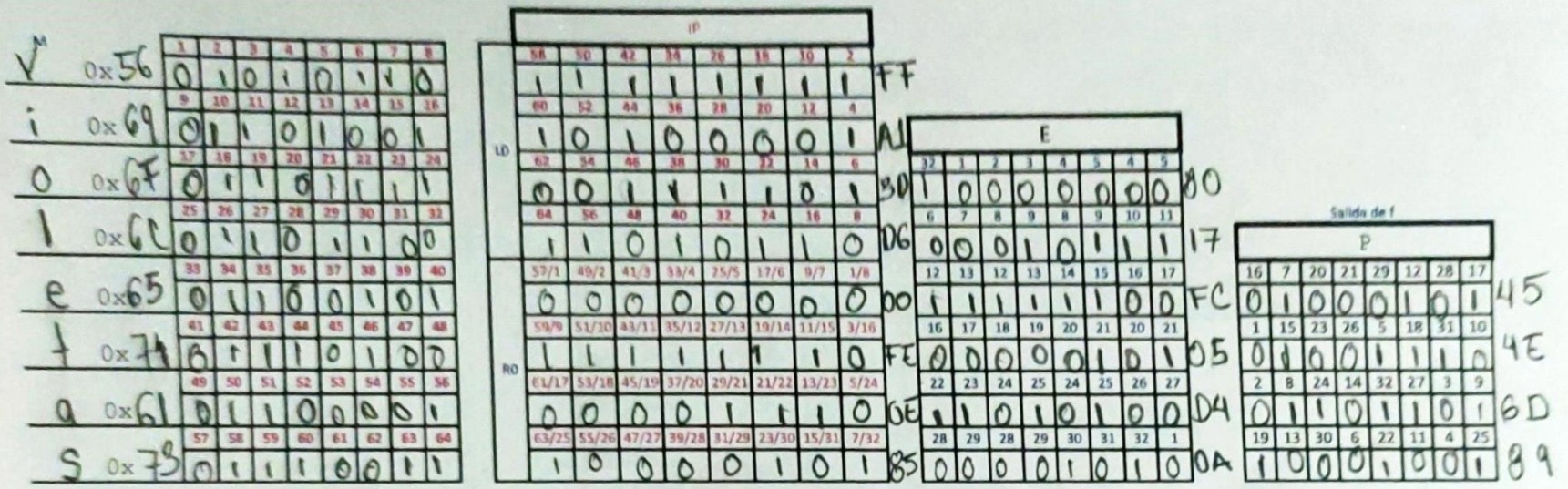
DES

NCD



E(R0) 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 1 0 1 0

XOR k1 1 1 1 1 0 0 0 0 1 0 1 1 1 1 0 0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 1 1 1 0 1 0 0 0 0 0 1 1 0 0 0 0

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

S1	S2	S3	S4	S5	S6	S7	S8
0 0 0 0	1 0 1 1	1 0 0 1	0 0 1 0	1 1 1 0	0 1 0 1	1 0 1 0	0 0 1 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	29 30 31 32
F=00=0	F=00=0	F=10=2	F=00=0	F=00=0	F=01=1	F=10=2	F=10=2
C=1110=14	C=0101=5	C=0011=3	C=1001=9	C=1110=14	C=0111=7	C=1000=8	C=1101=13

L0 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0 1 1 1 1 0 1 1 1 0 1 0 1 1 0

XOR f 0 1 0 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 1 0 1 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 1 0 1 0 1 0 0 0 0 0 1 0 1 1 1 1 1

L1= 0X 0 0 F E 0 E 0 5

R1= 0X B A E F 5 0 5 F

Sanchez Hendez Edmundo Jose

Proceso para la Generación de Subllaves Ki

Key

	1	2	3	4	5	6	7	8
S 0x B	0	1	1	1	0	0	1	1
e 0x 65	0	1	1	0	0	1	0	1
C 0x 63	0	1	1	0	0	0	1	1
U 0x 75	0	1	1	1	0	1	0	1
r 0x 72	0	1	1	1	0	0	1	0
i 0x 69	0	1	1	0	1	0	0	1
t 0x 74	0	1	1	1	0	1	0	0
y 0x 79	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	00
	58	50	42	34	26	18	10	2
C0	1	1	1	1	1	1	1	1	FF
	59	51	43	35	27	19	11	3
	1	1	1	1	1	1	1	1	FF
	60	52	44	36	63	55	47	39
	1	1	0	1	0	0	0	1	D1
	31	23	15	7	62	54	46	38
	0	1	0	1	0	1	0	0	54 D0
	30	22	14	6	61	53	45	37
	1	0	1	0	1	0	1	0	AA
	29	21	13	5	28	20	12	4
	0	0	0	0	1	0	0	1	09

PC-2 para K1

	14	17	11	24	1	5	3	28
	1	1	1	1	0	0	0	0	F0
	15	6	21	10	23	19	12	4
	1	0	1	1	1	1	1	0	BE
	26	8	16	7	27	20	13	2
	0	1	1	0	1	1	1	0	6E
	41	52	31	37	47	55	30	40
	0	1	1	1	0	1	0	1	75
	51	45	33	48	44	49	39	56
	0	0	1	0	1	0	0	0	28
	34	53	46	42	50	36	29	32
	0	0	1	1	0	0	0	0	30

	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
C0=	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	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
D0=	0	0	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	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	0

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

14

	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	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	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	BF
	15	6	21	10	23	19	12	4
	0	1	0	1	1	0	1	1	5B
	26	8	16	7	27	20	13	2
	1	1	0	1	1	0	0	1	D9
	41	52	31	37	47	55	30	40
	0	1	1	0	0	1	0	0	64
	51	45	33	48	44	49	39	56
	0	0	1	1	0	0	1	0	32
	34	53	46	42	50	36	29	32
	0	0	1	1	1	0	1	0	3A

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

K8= 0x B F 5 B D 9 6 4 3 2 3 A

Sanchez Mendez Edmundo Jesus