
02	03	01	01	*	d4	e0	b8	1e	=	04	?	?	?	
01	02	03	01		bf	b4	41	27		?	?	?	?	?
01	01	02	03		5d	52	11	98		?	?	?	?	?
03	01	01	02		30	ae	f1	e5		?	?	?	?	?

dhe në fund fitohet kjo matricë

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

4. Add round Key

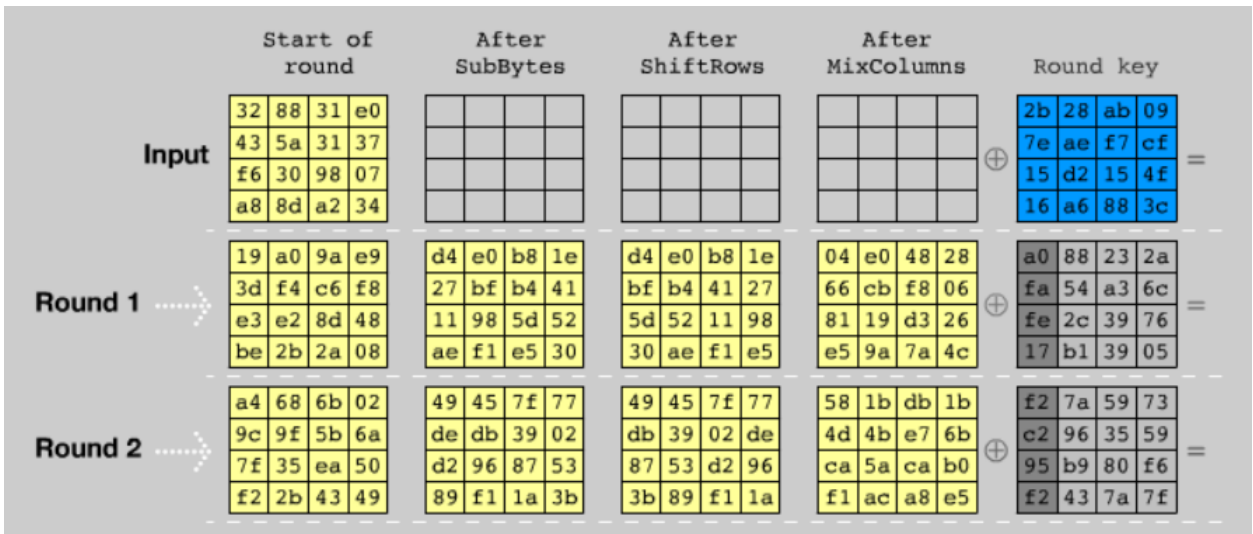
Tani rezultati i prodhimit të fazës së mëparshme është bërë XOR me çelësin e rrethit të përshtatshëm.



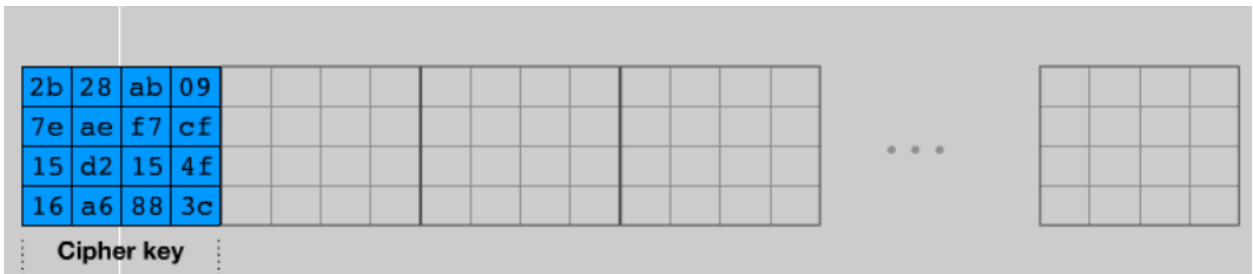
Njëjtë veprohet edhe me kolonat e tjera kolona e dytë e state bëhet xor me kolonën e dytë të çelësit round key etj, dhe në fund fitojmë:

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

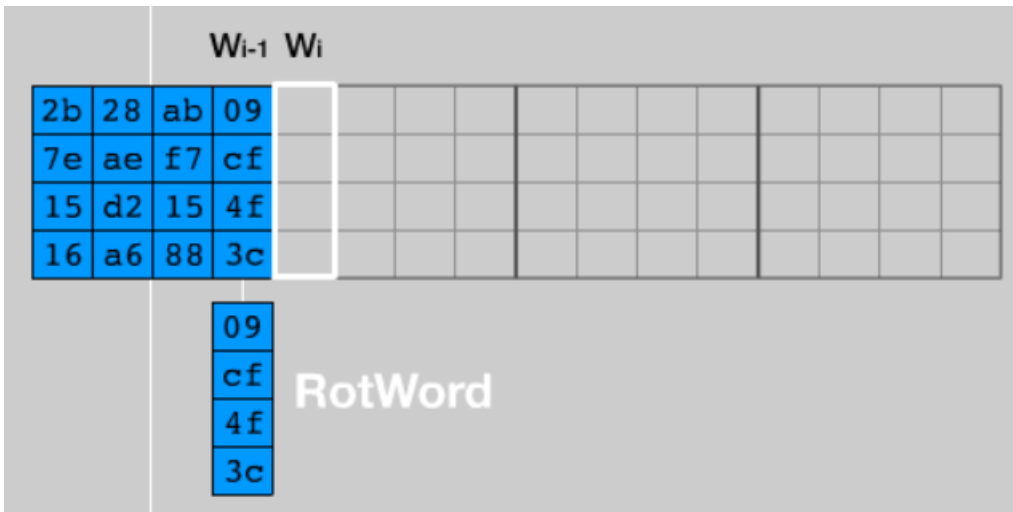
Këto transformime aplikohen në shtet edhe për 9 raunde të tjera. Raundi përfundimtar nuk përfshin transformimin MixColumns.



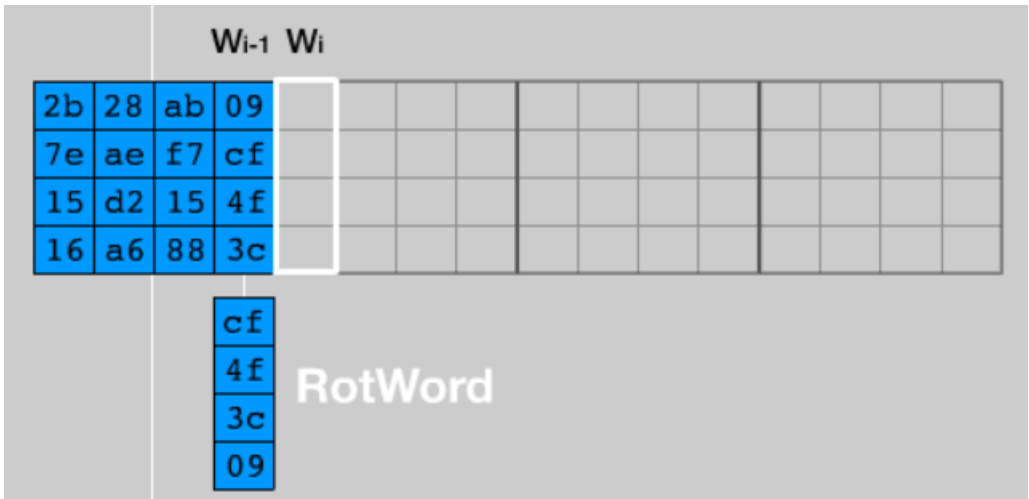
Çelësi i roundit të parë është fituar nga çelësi bazë i dhënë në fillim në këtë mënyrë:



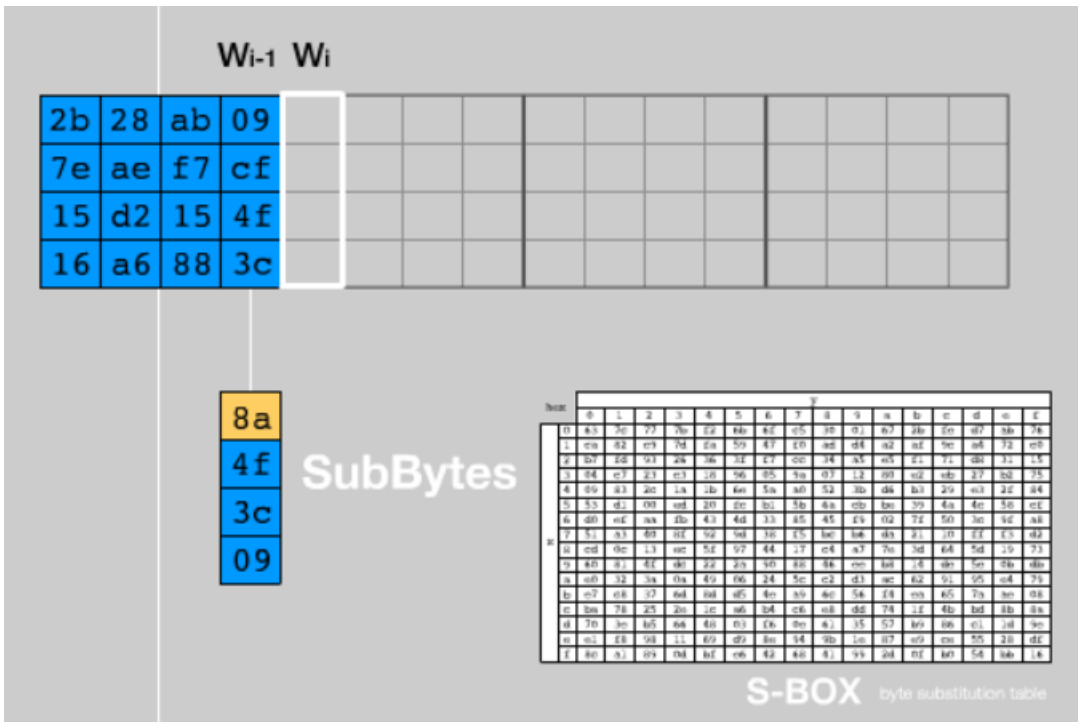
Nga çelësi bazë mirëto kolona e fundit dhe lëvizet për1 vertikalisht



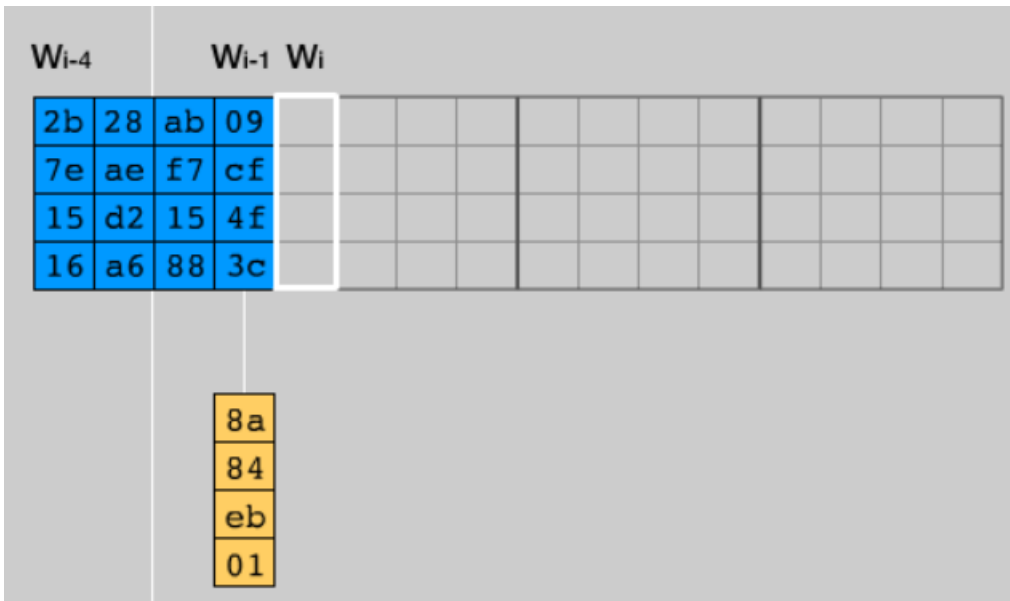
Dhe fitohet:



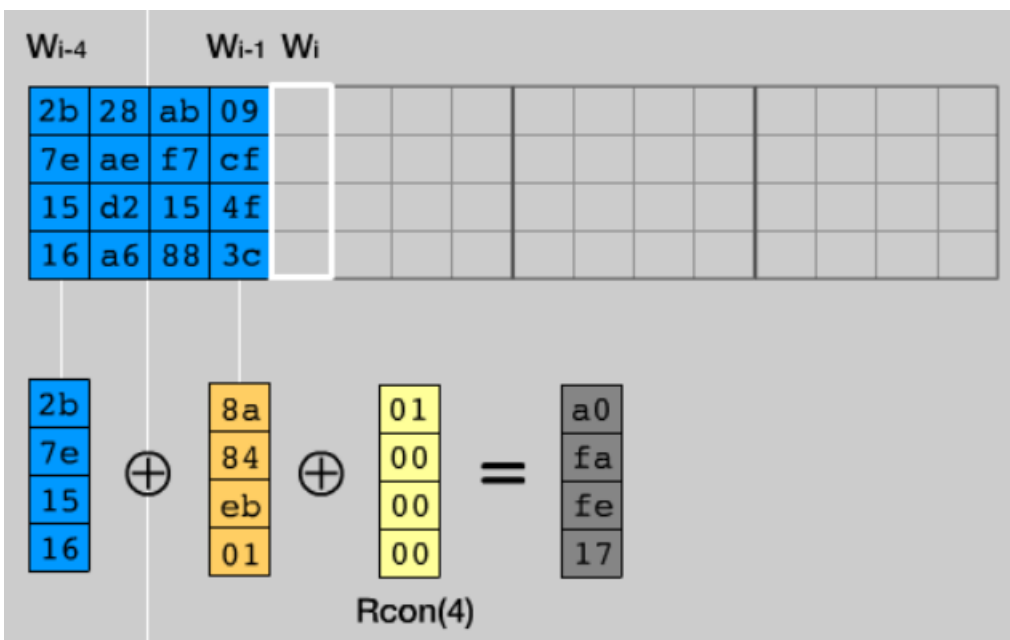
Pastaj numrat e kësaj kolone shikohen në tabelën S-BOX



Dhe fitohet:



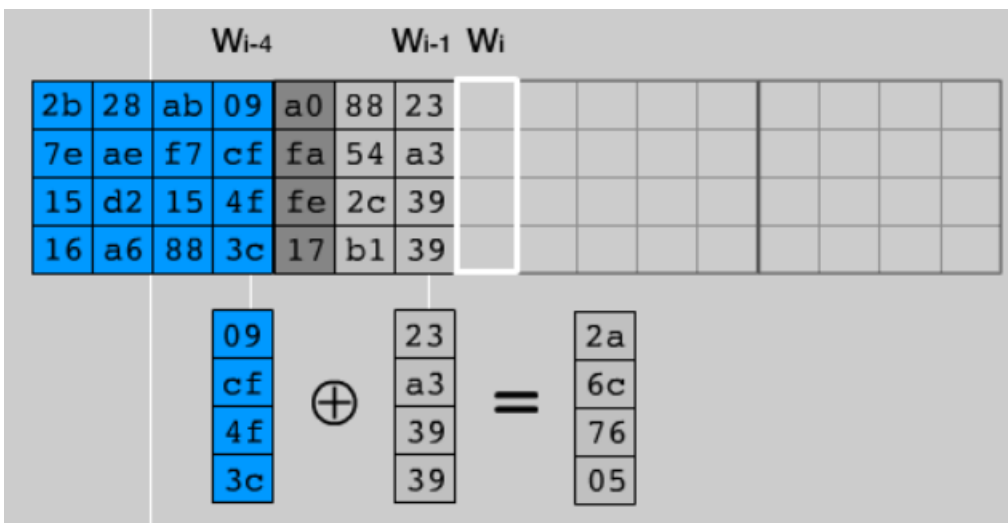
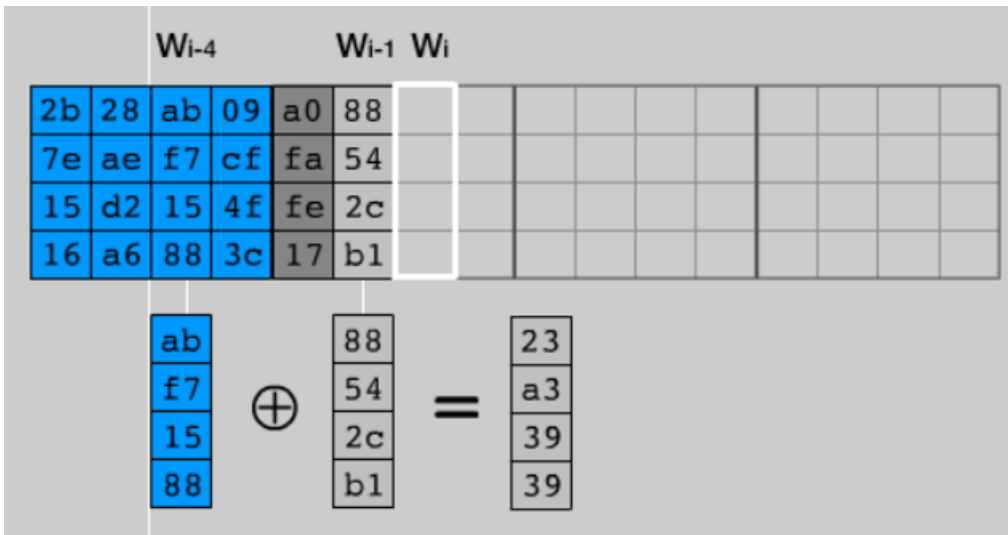
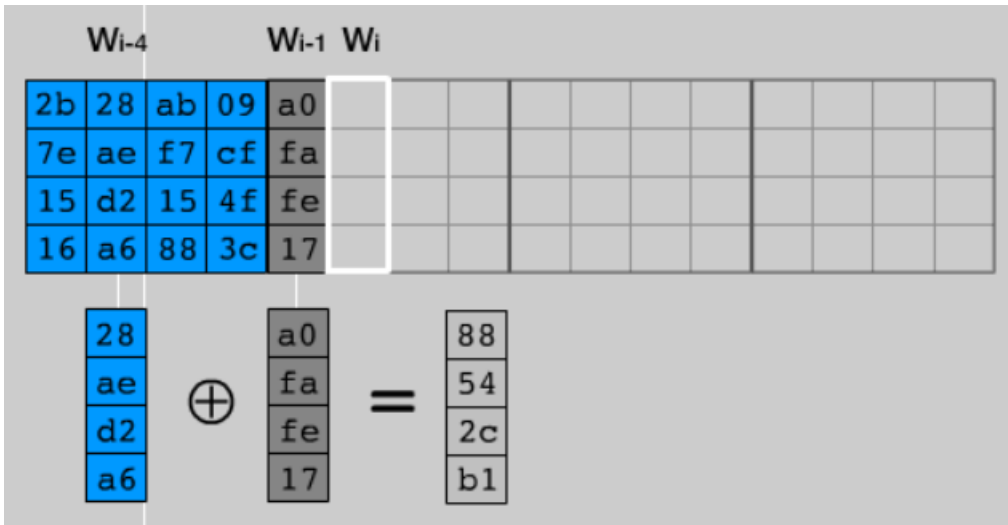
Pastaj kolona e parë bëhet xor me rezultatin e fituar më parë dhe round konstanten Rcon



01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Rcon

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



2b	28	ab	09	a0	88	23	2a										
7e	ae	f7	cf	fa	54	a3	6c										
15	d2	15	4f	fe	2c	39	76										
16	a6	88	3c	17	b1	39	05										
Cipher key				Round key 1													

Njejt veprohet për ti fituar edhe çelësat e roundeve të tjera

2b	28	ab	09	a0	88	23	2a	f2	7a	59	73	3d	47	1e	6d			d0	c9	e1	b6
7e	ae	f7	cf	fa	54	a3	6c	c2	96	35	59	80	16	23	7a			14	ee	3f	63
15	d2	15	4f	fe	2c	39	76	95	b9	80	f6	47	fe	7e	88			f9	25	0c	0c
16	a6	88	3c	17	b1	39	05	f2	43	7a	7f	7d	3e	44	3b			a8	89	c8	a6
Cipher key				Round key 1				Round key 2				Round key 3				Round key 10					

	Start of round	After SubBytes	After ShiftRows	After MixColumns	Round key																																																																																
Input	<table border="1"> <tr><td>32</td><td>88</td><td>31</td><td>e0</td></tr> <tr><td>43</td><td>5a</td><td>31</td><td>37</td></tr> <tr><td>f6</td><td>30</td><td>98</td><td>07</td></tr> <tr><td>a8</td><td>8d</td><td>a2</td><td>34</td></tr> </table>	32	88	31	e0	43	5a	31	37	f6	30	98	07	a8	8d	a2	34	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																	<table border="1"> <tr><td>2b</td><td>28</td><td>ab</td><td>09</td></tr> <tr><td>7e</td><td>ae</td><td>f7</td><td>cf</td></tr> <tr><td>15</td><td>d2</td><td>15</td><td>4f</td></tr> <tr><td>16</td><td>a6</td><td>88</td><td>3c</td></tr> </table>	2b	28	ab	09	7e	ae	f7	cf	15	d2	15	4f	16	a6	88	3c
32	88	31	e0																																																																																		
43	5a	31	37																																																																																		
f6	30	98	07																																																																																		
a8	8d	a2	34																																																																																		
2b	28	ab	09																																																																																		
7e	ae	f7	cf																																																																																		
15	d2	15	4f																																																																																		
16	a6	88	3c																																																																																		
Round 1	<table border="1"> <tr><td>19</td><td>a0</td><td>9a</td><td>e9</td></tr> <tr><td>3d</td><td>f4</td><td>c6</td><td>f8</td></tr> <tr><td>e3</td><td>e2</td><td>8d</td><td>48</td></tr> <tr><td>be</td><td>2b</td><td>2a</td><td>08</td></tr> </table>	19	a0	9a	e9	3d	f4	c6	f8	e3	e2	8d	48	be	2b	2a	08	<table border="1"> <tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr> <tr><td>27</td><td>bf</td><td>b4</td><td>41</td></tr> <tr><td>11</td><td>98</td><td>5d</td><td>52</td></tr> <tr><td>ae</td><td>f1</td><td>e5</td><td>30</td></tr> </table>	d4	e0	b8	1e	27	bf	b4	41	11	98	5d	52	ae	f1	e5	30	<table border="1"> <tr><td>d4</td><td>e0</td><td>b8</td><td>1e</td></tr> <tr><td>bf</td><td>b4</td><td>41</td><td>27</td></tr> <tr><td>5d</td><td>52</td><td>11</td><td>98</td></tr> <tr><td>30</td><td>ae</td><td>f1</td><td>e5</td></tr> </table>	d4	e0	b8	1e	bf	b4	41	27	5d	52	11	98	30	ae	f1	e5	<table border="1"> <tr><td>04</td><td>e0</td><td>48</td><td>28</td></tr> <tr><td>66</td><td>cb</td><td>f8</td><td>06</td></tr> <tr><td>81</td><td>19</td><td>d3</td><td>26</td></tr> <tr><td>e5</td><td>9a</td><td>7a</td><td>4c</td></tr> </table>	04	e0	48	28	66	cb	f8	06	81	19	d3	26	e5	9a	7a	4c	<table border="1"> <tr><td>a0</td><td>88</td><td>23</td><td>2a</td></tr> <tr><td>fa</td><td>54</td><td>a3</td><td>6c</td></tr> <tr><td>fe</td><td>2c</td><td>39</td><td>76</td></tr> <tr><td>17</td><td>b1</td><td>39</td><td>05</td></tr> </table>	a0	88	23	2a	fa	54	a3	6c	fe	2c	39	76	17	b1	39	05
19	a0	9a	e9																																																																																		
3d	f4	c6	f8																																																																																		
e3	e2	8d	48																																																																																		
be	2b	2a	08																																																																																		
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																																																																																		
04	e0	48	28																																																																																		
66	cb	f8	06																																																																																		
81	19	d3	26																																																																																		
e5	9a	7a	4c																																																																																		
a0	88	23	2a																																																																																		
fa	54	a3	6c																																																																																		
fe	2c	39	76																																																																																		
17	b1	39	05																																																																																		
Round 2	<table border="1"> <tr><td>a4</td><td>68</td><td>6b</td><td>02</td></tr> <tr><td>9c</td><td>9f</td><td>5b</td><td>6a</td></tr> <tr><td>7f</td><td>35</td><td>ea</td><td>50</td></tr> <tr><td>f2</td><td>2b</td><td>43</td><td>49</td></tr> </table>	a4	68	6b	02	9c	9f	5b	6a	7f	35	ea	50	f2	2b	43	49	<table border="1"> <tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr> <tr><td>de</td><td>db</td><td>39</td><td>02</td></tr> <tr><td>d2</td><td>96</td><td>87</td><td>53</td></tr> <tr><td>89</td><td>f1</td><td>1a</td><td>3b</td></tr> </table>	49	45	7f	77	de	db	39	02	d2	96	87	53	89	f1	1a	3b	<table border="1"> <tr><td>49</td><td>45</td><td>7f</td><td>77</td></tr> <tr><td>db</td><td>39</td><td>02</td><td>de</td></tr> <tr><td>87</td><td>53</td><td>d2</td><td>96</td></tr> <tr><td>3b</td><td>89</td><td>f1</td><td>1a</td></tr> </table>	49	45	7f	77	db	39	02	de	87	53	d2	96	3b	89	f1	1a	<table border="1"> <tr><td>58</td><td>1b</td><td>db</td><td>1b</td></tr> <tr><td>4d</td><td>4b</td><td>e7</td><td>6b</td></tr> <tr><td>ca</td><td>5a</td><td>ca</td><td>b0</td></tr> <tr><td>f1</td><td>ac</td><td>a8</td><td>e5</td></tr> </table>	58	1b	db	1b	4d	4b	e7	6b	ca	5a	ca	b0	f1	ac	a8	e5	<table border="1"> <tr><td>f2</td><td>7a</td><td>59</td><td>73</td></tr> <tr><td>c2</td><td>96</td><td>35</td><td>59</td></tr> <tr><td>95</td><td>b9</td><td>80</td><td>f6</td></tr> <tr><td>f2</td><td>43</td><td>7a</td><td>7f</td></tr> </table>	f2	7a	59	73	c2	96	35	59	95	b9	80	f6	f2	43	7a	7f
a4	68	6b	02																																																																																		
9c	9f	5b	6a																																																																																		
7f	35	ea	50																																																																																		
f2	2b	43	49																																																																																		
49	45	7f	77																																																																																		
de	db	39	02																																																																																		
d2	96	87	53																																																																																		
89	f1	1a	3b																																																																																		
49	45	7f	77																																																																																		
db	39	02	de																																																																																		
87	53	d2	96																																																																																		
3b	89	f1	1a																																																																																		
58	1b	db	1b																																																																																		
4d	4b	e7	6b																																																																																		
ca	5a	ca	b0																																																																																		
f1	ac	a8	e5																																																																																		
f2	7a	59	73																																																																																		
c2	96	35	59																																																																																		
95	b9	80	f6																																																																																		
f2	43	7a	7f																																																																																		
Round 3	<table border="1"> <tr><td>aa</td><td>61</td><td>82</td><td>68</td></tr> <tr><td>8f</td><td>dd</td><td>d2</td><td>32</td></tr> <tr><td>5f</td><td>e3</td><td>4a</td><td>46</td></tr> <tr><td>03</td><td>ef</td><td>d2</td><td>9a</td></tr> </table>	aa	61	82	68	8f	dd	d2	32	5f	e3	4a	46	03	ef	d2	9a	<table border="1"> <tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr> <tr><td>73</td><td>c1</td><td>b5</td><td>23</td></tr> <tr><td>cf</td><td>11</td><td>d6</td><td>5a</td></tr> <tr><td>7b</td><td>df</td><td>b5</td><td>b8</td></tr> </table>	ac	ef	13	45	73	c1	b5	23	cf	11	d6	5a	7b	df	b5	b8	<table border="1"> <tr><td>ac</td><td>ef</td><td>13</td><td>45</td></tr> <tr><td>c1</td><td>b5</td><td>23</td><td>73</td></tr> <tr><td>d6</td><td>5a</td><td>cf</td><td>11</td></tr> <tr><td>b8</td><td>7b</td><td>df</td><td>b5</td></tr> </table>	ac	ef	13	45	c1	b5	23	73	d6	5a	cf	11	b8	7b	df	b5	<table border="1"> <tr><td>75</td><td>20</td><td>53</td><td>bb</td></tr> <tr><td>ec</td><td>0b</td><td>c0</td><td>25</td></tr> <tr><td>09</td><td>63</td><td>cf</td><td>d0</td></tr> <tr><td>93</td><td>33</td><td>7c</td><td>dc</td></tr> </table>	75	20	53	bb	ec	0b	c0	25	09	63	cf	d0	93	33	7c	dc	<table border="1"> <tr><td>3d</td><td>47</td><td>1e</td><td>6d</td></tr> <tr><td>80</td><td>16</td><td>23</td><td>7a</td></tr> <tr><td>47</td><td>fe</td><td>7e</td><td>88</td></tr> <tr><td>7d</td><td>3e</td><td>44</td><td>3b</td></tr> </table>	3d	47	1e	6d	80	16	23	7a	47	fe	7e	88	7d	3e	44	3b
aa	61	82	68																																																																																		
8f	dd	d2	32																																																																																		
5f	e3	4a	46																																																																																		
03	ef	d2	9a																																																																																		
ac	ef	13	45																																																																																		
73	c1	b5	23																																																																																		
cf	11	d6	5a																																																																																		
7b	df	b5	b8																																																																																		
ac	ef	13	45																																																																																		
c1	b5	23	73																																																																																		
d6	5a	cf	11																																																																																		
b8	7b	df	b5																																																																																		
75	20	53	bb																																																																																		
ec	0b	c0	25																																																																																		
09	63	cf	d0																																																																																		
93	33	7c	dc																																																																																		
3d	47	1e	6d																																																																																		
80	16	23	7a																																																																																		
47	fe	7e	88																																																																																		
7d	3e	44	3b																																																																																		
Round 4	<table border="1"> <tr><td>48</td><td>67</td><td>4d</td><td>d6</td></tr> <tr><td>6c</td><td>1d</td><td>e3</td><td>5f</td></tr> <tr><td>4e</td><td>9d</td><td>b1</td><td>58</td></tr> <tr><td>ee</td><td>0d</td><td>38</td><td>e7</td></tr> </table>	48	67	4d	d6	6c	1d	e3	5f	4e	9d	b1	58	ee	0d	38	e7	<table border="1"> <tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr> <tr><td>50</td><td>a4</td><td>11</td><td>cf</td></tr> <tr><td>2f</td><td>5e</td><td>c8</td><td>6a</td></tr> <tr><td>28</td><td>d7</td><td>07</td><td>94</td></tr> </table>	52	85	e3	f6	50	a4	11	cf	2f	5e	c8	6a	28	d7	07	94	<table border="1"> <tr><td>52</td><td>85</td><td>e3</td><td>f6</td></tr> <tr><td>a4</td><td>11</td><td>cf</td><td>50</td></tr> <tr><td>c8</td><td>6a</td><td>2f</td><td>5e</td></tr> <tr><td>94</td><td>28</td><td>d7</td><td>07</td></tr> </table>	52	85	e3	f6	a4	11	cf	50	c8	6a	2f	5e	94	28	d7	07	<table border="1"> <tr><td>0f</td><td>60</td><td>6f</td><td>5e</td></tr> <tr><td>d6</td><td>31</td><td>c0</td><td>b3</td></tr> <tr><td>da</td><td>38</td><td>10</td><td>13</td></tr> <tr><td>a9</td><td>bf</td><td>6b</td><td>01</td></tr> </table>	0f	60	6f	5e	d6	31	c0	b3	da	38	10	13	a9	bf	6b	01	<table border="1"> <tr><td>ef</td><td>a8</td><td>b6</td><td>db</td></tr> <tr><td>44</td><td>52</td><td>71</td><td>0b</td></tr> <tr><td>a5</td><td>5b</td><td>25</td><td>ad</td></tr> <tr><td>41</td><td>7f</td><td>3b</td><td>00</td></tr> </table>	ef	a8	b6	db	44	52	71	0b	a5	5b	25	ad	41	7f	3b	00
48	67	4d	d6																																																																																		
6c	1d	e3	5f																																																																																		
4e	9d	b1	58																																																																																		
ee	0d	38	e7																																																																																		
52	85	e3	f6																																																																																		
50	a4	11	cf																																																																																		
2f	5e	c8	6a																																																																																		
28	d7	07	94																																																																																		
52	85	e3	f6																																																																																		
a4	11	cf	50																																																																																		
c8	6a	2f	5e																																																																																		
94	28	d7	07																																																																																		
0f	60	6f	5e																																																																																		
d6	31	c0	b3																																																																																		
da	38	10	13																																																																																		
a9	bf	6b	01																																																																																		
ef	a8	b6	db																																																																																		
44	52	71	0b																																																																																		
a5	5b	25	ad																																																																																		
41	7f	3b	00																																																																																		
Round 5	<table border="1"> <tr><td>e0</td><td>c8</td><td>d9</td><td>85</td></tr> <tr><td>92</td><td>63</td><td>b1</td><td>b8</td></tr> <tr><td>7f</td><td>63</td><td>35</td><td>be</td></tr> <tr><td>e8</td><td>c0</td><td>50</td><td>01</td></tr> </table>	e0	c8	d9	85	92	63	b1	b8	7f	63	35	be	e8	c0	50	01	<table border="1"> <tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr> <tr><td>4f</td><td>fb</td><td>c8</td><td>6c</td></tr> <tr><td>d2</td><td>fb</td><td>96</td><td>ae</td></tr> <tr><td>9b</td><td>ba</td><td>53</td><td>7c</td></tr> </table>	e1	e8	35	97	4f	fb	c8	6c	d2	fb	96	ae	9b	ba	53	7c	<table border="1"> <tr><td>e1</td><td>e8</td><td>35</td><td>97</td></tr> <tr><td>fb</td><td>c8</td><td>6c</td><td>4f</td></tr> <tr><td>96</td><td>ae</td><td>d2</td><td>fb</td></tr> <tr><td>7c</td><td>9b</td><td>ba</td><td>53</td></tr> </table>	e1	e8	35	97	fb	c8	6c	4f	96	ae	d2	fb	7c	9b	ba	53	<table border="1"> <tr><td>25</td><td>bd</td><td>b6</td><td>4c</td></tr> <tr><td>d1</td><td>11</td><td>3a</td><td>4c</td></tr> <tr><td>a9</td><td>d1</td><td>33</td><td>c0</td></tr> <tr><td>ad</td><td>68</td><td>8e</td><td>b0</td></tr> </table>	25	bd	b6	4c	d1	11	3a	4c	a9	d1	33	c0	ad	68	8e	b0	<table border="1"> <tr><td>d4</td><td>7c</td><td>ca</td><td>11</td></tr> <tr><td>d1</td><td>83</td><td>f2</td><td>f9</td></tr> <tr><td>c6</td><td>9d</td><td>b8</td><td>15</td></tr> <tr><td>f8</td><td>87</td><td>bc</td><td>bc</td></tr> </table>	d4	7c	ca	11	d1	83	f2	f9	c6	9d	b8	15	f8	87	bc	bc
e0	c8	d9	85																																																																																		
92	63	b1	b8																																																																																		
7f	63	35	be																																																																																		
e8	c0	50	01																																																																																		
e1	e8	35	97																																																																																		
4f	fb	c8	6c																																																																																		
d2	fb	96	ae																																																																																		
9b	ba	53	7c																																																																																		
e1	e8	35	97																																																																																		
fb	c8	6c	4f																																																																																		
96	ae	d2	fb																																																																																		
7c	9b	ba	53																																																																																		
25	bd	b6	4c																																																																																		
d1	11	3a	4c																																																																																		
a9	d1	33	c0																																																																																		
ad	68	8e	b0																																																																																		
d4	7c	ca	11																																																																																		
d1	83	f2	f9																																																																																		
c6	9d	b8	15																																																																																		
f8	87	bc	bc																																																																																		

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