

NCD

$\sqrt{^M}$ 0x56	1	2	3	4	5	6	7	8
	0	1	0	1	0	1	1	0
i 0x69	9	10	11	12	13	14	15	16
	0	1	1	0	1	0	0	1
o 0x6F	17	18	19	20	21	22	23	24
	0	1	1	0	1	1	1	1
l 0x6C	25	26	27	28	29	30	31	32
	0	1	1	0	1	1	0	0
e 0x65	33	34	35	36	37	38	39	40
	0	1	1	0	0	1	0	1
t 0x74	41	42	43	44	45	46	47	48
	0	1	1	1	0	1	0	0
a 0x61	49	50	51	52	53	54	55	56
	0	1	1	0	0	0	0	1
s 0x73	57	58	59	60	61	62	63	64
	0	1	1	1	0	0	1	1

		IP								
		58	50	42	34	26	18	10	2	
UD		1	1	1	1	1	1	1	1	FF
	60	52	44	36	28	20	12	4		
	1	0	1	0	0	0	0	1		AF
	62	54	46	38	30	22	14	6		
	0	0	1	1	1	1	0	1		3D
	64	56	48	40	32	24	16	8		
	1	1	0	1	0	1	1	0		D6
	S7/1	49/2	41/3	33/4	25/5	17/6	9/7	1/8		
RO	0	0	0	0	0	0	0	0		00
	59/9	51/10	43/11	35/12	27/13	19/14	11/15	3/16		
	1	1	1	1	1	1	1	0		FE
	61/17	53/18	45/19	37/20	29/21	21/22	13/23	5/24		
	0	0	0	0	1	1	1	0		06
	63/25	55/26	47/27	39/28	31/29	23/30	15/31	7/32		
	1	0	0	0	0	1	0	1		85

E									
32	1	2	3	4	5	4	5		
1	0	0	0	0	0	0	0		
6	7	8	9	8	9	10	11		
0	0	0	1	0	1	1	1		
12	13	12	13	14	15	16	17		
1	1	1	1	1	1	0	0		
16	17	18	19	20	21	20	21		
0	0	0	0	0	1	0	1		
22	23	24	25	24	25	26	27		
1	1	0	1	0	1	0	0		
28	29	28	29	30	31	32	1		
0	0	0	0	1	0	1	0		

Salida de f

P								
16	7	20	21	29	12	28	17	
0	1	0	0	0	1	0	1	45
1	15	23	26	5	18	31	10	
0	0	0	0	1	1	1	0	4E
2	8	24	14	32	27	3	9	
0	1	1	0	1	1	0	1	6D
19	13	30	6	22	11	4	25	
1	0	0	0	1	0	0	1	89

The diagram shows an 8-bit ALU. The input $E(R0)$ is a 16-bit value: 1 0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 1 1 1 0 1 0 1 0 0 0 0 0 1 0 1 0. The input $XOR\ k1$ is a 16-bit value: 1 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 1 1 0 1 1 1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 0 0 0 0 0 1 1 0 0 0 0. The output is an 8-bit value S divided into four 4-bit segments: $S1$ (0 0 0 0), $S2$ (1 0 1 1), $S3$ (1 0 0 1), $S4$ (0 0 1 0), $S5$ (1 1 1 0), $S6$ (0 1 0 1), $S7$ (1 0 1 0), and $S8$ (0 0 1 1). Below each segment, the value is converted to decimal: $F=00=0, C=1110=14$; $F=00=0, C=0101=5$; $F=10=2, C=0011=3$; $F=00=0, C=1001=9$; $F=00=0, C=1110=14$; $F=01=1, C=0111=7$; $F=10=2, C=1000=8$; $F=10=2, C=1101=13$.

LO 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 0 1 0 1 1 0
 XOR f 0 1 6 0 0 1 0 1 0 1 0 0 1 1 1 6 0 1 1 0 1 1 0 0 0 1 0 0 1

 1 0 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 0 0 0 0 1 1 0 1 1 1 1

L1= 0X 00 FE 0E 85
R1= 0X B4 E F 5 0 5 F

Sanchez Mendez Edmundo Jose

Proceso para la Generación de Subllaves Ki

Key	1	2	3	4	5	6	7	8
50x7B	0	1	1	1	0	0	1	1
9	10	11	12	13	14	15	16	
e0x65	0	1	1	0	0	1	0	1
17	18	19	20	21	22	23	24	
c0x63	0	1	1	0	0	0	1	1
25	26	27	28	29	30	31	32	
u0x75	0	1	1	1	0	1	0	1
33	34	35	36	37	38	39	40	
r0x72	0	1	1	1	0	0	1	0
41	42	43	44	45	46	47	48	
i0x69	0	1	1	0	1	0	0	1
49	50	51	52	53	54	55	56	
t0x7A	0	1	1	1	0	1	0	0
57	58	59	60	61	62	63	64	
y0x79	0	1	1	1	1	0	0	1

PC-1							
57	49	41	33	25	17	9	1
0	0	0	0	0	0	0	0
58	50	42	34	26	18	10	2
1	1	1	1	1	1	1	1
59	51	43	35	27	19	11	3
1	1	1	1	1	1	1	1
60	52	44	36	63	55	47	39
1	1	0	1	0	0	0	1
31	23	15	7	62	54	46	38
0	1	0	1	0	1	0	0
30	22	14	6	61	53	45	37
1	0	1	0	1	0	1	0
29	21	13	5	28	20	12	4
0	0	0	0	1	0	0	1

PC-2 para K1							
14	17	11	24	1	5	3	28
1	1	1	1	0	0	0	0
15	6	21	10	23	19	12	4
1	0	1	1	1	1	1	0
26	8	16	7	27	20	13	2
0	1	1	0	1	1	1	0
41	52	31	37	47	55	30	40
0	1	1	1	0	1	0	1
51	45	33	48	44	49	39	56
0	0	1	0	1	0	0	0
34	53	46	42	50	36	29	32
0	0	1	1	0	0	0	0

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
CO=	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
DO=	0	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
C1=	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
D1=	0	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	1	0

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
C8=	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
D8=	1	0	1	0	1	0	0	0	0	0	1	0	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0

PC-2 para K8							
14	17	11	24	1	5	3	28
1	0	1	1	1	1	1	1
15	6	21	10	23	19	12	4
0	1	0	1	1	0	1	1
26	8	16	7	27	20	13	2
1	1	0	1	1	0	0	1
41	52	31	37	47	55	30	40
0	1	1	0	0	1	0	0
51	45	33	48	44	49	39	56
0	0	1	1	0	0	1	0
34	53	46	42	50	36	29	32
0	0	1	1	1	0	1	0

K1= 0x F 0 B E 6 E 7 5 2 8 3 0

K8= 0x B E 5 0 9 6 9 3 2 3 A

Sanchez Mendez Edmundo Joss