

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

Subbytes

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
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.

	Shift CF		Shift CA
4A84C = 06		73063 = 10	
54065 = 31	C7	6504F = 2A	F5
61074 = 15	59	59066 = 3F	75
75065 = 10	CA	72076 = 04	F2
7506F = 3A	A2	7406B = 1F	00
68069 = 0C	FE	51075 = 22	93
7904F = 3C	05	6F048 = 27	0C
41061 = 20	B7	65065 = 00	63

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

CF = 0110	1111	FE = 1111	1110
K2 = 0110	11110	K = 1111	11100
D	E	FE	3111 11110

DE	1000	00010
19	1000	11011
35	0000	11001
63		

xor

DE	1	9
19		
35		
63		

DI

[illegible]

$$D) 02 \times CA \oplus 03 \times A2 \oplus 01 \times FE \oplus 01 \times CC =$$

CA = 1100	1010	A2 = 1010	0010
X2 = 1100	10100	X2 = 1010	001000
X0R = 1000	11011	A2 = 0101	00010
0100	01111	1111	00110
8	7	X21000	11011
8F		0111	11101
FD		F	D
X0R	CC		

$$0B \times$$

$$E) 01 \times CF \oplus 02 \times FE \oplus 03 \times 75 \oplus 01 \times 63 =$$

FE = 1111	1110	FE = 0111	0101
X2 = 1111	11100	X2 = 0111	01010
X0R = 1000	11011	75 = 0011	10101
0111	0111	0100	11111
F	7	9	F

$$CF$$

$$D3$$

$$X0R$$

$$8F$$

$$63$$

$$74$$

f) $01 \text{ KCF} + 03 \text{ K05} + 03 \text{ KF2} + 01 \text{ K60} =$

05 = 000 0	0101	F2 = 1111	0010
x2 = 000 0	0101 0	x2 = 1111	0010 00
	0 A	F2 = 0111	1001 10

C3	1000	10110
0A	1000	11011
x0R 0 D	0000	01101
CO	0	D

00 ~~4~~

g) $01 \text{ K09} + 02 \text{ KB7} + 03 \text{ KCA} + 01 \text{ K13} =$

B7 = 1011	0111	CA = 1100	1010	59
x2 = 1011	0111 0	x2 = 1100	1010 00	59 25
x0R 1000	1101 1	CA = 1100	1010 10	59 25
	0011	1010	11110	93
	7	5	1011	FA 4
		0010	00101	
		4	5	

h) $01 \text{ KCA} + 02 \text{ K48} + 03 \text{ KES4} + 01 \text{ KCC} =$

A2 = 1010	0010	E5 = 1110	0101	CA
x2 = 1010	0010 00	E2 = 1110	0101 0	5F
x0R 1000	11011	E5 = 0111	00101	5F CC
	0010	1001	01111	60 4
	5	F	1000	11011
		0001	10100	
		3	F	

$$J) 0101 \oplus 1011 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 =$$

$\begin{array}{r} 75 = 0111 \quad 0101 \\ x2 = 0111 \quad 0101 \quad 10 \\ \hline \quad \quad \quad E \quad A \end{array}$	$\begin{array}{r} 63 = 0110 \quad 0111 \\ x2 = 0110 \quad 0110 \quad 10 \\ 632 = 0011 \quad 0001 \quad 11 \\ \hline \quad \quad \quad 0101 \quad 0101 \\ \quad \quad \quad A \quad \quad B \end{array}$
--	---

$\begin{array}{c} GF \\ FE \\ CA \\ AS \\ \hline DC \end{array}$

$$J) 0101 \oplus 1011 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 =$$

$\begin{array}{r} 72 = 1111 \\ x2 = 1111 \quad 0101 \\ x0R = 1000 \quad 1110 \\ \hline \quad \quad \quad 0111 \quad 1110 \\ \quad \quad \quad F \quad \quad E \end{array}$	$\begin{array}{r} 60 = 1100 \quad 0000 \\ x2 = 1100 \quad 0000 \\ 10 = 0110 \quad 0000 \quad 10 \\ \hline \quad \quad \quad 1010 \quad 0000 \\ x0R = 1000 \quad 1011 \\ \hline \quad \quad \quad 0010 \quad 1101 \\ \quad \quad \quad \quad \quad B \end{array}$
--	--

$\begin{array}{c} CD \\ 00 \\ GF \\ SE \\ \hline 63 \end{array}$

$$K) 0101 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 =$$

$\begin{array}{r} 67 = 0000 \quad 0111 \\ x2 = 0000 \quad 0111 \quad 10 \\ \hline \quad \quad \quad 0 \quad E \end{array}$	$\begin{array}{r} 58 = 0001 \quad 1011 \\ x2 = 0001 \quad 1011 \quad 10 \\ 58 = 0000 \quad 1011 \quad 11 \\ \hline \quad \quad \quad 0001 \quad 0110 \\ \quad \quad \quad \quad \quad 2 \quad D \end{array}$
--	--

$\begin{array}{c} B3 \\ 7C \\ 0E \\ 7D \\ \hline FC \end{array}$

$$N) 1011 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 \oplus 0101 =$$

$\begin{array}{r} 75 = 1110 \quad 1010 \\ x2 = 1110 \quad 1010 \\ x0R = 1000 \quad 1101 \\ \hline \quad \quad \quad 0110 \quad 1000 \\ \quad \quad \quad D \quad \quad I \end{array}$	$\begin{array}{r} 70 = 1100 \quad 1100 \\ x2 = 1100 \quad 1100 \quad 10 \\ 70 = 0110 \quad 0110 \quad 10 \\ \hline \quad \quad \quad 1010 \quad 1010 \\ x0R = 1000 \quad 1011 \\ \hline \quad \quad \quad 0010 \quad 0111 \end{array}$
---	--

$\begin{array}{c} GA \\ AP \\ BI \\ 9E \\ \hline FG \end{array}$

$M \rightarrow 3 * 6F + 1 * FE + 1 * 95 + 2 * 43$
 ①
 $A: 0x6F = 01101111$
 $0x6F * 2 = 11011110$
 $0x6F * 3 = 10110001$
 $B \quad 1$

$B: 0x43 = 01100011$
 $0x43 * 2 = 11000110$
 $C \quad 6$

$N \rightarrow 1 * C9 + 1 * 05 + 1 * F2 + 2 * C0$
 ②
 $A: 0xC9 = 11000111$
 $0xC9 * 2 = 11000110$
 $0xC9 * 3 = 10100101$
 10001101
 01010101
 $5 \quad 2$

$B: 0x05 = 01100000$
 $0x05 * 2 = 11000000$
 10001101
 01001101
 $9 \quad B$

Xor
 $\begin{array}{r} 52 \\ 05 \\ F2 \\ \hline 9B \\ 3E \end{array}$

$0 \rightarrow 2 * 59 + 01 * 89 + 01 * CA + 02 * 93$
 ④
 $A: 0x59 = 01011001$
 $0x93 * 2 = 010110010$
 $0x59 * 3 = 011101011$
 $\begin{array}{cc} E & B \end{array}$
 $\begin{array}{c} EB \\ 3 \\ C \\ A \\ 3 \\ D \\ AB \end{array}$
 $\begin{array}{c} 4 \\ 5 \end{array}$
 xor
 $\begin{array}{c} 4 \\ 5 \\ 8 \\ 3 \\ 81 \end{array}$

Downloaded from <http://ajph.org/> at University of California, San Diego on June 11, 2015
