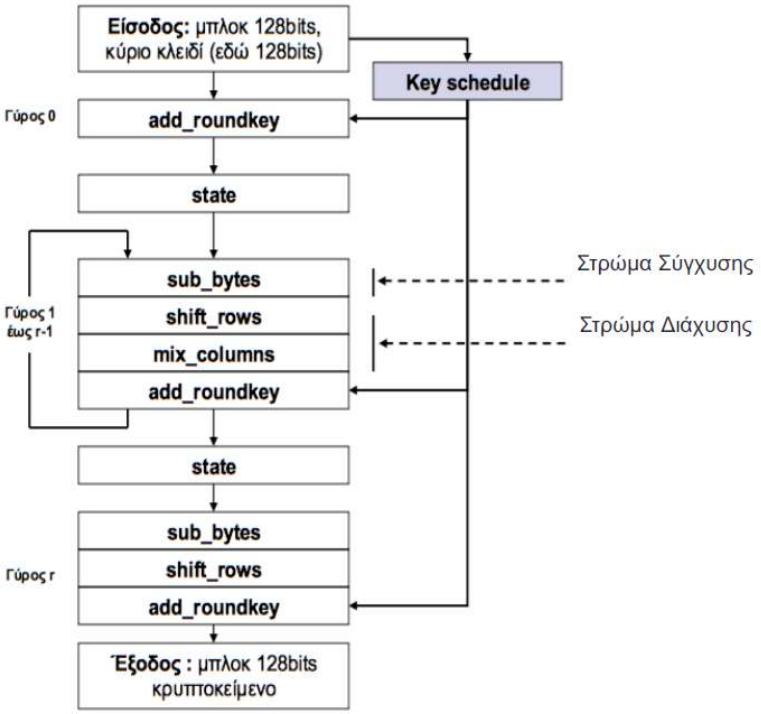
Advanced Encryption Standard (AES)

Ο AES δεν βασίζεται στα δίκτυα Feistel αλλά στην χρήση blocks, όπου κάθε block για οποιοδήποτε μέγεθος κλειδιού έχει σταθερό μέγεθος 128bit (16 bytes). Τα κλειδιά που μπορεί να χρησιμοποιήσει για να κρυπτογραφήσει-αποκρυπτογραφήσει είναι μεταβλητού μεγέθους. Το μέγεθος αυτό μπορεί να είναι 128 ή 192 ή 256 bits και από το μέγεθος του κλειδιού εξαρτάτε και πόσους γύρους (rounds) θα εκτελέσει ο αλγόριθμος. Συγκεκριμένα για τους γύρους έχουμε: $r_{128} = 10, r_{192} = 12$ και $r_{256} = 14$. Από το μέγεθος των κλειδιών βλέπουμε ότι είναι αδύνατον να "σπάσει" ο αλγόριθμος αφού για παράδειγμα για κλειδί 128bits έχουμε $3.4 * 10^{38}$ πιθανούς συνδυασμού που πρέπει να γίνουν για να βρεθεί το σωστό κλειδί, πράγμα που για τους σημερινούς υπολογιστές θα χρειαστεί αρκετά δισεκατομμύρια χρόνια. Όσο για την αποκρυπτογράφηση του μηνύματος, προκύπτει κάνοντας αναστροφή τον αλγόριθμο (φθίνουσα αρίθμηση των γύρων, ώστε να ισχύει η αντιστοιχία με τα κλειδιά του κάθε γύρου) και αντικατάσταση όλων των συναρτήσεων με τις αντίστροφές τους.

Ας μιλήσουμε τώρα για τα χαρακτηριστικά και τον τρόπο λειτουργία του. Υπάρχει ένας αποθηκευτικός χώρος state που αποθηκεύονται όλα τα ενδιάμεσα αποτελέσματα. Κάθε γύρος έχει τρία επίπεδα:

1. **Σύγχυσης**: πετυχαίνετε με την διαδικασία μετάθεσης (substitute) sub_bytes μέσω των S-Boxes
2. **Διάχυσης**: πετυχαίνετε με τις διαδικασίες ολίσθησης shift_rows και μίξης mix_columns
3. **Κρυπτογράφησης**: πετυχαίνετε με την διαδικασία add_roundkey που γίνεται XOR με το κλειδί του γύρου

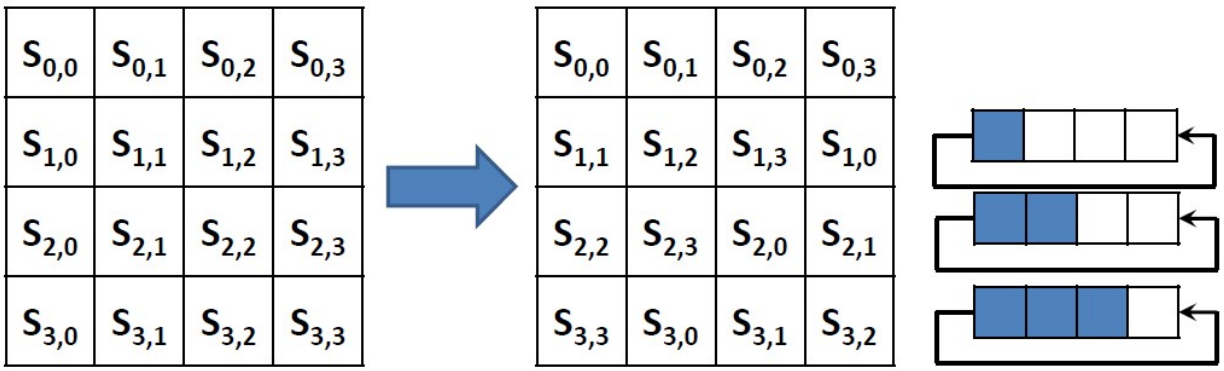


Συγκεκριμένα:

- **add_roundkey**: κάνει XOR (⊕) τον πίνακα state με το κλειδί που παράγεται από την διαδικασία key_schedule
- **sub_bytes**: κάθε byte του πίνακα state αντικαθίσταται από ένα άλλο byte μέσω ενός S-box (ο πρώτος αριθμός της εισόδου προσδιορίζει την γραμμή στον πίνακα του S-Box και ο δεύτερος την στήλη). Για κάθε byte έχουμε το ίδιο S-box. Ο πίνακας που δείχνει την αντικατάσταση των bytes μέσω του S-Box είναι:

	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

- **shift_rows**: γίνεται αριστερή ολίσθηση στις γραμμές του πίνακα state κατά 0, 1, 2 και 3 θέσεις αντίστοιχα.



- **mix_columns**: σε αυτήν την διαδικασία πολλαπλασιάζεται ο πίνακας state με έναν σταθερό πίνακα που προκύπτει από πράξεις μεταξύ πολυωνύμων ο οποίος είναι:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

- **key_schedule**: είναι η διαδικασία που παράγει το κλειδί του κάθε γύρου με βάση το αρχικό κλειδί. Αναλόγως με το μέγεθος του κλειδιού χωρίζουμε το κλειδί του κάθε γύρου σε λέξεις (words) (1 λέξη = 4 bytes).

  Για κλειδί:

  - 128bits χωρίζουμε σε 4 λέξεις
  - 192bits χωρίζουμε σε 6 λέξεις
  - και για 256bits χωρίζουμε σε 8 λέξεις

  Τώρα για τον υπολογισμό των λέξεων στον AES-128bits χρησιμοποιούμε τον αλγόριθμο:

```
(w0,...,w3) = key
for i = 4 to 43 {
    temp = wi-1
    if (i = 0 mod 4)
        then temp = sub_word(rot_word(temp)) ⊕ RCi/4
    wi = wi-4 ⊕ temp
}
```

Για τον AES-192bits και AES-256bits ο αλγόριθμος είναι πιο πολύπλοκος. Η συνάρτηση sub_word στον παραπάνω αλγόριθμο αντικαταστεί κάθε byte μέσω ενός S-Box και η συνάρτηση rot_word κάνει αριστερή ολίσθηση κατά 1 byte. Όσο για την μεταβλητή RC έχει προκαθορισμένες τιμές.

Παράδειγμα

Στο παράδειγμα θα χρησιμοποιηθεί ο AES-128bits άρα θα έχουμε 10 γύρους (rounds).

Έχουμε το κλειδί Thats my Kung Fu (16 ASCII χαρακτήρες από 1 byte (8 bit) ο καθένας), $16 * 8 = 128$ bit και το μήνυμα που θα κρυπτογραφηθεί είναι το Two One Nine Two.

Πριν αρχίσουμε τους γύρους κρυπτογράφησης, μετατρέπουμε το κλειδί και το μήνυμα σε δεκαεξαδική μορφή (hex).

Thats my Kung Fu = $(54\ 68\ 61\ 74\ 73\ 20\ 6D\ 79\ 20\ 4B\ 75\ 6E\ 67\ 20\ 46\ 75)_{16}$

Two One Nine Two = $(54\ 77\ 6F\ 20\ 4F\ 6E\ 65\ 20\ 4E\ 69\ 6E\ 65\ 20\ 54\ 77\ 6F)_{16}$

Τώρα θα βρούμε όλα τα round keys. Για 10 γύρους χρειαζόμαστε 11 υπό-κλειδιά των 128bits.

- Για κάθε κλειδί θα έχουμε 4 λέξεις
- Συνολικά πρέπει να παράγουμε 44 λέξεις ($44 * 32 = 1408$ bits) σε ένα πίνακα w_0,..., w_{43}
- Οι λέξεις w χρησιμοποιούνται ανά τέσσερις σε κάθε διαδικασία δημιουργίας round key.
- Αρχικά οι τέσσερις πρώτες λέξεις w_0 έως w_3 φορτώνονται με τα 128 bits του αρχικού κλειδιού στην δεκαεξαδική του μορφή.

$$w[0] = (54,68,61,74), w[1] = (73,20,6D, 79), w[2] = (20,4B, 75,6E), w[3] = (67,20,46,75)$$

Άρα το round key 0 είναι: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Στη συνέχεια ακολουθεί διαδικασία που επαναλαμβάνεται 40 φορές (4 λέξεις για τους υπόλοιπους 10 γύρους) για να βρούμε και τις λέξεις w_4 έως w_{43}. Για τον υπολογισμό τους χρησιμοποιούμε το αλγόριθμο:

```
for i = 4 to 43 {
    temp = w_{i-1}
    if (i = 0 mod 4)
        then temp = sub_word(rot_word(temp)) ⊕ RC_{i/4}
    w_i = w_{i-4} ⊕ temp
}
```

Για την μεταβλητή RC έχουμε:

RC_1 = 01000000

RC_2 = 02000000

RC_3 = 04000000

RC_4 = 08000000

RC_5 = 10000000

RC_6 = 20000000

RC_7 = 40000000

RC_8 = 80000000

RC_9 = 1B000000

RC_{10} = 36000000

Έτσι έχουμε $w[4] = w[0] \oplus g(w[3])$ όπου g είναι οι διαδικασίες ολίσθησης, μετάθεσης και πρόσθεσης του round constant (RC).

Έτσι $g(w[3])$ κάνει:

- Αριστερή ολίσθηση κατά 1: $(20,46,75,67)$
- Μετάθεση (S-Box): $(B7,5A,9D,85)$
- Πρόσθεση του RC_1 (01000000): $(B6,5A,9D,85)$

Άρα τελικά $g(w[3]) = (B6,5A,9D,85)$ και $w[4] = w[0] \oplus g(w[3]) = (E2,32,FC,F1)$

και

$w[5] = w[4] \oplus w[1] = (91,12,91,88)$

$w[6] = w[5] \oplus w[2] = (B1,59,E4,E6)$

$w[7] = w[6] \oplus w[3] = (D6,79,A2,93)$

Άρα το round key 1 είναι: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

Εφαρμόζοντας τον ίδιο αλγόριθμο και για τα υπόλοιπα προκύπτουν τα παρακάτω round keys:

Round key 0:	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Round key 1:	E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
Round key 2:	56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
Round key 3:	D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
Round key 4:	A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
Round key 5:	B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
Round key 6:	BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
Round key 7:	CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
Round key 8:	8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
Round key 9:	BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
Round key 10:	28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

Round 0

Κάνουμε XOR ($\oplus$) τον πίνακα state με το round key 0:

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \oplus \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix}$$

Και έχουμε το αποτέλεσμα όπου γίνεται και ο νέος state πίνακας:

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον γύρο μηδέν είναι:

00 1F 0E 54 3C 4E 08 59 6E 22 1B 0B 47 74 31 1A

Round 1

Τώρα κάνουμε μετάθεση (sub_bytes) κάθε byte του πίνακα state με το byte που ορίζει το S-Box και έχουμε τον νέο πίνακα state:

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

Στην συνέχεια κάνουμε αλλαγή (shift_rows) και των τεσσάρων γραμμών του πίνακα state και προκύπτει ο νέος πίνακας state:

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

Συνεχίζουμε κάνοντας XOR τον σταθερό πίνακα αυτής της διαδικασίας (mix_columns) με τον πίνακα state:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \oplus \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

Και σαν αποτέλεσμα έχουμε πάλι τον νέο πίνακα state:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

Τελευταίο βήμα του γύρου 1 είναι διαδικασία (add_roundkey) XOR του πίνακα state με το κλειδί του συγκεκριμένου γύρου:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \oplus \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

Με αποτέλεσμα τον νέο πίνακα state που θα χρησημοποιηθεί με ίδιο τρόπο και στους επόμενους γύρους:

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον πρώτο γύρο είναι:

58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE

Round 2

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} 6A & 59 & CB & BD \\ A0 & 4E & 48 & 12 \\ 30 & 9C & 98 & 9E \\ 3D & F4 & 9B & 8B \end{pmatrix} \qquad \begin{pmatrix} 6A & 59 & CB & BD \\ E4 & 48 & 12 & A0 \\ 98 & 9E & 30 & 9B \\ 8B & 3D & F4 & 9B \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} 15 & C9 & 7F & 9D \\ CE & 4D & 4B & C2 \\ 89 & 71 & BE & 88 \\ 65 & 47 & 97 & CD \end{pmatrix} \qquad \begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον δεύτερο γύρο είναι:

43 C9 A9 62 0E 57 C0 C8 09 08 EB FE 3D F8 7F 37

Round 3

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} 1A & AB & 01 & 27 \\ B4 & 5B & 30 & 41 \\ D3 & BA & E9 & D2 \\ AA & E8 & BB & 9A \end{pmatrix} \qquad \begin{pmatrix} 1A & AB & 01 & 27 \\ 5B & 30 & 41 & B4 \\ E9 & D2 & D3 & BA \\ A9 & AA & E8 & BB \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} AA & 65 & FA & 88 \\ 16 & 0C & 05 & 3A \\ 3D & C1 & DE & 2A \\ B3 & 4B & 5A & 0A \end{pmatrix} \qquad \begin{pmatrix} 78 & 70 & 99 & 4B \\ 76 & 76 & 3C & 39 \\ 30 & 7D & 37 & 43 \\ 54 & 23 & 5B & F1 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον τρίτο γύρο είναι:

78 76 30 54 70 76 7D 23 99 3C 37 5B 4B 39 43 F1

Round 4

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} BC & 51 & EE & B3 \\ 38 & 38 & EB & 12 \\ 04 & FF & 9A & 18 \\ 20 & 26 & 39 & A1 \end{pmatrix} \qquad \begin{pmatrix} BC & 51 & EE & B3 \\ 38 & EB & 12 & 38 \\ 9A & 18 & 04 & FF \\ A1 & 20 & 26 & 39 \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} 10 & BC & D3 & F3 \\ D8 & 94 & E0 & E0 \\ 53 & EA & 9E & 25 \\ 24 & 40 & 73 & 7B \end{pmatrix} \qquad \begin{pmatrix} B1 & 08 & 04 & E7 \\ CA & DC & B1 & B2 \\ 51 & 54 & C9 & 6C \\ ED & E1 & D3 & 20 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον τέταρτο γύρο είναι:

B1 CA 51 ED 08 DC 54 E1 04 B1 C9 D3 E7 B2 6C 20

Round 5

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} C8 & 30 & F2 & 94 \\ 74 & B0 & C8 & 37 \\ D1 & 20 & DD & 50 \\ 55 & F8 & 66 & B7 \end{pmatrix} \qquad \begin{pmatrix} C8 & 30 & F2 & 94 \\ B0 & C8 & 37 & 74 \\ DD & 50 & D1 & 20 \\ B7 & 55 & F8 & 66 \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} 2A & 26 & 8F & E9 \\ 78 & 1E & 0C & 7A \\ 1B & A7 & 6F & 0A \\ 5B & 62 & 00 & 3F \end{pmatrix} \qquad \begin{pmatrix} 9B & 23 & 5D & 2F \\ 51 & 5F & 1C & 38 \\ 20 & 22 & BD & 91 \\ 68 & F0 & 32 & 56 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον πέμπτο γύρο είναι:

9B 51 20 68 23 5F 22 F0 5D 1C BD 32 2F 38 91 56

Round 6

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} 14 & 26 & 4C & 15 \\ D1 & CF & 9C & 07 \\ B7 & 93 & 7A & 81 \\ 45 & 8C & 23 & B1 \end{pmatrix} \qquad \begin{pmatrix} 14 & 26 & 4C & 15 \\ CF & 9C & 07 & D1 \\ 7A & 81 & B7 & 93 \\ B1 & 45 & 8C & 23 \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} A9 & 37 & AA & F2 \\ AE & D8 & 0C & 21 \\ E7 & 6C & B1 & 9C \\ F0 & FD & 67 & 3B \end{pmatrix} \qquad \begin{pmatrix} 14 & 8F & C0 & 5E \\ 93 & A4 & 60 & 0F \\ 25 & 2B & 24 & 92 \\ 77 & E8 & 40 & 75 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον έκτο γύρο είναι:

14 93 25 77 8F A4 2B E8 C0 60 24 40 5E 0F 92 75

Round 7

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} FA & 73 & BA & 58 \\ DC & 49 & D0 & 76 \\ 3F & F1 & 36 & 4F \\ F5 & 9B & 09 & 9D \end{pmatrix} \qquad \begin{pmatrix} FA & 73 & BA & 58 \\ 49 & D0 & 76 & DC \\ 36 & 4F & 3F & F1 \\ 9D & F5 & 9B & 09 \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} 9F & 37 & 51 & 37 \\ AF & EC & 8C & FA \\ 63 & 39 & 04 & 66 \\ 4B & DB & B1 & D7 \end{pmatrix} \qquad \begin{pmatrix} 53 & 43 & 4F & 85 \\ 39 & 06 & 0A & 52 \\ 8E & 93 & 3B & 57 \\ 5D & F8 & 95 & BD \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον έβδομο γύρο είναι:

53 39 8E 5D 43 06 93 F8 4F 0A 3B 95 85 52 57 BD

Round 8

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} ED & 1A & 84 & 97 \\ 12 & 6F & 67 & 00 \\ 19 & DC & E2 & 5B \\ 4C & 41 & 2A & 7A \end{pmatrix} \qquad \begin{pmatrix} ED & 1A & 84 & 97 \\ 6F & 67 & 00 & 12 \\ E2 & 5B & 19 & DC \\ 7A & 4C & 41 & 2A \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} E8 & 8A & 4B & F5 \\ 74 & 75 & EE & E6 \\ D3 & 1F & 75 & 58 \\ 55 & 8A & 0C & 38 \end{pmatrix} \qquad \begin{pmatrix} 66 & 70 & AF & A3 \\ 25 & CE & D3 & 73 \\ 3C & 5A & 0F & 13 \\ 74 & A8 & 0A & 54 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον όγδοο γύρο είναι:

66 25 3C 74 70 CE 5A A8 AF D3 0F 0A A3 73 13 54

Round 9

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 3F & 8B & 66 & 8F \\ EB & BE & 76 & 7D \\ 92 & C2 & 67 & 20 \end{pmatrix} \qquad \begin{pmatrix} 33 & 51 & 79 & 0A \\ 8B & 66 & 8F & 3F \\ 76 & 7D & EB & BE \\ 20 & 92 & C2 & 67 \end{pmatrix}$$

Μετά από mix_columns και add_roundkey:

$$\begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix} \qquad \begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & 30 \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον ένατο γύρο είναι:

09 66 8B 78 A2 D1 9A 65 F0 FC E6 C4 7B 3B 30 89

Round 10

Μετά από sub_bytes και shift_rows:

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & A7 \end{pmatrix} \qquad \begin{pmatrix} 01 & 3A & 8C & 21 \\ 3E & B0 & E2 & 33 \\ 8E & 04 & 3D & B8 \\ A7 & BC & 4D & 1C \end{pmatrix}$$

Μετά από add_roundkey (στον τελευταίο γύρο δεν κάνουμε mix_columns):

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

Άρα το αποτέλεσμα του AES στον δέκατο γύρο είναι:

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Οπότε το μήνυμα Two One Nine Two με κλειδί Thats my Kung Fu και αλγόριθμο AES-128bits κρυπτογραφείτε σε 29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A.