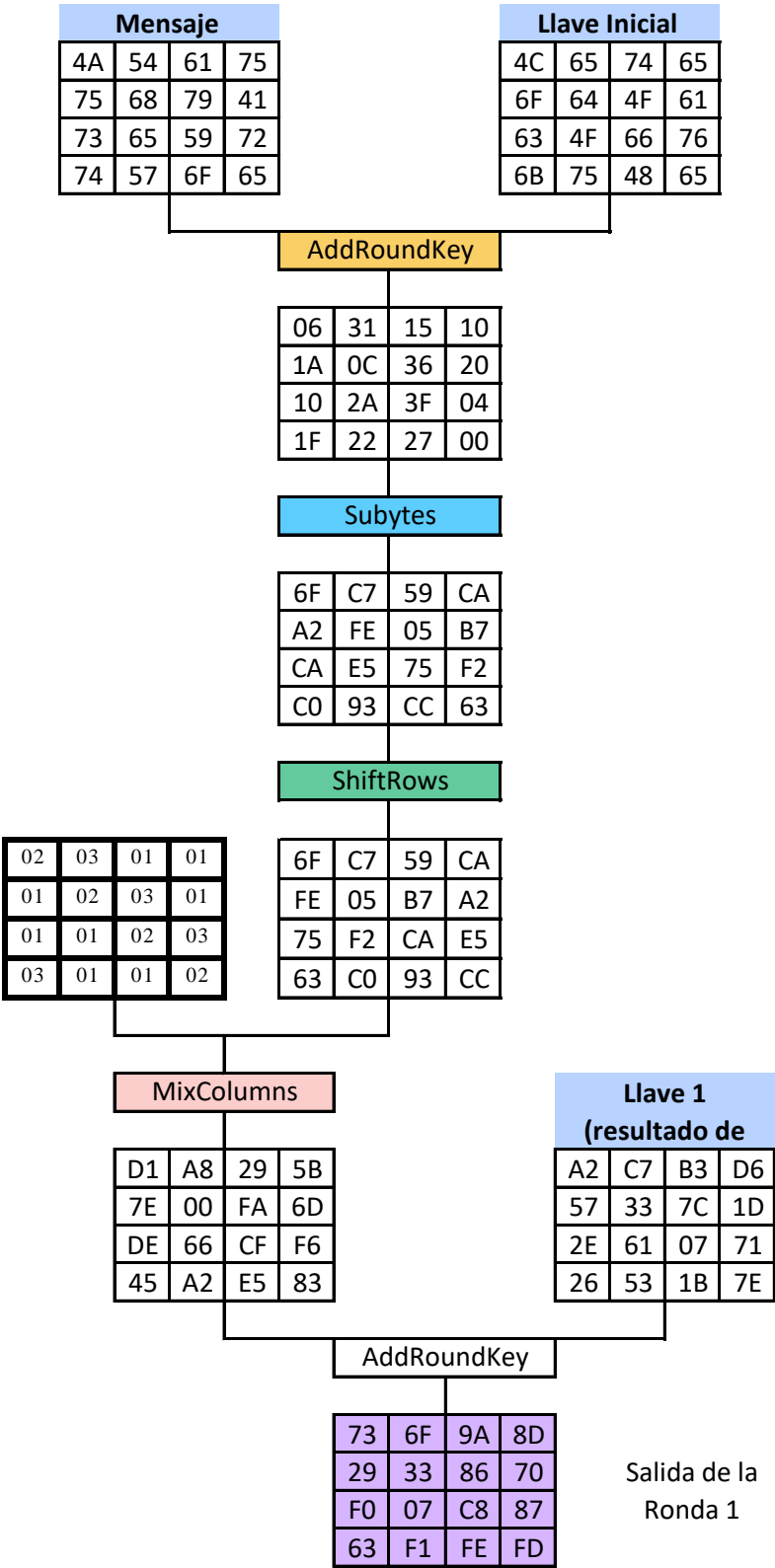


Actividad 12.-Una Ronda de AES

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.

4A 41 = 06	SHL	6F	30 63 = 10	SHL	CA
57 65 = 31	CF		65 61 F = 2A	ES	
61 64 = 15	57		59 66 = 3F	75	
25 65 = 10	CA		20 26 = 04	F2	
75 66 = 3A	A2		24 6B = 3F	00	
68 69 = 0C	FE		61 75 = 22	93	
29 4F = 3C	05		6F 54 = 27	0C	
11 61 = 20	B7		65 65 = 00	63	

$01 \times 6F + 03 \times EE + 01 \times 75 + 01 \times 63 =$
 $6F = 0110 \ 1111$
 $EE = 1111 \ 1110$
 $75 = 0110 \ 1110$
 $63 = 0111 \ 1110$
 $0110 \ 1111$
 $1000 \ 0010$
 $1000 \ 1101$
 $0000 \ 11001$
 $1 \ 9$

$2F$
 19
 33
 63
 101

$01 \times C7 + 02 \times K05 + 03 \times K52 + 01 \times K63 =$
 $05 = 0000 \ 0101$
 $K2 = 0000 \ 01010$
 $0 \ A$
 $C7 = 1000 \ 10110$
 $0A = 1000 \ 11011$
 00
 00

$01 \times 09 + 02 \times B7 + 03 \times CA + 01 \times B3 =$
 $B7 = 1011 \ 0111$
 $K2 = 1011 \ 01110$
 $0A = 1000 \ 11011$
 $0011 \ 10101$
 $2 \ 5$
 $1010 \ 11110$
 $1000 \ 11011$
 $0010 \ 01101$
 $4 \ 9$

$01 \times CA + 02 \times K63 + 03 \times K52 + 01 \times K63 =$
 $A2 = 1010 \ 0010$
 $K2 = 1010 \ 00100$
 $K0 = 1000 \ 11011$
 $0010 \ 11111$
 $5 \ F$
 $1001 \ 01111$
 $K0 = 1000 \ 11011$
 $0001 \ 10100$
 $3 \ F$

$01 \times 59 + 01 \times B7 + 01 \times CA + 02 \times 93$
 $A: 0x59 = 01011001$
 $0x93 = 010110010$
 $0x59 \times 3 = 01101011$
 $E \ B$
 EB
 CA
 $3D$
 AB

$P: 3 \times CA + 1 \times A2 + 1 \times E5 + 2 \times CC$
 $A: 0xCA = 11001010$
 $0xCA2 = 110010100$
 $0xCA3 = 101011110$
 100011011
 001000101
 $4 \ 5$
 45
 $A2$
 $E5$
 83
 $E1$

$002 \times C7 + 03 \times K05 + 01 \times K52 + 01 \times K63 =$
 $C7 = 1100 \ 0111$
 $K2 = 1100 \ 01110$
 $K0 = 1000 \ 11011$
 $0100 \ 10101$
 $9 \ 5$
 $0 \ F$

$002 \times 09 + 03 \times B7 + 01 \times CA + 01 \times B3 =$
 $09 = 0101 \ 1001$
 $K2 = 0101 \ 10010$
 $B \ 2$
 $B7 = 1011 \ 0111$
 $K2 = 1011 \ 01110$
 $B7 = 0101 \ 10111$
 $1110 \ 11001$
 $K0 = 1000 \ 11011$
 $0110 \ 01013$
 $C \ 2$
 $B2$
 $C7$
 CA
 93
 29

$01 \times 0F + 01 \times K52 + 02 \times K75 + 03 \times K63 =$
 $0F = 0111 \ 0101$
 $K2 = 0111 \ 01010$
 $E \ A$
 $03 = 0110 \ 0011$
 $K0 = 0011 \ 00111$
 $0101 \ 01101$
 $A \ 5$

$01 \times K7 + 01 \times K05 + 02 \times K52 + 03 \times K63 =$
 $K7 = 1111 \ 0010$
 $K2 = 1111 \ 00101$
 $K0 = 1000 \ 11011$
 $0111 \ 11110$
 $E \ E$
 $1010 \ 00000$
 $K0 = 1000 \ 11011$
 $0010 \ 11011$
 $7 \ 1D$

$01 \times B3 + 01 \times K63 + 02 \times K05 + 03 \times B3 =$
 $B3 = 0000 \ 0111$
 $K2 = 0000 \ 01110$
 $0 \ E$
 $0001 \ 01101$
 $2 \ D$
 $0010 \ 01101$
 $2 \ D$
 $0110 \ 01101$
 $E5 = 1110 \ 0101$
 $K2 = 1110 \ 01010$
 $K0 = 1000 \ 11011$
 $0110 \ 10001$
 $D \ 1$
 $1010 \ 10100$
 $K0 = 1000 \ 11011$
 $0010 \ 01111$
 $1 \ F$

$01 \times 0F \ A2 = 73$
 $A8 \times 0F \ C9 = 6F$
 $29 \times 0F \ B3 = 9A$
 $5B \times 0F \ D6 = 8D$
 $9E \times 0F \ 59 = 29$
 $00 \times 0F \ 33 = 33$
 $FA \times 0F \ 7C = 86$

$01 \times CA + 03 \times K63 + 01 \times K52 + 01 \times K63 =$
 $CA = 1100 \ 1010$
 $K2 = 1100 \ 10100$
 $K0 = 1000 \ 11011$
 $0100 \ 01111$
 $7 \ E$
 $0F$
 FD
 $K0 = 1000 \ 11011$
 $0111 \ 11101$
 $F \ D$

$01 \times 6F + 02 \times FE + 03 \times K75 + 01 \times K63 =$
 $FE = 1111 \ 1110$
 $K2 = 1111 \ 11100$
 $K0 = 1000 \ 11011$
 $0111 \ 01111$
 $E \ 7$
 65
 FE
 FE
 63
 $7E$

$M: 3 \times 1F + 1 \times FE + 1 \times 95 + 2 \times 63$
 $A: 0x1F = 01101111$
 $0x63 = 01101110$
 $0x1F \times 3 = 101100011$
 $B \ 1$
 FE
 95
 63
 FC
 $B: 0x13 = 01100011$
 $0x63 \times 2 = 11000110$
 $C \ 6$

$N: 3 \times C9 + 1 \times 05 + 1 \times F2 + 2 \times C0$
 $A: 0xC9 = 11000111$
 $0xC0 = 11000000$
 $0xC9 \times 3 = 110001101$
 $0xC0 \times 2 = 100011011$
 010110101
 $5 \ 2$
 $S2$
 05
 $F2$
 98
 $3E$

$DE \times 2E = F0$
 $66 \times 01 = 07$
 $CF \times 07 = C8$
 $FG \times 71 = 87$
 $45 \times 26 = 63$
 $A2 \times 53 = F1$
 $E5 \times 1B = FE$
 $B3 \times 7E = FD$
 $6D \times 1D = 70$