Actividad 12.-Una Ronda de AES
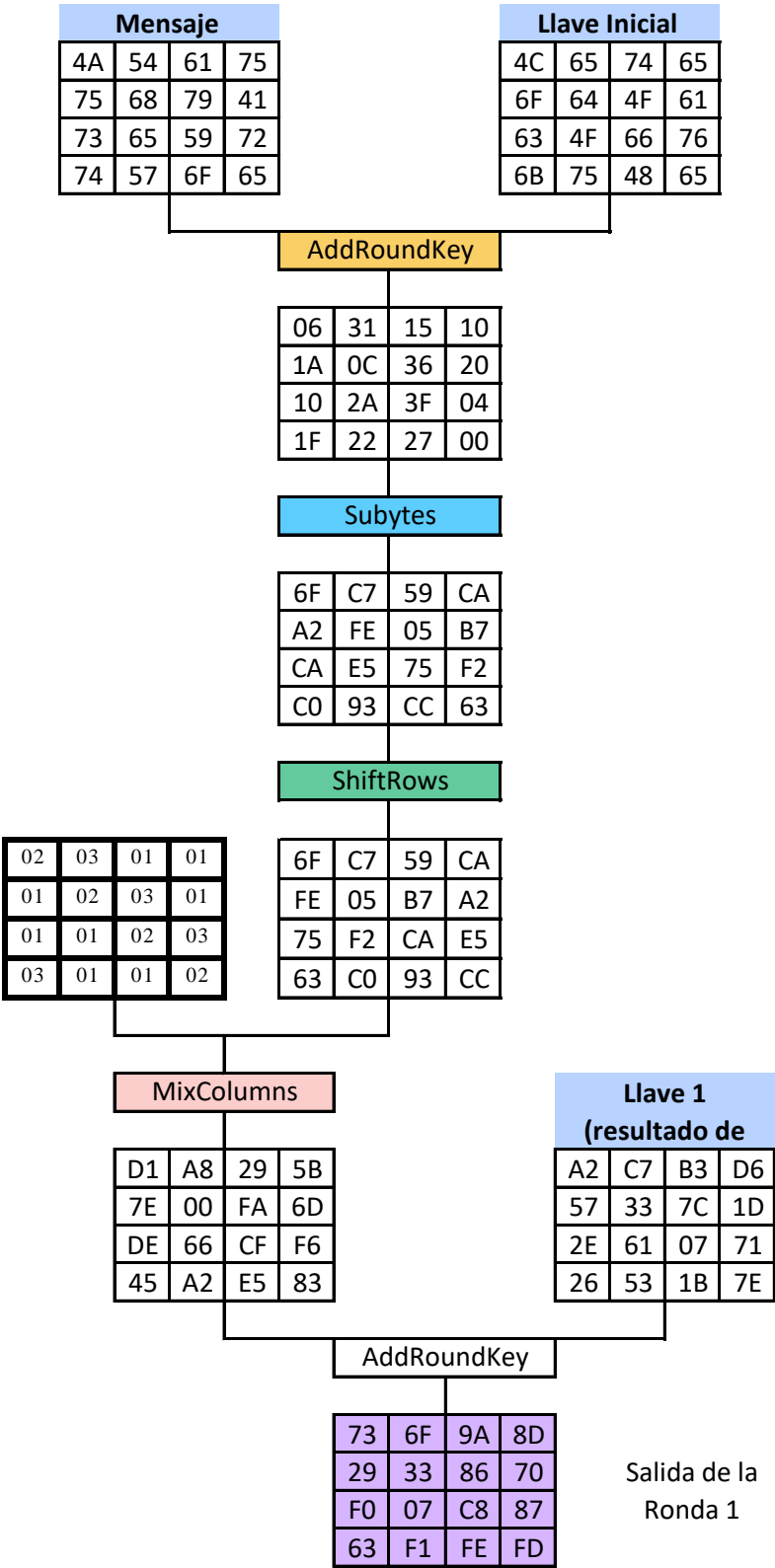
Nombres: Chacón Inostrosa Jaime Enrique, Ramírez Olvera Guillermo, Sánchez Méndez Edmundo Josué

Message:	**J**	**u**	**s**	**t**	**T**	**h**	**e**	**W**	**a**	**y**	**Y**	**o**	**u**	**A**	**r**	**e**
	4A	75	73	74	54	68	65	57	61	79	59	6F	75	41	72	65
Key:	**L**	**o**	**c**	**k**	**e**	**d**	**O**	**u**	**t**	**O**	**f**	**H**	**e**	**a**	**v**	**e**
	4C	6F	63	6B	65	64	4F	75	74	4F	66	48	65	61	76	65

Mensaje

4A	54	61	75
75	68	79	41
73	65	59	72
74	57	6F	65

Llave Inicial

4C	65	74	65
6F	64	4F	61
63	4F	66	76
6B	75	48	65

AddRoundKey

06	31	15	10
1A	0C	36	20
10	2A	3F	04
1F	22	27	00

Subytes

6F	C7	59	CA
A2	FE	05	B7
CA	E5	75	F2
C0	93	CC	63

ShiftRows

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

6F	C7	59	CA
FE	05	B7	A2
75	F2	CA	E5
63	C0	93	CC

MixColumns

D1	A8	29	5B
7E	00	FA	6D
DE	66	CF	F6
45	A2	E5	83

Llave 1 (resultado de

A2	C7	B3	D6
57	33	7C	1D
2E	61	07	71
26	53	1B	7E

AddRoundKey

73	6F	9A	8D
29	33	86	70
F0	07	C8	87
63	F1	FE	FD

Salida de la Ronda 1

Actividad #12.

The following are handwritten worksheets of hexadecimal XOR and GF multiplication calculations.

Panel 1 (Actividad #12):

```
9A ⊕ 4C = 06    Shit  6F        73 ⊕ 63 = 10    Shit  CA
59 ⊕ 65 = 31    C7              65 ⊕ 4F = 2A          E5
61 ⊕ 74 = 15    59              59 ⊕ 66 = 3F          75
75 ⊕ 65 = 10    CA              72 ⊕ 76 = 04          F2
75 ⊕ 6F = 3A    A2              2A ⊕ 6B = 1F          C0
68 ⊕ 64 = 0C    FE              51 ⊕ 75 = 22          93
29 ⊕ 1F = 36    05              6F ⊕ 48 = 27          CC
91 ⊕ 61 = 20    B7              65 ⊕ 65 = 00          63
```

Panel (right card 1):

```
01 xor A2 = 73
A8 xor C9 = 6F
29 xor B3 = 9A
5B xor 06 = 8D
9E xor 59 = 29
00 xor 33 = 33
FA xor 7C = 86
```

Panel (right card 2):

```
DE xor 2E = F0
66 xor 61 = 07
CE xor 07 = C8
F6 xor 71 = 87
45 xor 26 = 63
A2 xor 53 = F1
E5 xor 1B = FE
B3 xor 7E = FD
6D xor 1D = 70
```