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

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

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

MixColumns

D1	A8	29	5B
74	00	FA	6D
DE	66	CF	F6
FC	3E	AB	81

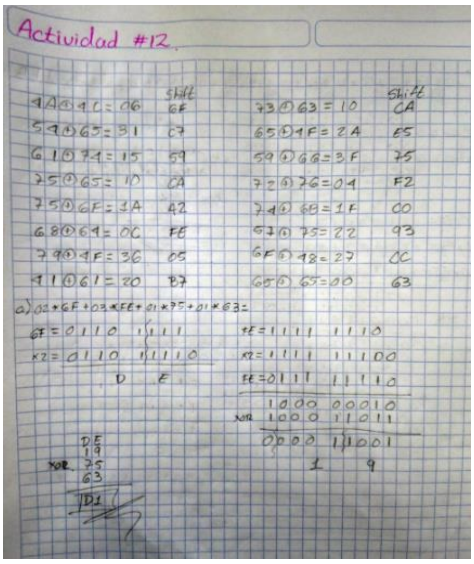
Llave 1 (resultado de

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

AddRoundKey

73	6F	9A	8D
23	33	86	70
F0	07	C8	87
DA	6D	B0	FF

Salida de la Ronda 1


Actividad #12