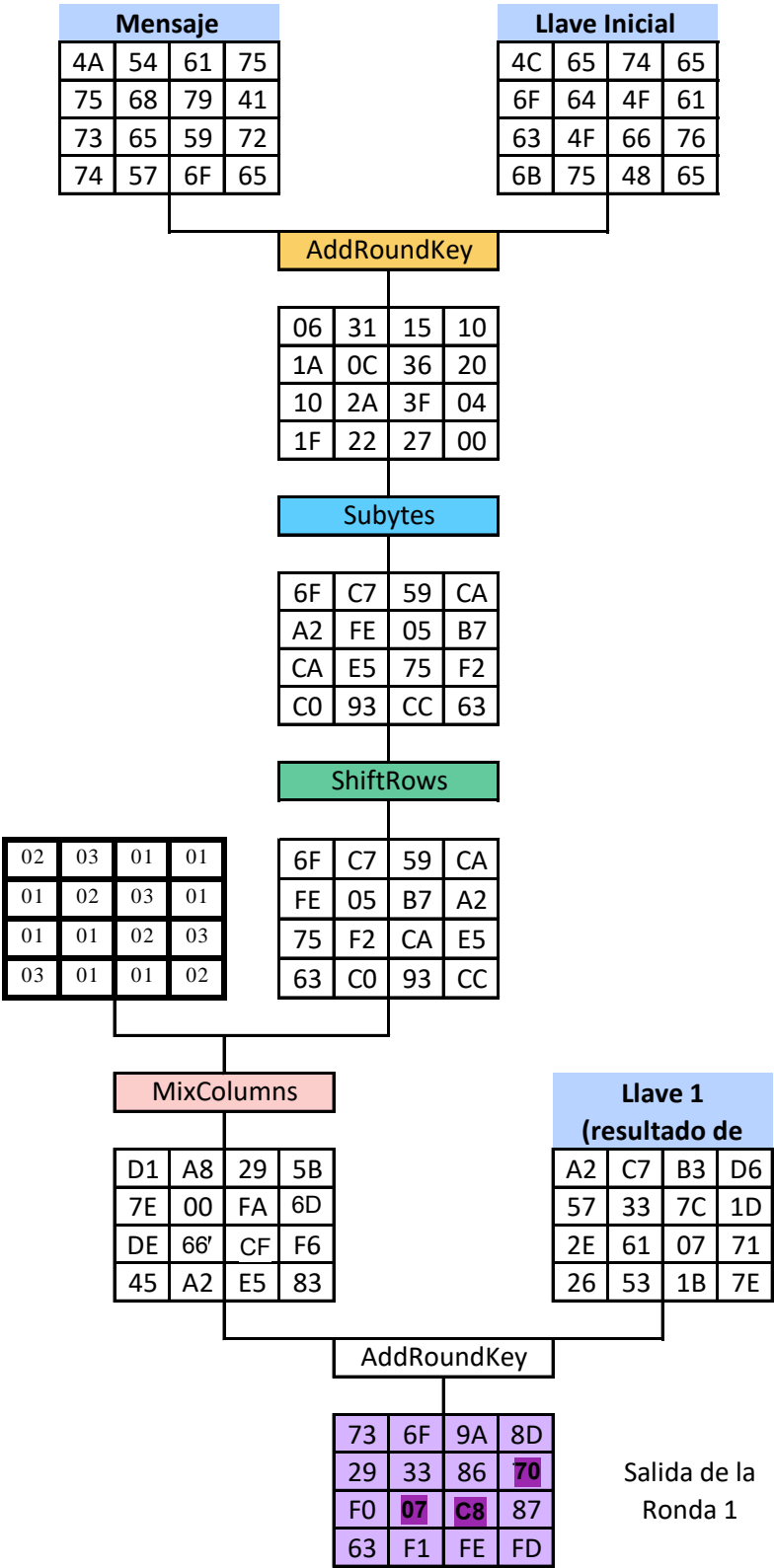


Actividad 12.-Una Ronda de AES

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



Actividad #12.

ShiftCA	ShiftCA
1A 0 9 1 = 06	73 0 63 = 10
5 9 0 65 = 31	65 5 4 F = 2A
6 1 0 7 1 = 15	59 5 6 8 = 3F
7 5 0 65 = 10	7 2 0 26 = 04
7 5 0 6 F = 3A	7 4 0 6 6 = 1F
6 8 0 6 9 = 0C	9 2 0 7 5 = 22
7 9 0 4 F = 36	6 F 5 18 = 27
7 1 0 6 1 = 20	6 5 0 6 7 = 00

c) $02 \oplus 6F \oplus 03 \oplus 5E \oplus 01 \oplus 75 \oplus 01 \oplus 63 =$

GF = 0110 1111

K2 = 0110 1111

D E

GF = 0111 1111

K2 = 1111 1110

GF = 0111 1111

K2 = 1000 0010

NOR 1000 1101

0000 11001

1 9

2F 19

75 25

NOR 63

1011

7

[illegible]

d) $02 \times 03A + 003 \times A2 + 01 \times FF + 01 \times CC =$

CA = 1 1 0 0	1 0 1 0	A2 = 1 0 1 0	0 0 1 0
X2 = 1 1 0 0	1 0 1 0 0	X2 = 1 0 1 0	0 0 1 0 0
XOR = 1 0 0 0	1 1 0 1 1	A2 = 0 1 0 1	0 0 0 1 0
0 1 0 0	0 1 1 1 1	1 1 1 1	0 0 1 1 0
8	F	X2 = 1 0 0 0	1 1 0 1 1
0F		0 1 1 1	1 1 0 1
FD		F	D
XOR	ES		
CO			
0B8			

e) $01 \times 6F + 02 \times FE + 03 \times 75 + 01 \times 63 =$

FE = 1 1 1 1	1 1 1 0	75 = 0 1 1 1	0 1 0 1
X2 = 1 1 1 1	1 1 1 0 0	X2 = 0 1 1 1	0 1 0 1 0
X2 = 1 0 0 0	1 1 0 1 1	75 = 0 0 1 1	1 0 1 0 1
0 1 1 1	0 1 1 1 1	0 1 0 0	1 1 1 1 1
E	7	9	F
65			
E3			
0F			
63			
XOR			
3E			

f) $01\ K C 7 + 03\ K 05 + 03\ K F 2 + 01\ K 50 =$

05 = 0 0 0 0	0 1 0 1	F2 = 1 1 1 1	0 0 1 0
x2 = 0 0 0 0	0 1 0 1 0	x2 = 1 1 1 1	0 0 1 0 0
	0	F2 = 0 1 1 1	1 0 0 1 0

C3	1 0 0 0	0 1 1 1 0
0 A	x0r 1 0 0 0	1 1 0 1 1
x0r 0 D		
CO	0 0 0 0	0 1 1 0 1
		0
		D

00 \times

g) $01\ K 09 + 02\ K B 7 + 03\ K C 4 + 01\ K 13 =$

B7 = 1 0 1 1	0 1 1 1	C4 = 1 1 0 0	1 0 1 0	59
x2 = 1 0 1 1	0 1 1 1 0	x2 = 1 1 0 0	1 0 1 0 0	35
x0r 1 0 0 0	1 1 0 1 1	C4 = 0 1 1 0	1 0 1 0 0	45
	0 0 1 1	1 0 1 1 0	1 1 1 1 0	73
	7	5		FA \times

	0 0 1 0	0 0 1 0 1
	4	5

h) $01\ K C 4 + 02\ K A 8 + 03\ K E 5 + 01\ K 1 C =$

AZ = 1 0 1 0	0 1 0 1	E5 = 1 1 1 0	0 1 0 1	CD
x2 = 1 0 1 0	0 0 1 0 0	x2 = 1 1 1 0	0 1 0 1 0	5F
x0r 1 0 0 0	1 1 1 0 1	E5 = 0 1 1 1	0 0 1 0 1	CC
	0 0 1 0	5	1 1 1 1	66
	5	5		\times

	0 0 0 1	1 0 1 0 0
	3	F

[illegible]

M: $3 \times 6F + 1 \times FE + 1 \times 95 + 2 \times 63$

(A)

A: $0 \times 6F = 01101111$

$0 \times 6F \times 2 = 11011110$

$0 \times 6F \times 3 = 10110001$

B 1

Ver

B
FE
95
26
FC

B: $0 \times 43 = 01100011$

$0 \times 63 \times 2 = 11000110$

C 6

N: $3 \times C9 + 1 \times 05 + 1 \times F2 + 2 \times C0$

(A)

A: $0 \times C9 = 11000111$

$0 \times C9 \times 2 = 11000110$

$0 \times C9 \times 3 = 10100100$

10001101

010101010

5 2

B: $0 \times C0 = 111000000$

$0 \times C0 \times 2 = 110000000$

100011011

010011011

9 8

Ver

S2
F2
98
3E

[illegible]

01 xor	A2 =	73
A8 xor	C4 =	6F
29 xor	83 =	9A
5B xor	06 =	8D
9E xor	54 =	29
00 xor	33 =	33
FA xor	7C =	86
66 xor	1D =	7B

$DE \text{ xor } 2E = FO$
 $67 \text{ xor } 61 = 06$
 $EC \text{ xor } 07 = EB$
 $FG \text{ xor } 71 = 87$
 $45 \text{ xor } 26 = 63$
 $A2 \text{ xor } 53 = F1$
 $E5 \text{ xor } 1B = FE$
 $83 \text{ xor } 7E = FD$