Proceso para la Generación de Subllaves Ki

Key	1	2	3	4	5	6	7	8																				
0x														PC	:-1													
	9	10	11	12	13	14	15	16	•		57	49	41	33	25	17	9	1										
0x																							PC	:-2 p	ara	K1		
	17	18	19	20	21	22	23	24			58	50	42	34	26	18	10	2			14	17	11	24	1	5	3	28
0x										CO																		
	25	26	27	28	29	30	31	32			59	51	43	35	27	19	11	3			15	6	21	10	23	19	12	4
0x																							- 15	_			- 10	
0x	33	34	35	36	37	38	39	40			60	52	44	36	63	55	47	39	,		26	8	16	7	27	20	13	2
UX	41	42	43	44	45	46	47	48			31	23	15	7	62	54	46	38			41	52	31	37	47	55	30	40
0x																												
	49	50	51	52	53	54	55	56			30	22	14	6	61	53	45	37	D0		51	45	33	48	44	49	39	56
0x																												
	57	58	59	60	61	62	63	64			29	21	13	5	28	20	12	4			34	53	46	42	50	36	29	32
0x																												
1 2	3	4	5	6	7	8	9	10	11	12	12	1/1	15	16	17	18	19	20	21	22	23	24	25	26	27	28		
C0=	٦	Ī	٦					10		12	13	14		10		10	13	20						20		20		
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	I	
D0=																												
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=																												
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=																												
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	ľ	
C_= 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	l	
D_=	31	32	33	54	35	30	5/	38	39	40	41	42	43	44	45	40	4/	48	49	50	21	52	5 3	54	22	30	Ī	
~ <u>-</u>		<u> </u>	<u> </u>																								l	

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

K1= 0x	_	_	_	_	_	_	_	_	_	_	_	_