																	\top
					(Driginal		Comp	lement		İ						\dagger
			K	Cey		234 12341234	E	DCBEDCE	BEDCBED	CB							T
			Plai	intext	123456	78ABCDEF12		EDCBA98									T
			Ciph	nertext	E112BE	1DEFC7A367		???????	???????	??							I
																	1
	Sr. No	Binary	IP	Output													+
	1	1	1														T
Е	2	1	0	9													
_	3	1	0														
	4	0	1														
	5	1	0														1
D	6	1	0	3													1
	7	0	1														4
	8	1	1					1			P			-			4
	9	1	0	4			58	50	42	34	26	18	10	2			4
С	10	1	1	7			60	52	44	36	28	20	12	4			4
	11	0	1				62	54	46	38	30	22	14	6			+
	12	0	1				64	56	48	40	32	24	16	8			+
	13	1	0				57	49	41	33	25	17	9	1			4
В	14	0	0	0			59	51	43	35	27	19	11	3			+
	15	1	0				61	53	45	37	29	21	13	5			+
	16	1	0				63	55	47	39	31	23	15	7			+
	17	1	1														+
Α	18	0	0	9						<u> </u>							+
	19	1	0					00	1 4		on P-box	1	-				+
	20	0	1					32	1 5	2	3	4	5				+
	21	1	1					4	5	6	7	8	9				+
9	22	0	0	9				8	9	10	11	12	13				+
	23	0	0					12	13	14	15	16	17				+
	24	1	1					16	17	18	19	20	21				+
	25	1	1					20	21	22	23	24	25				+
8	26	0	0	8				24	25	26	26	27	28				+
	27	0	0					28	29	30	31	32	1				+
	28	0	0														+
	29	0	1							01	1.5.1						+
7	30	1	1	F			40	7	1 00		t P-box	40	00	47			+
	31	1	1				16	7	20	21	29	12	28	17			+
	32	1	1				1	15	23	26	5	18	31	10			+
	33	0	1				2	8	24	14	32	27	3	9			+
5	34	1	0	8			19	13	30	6	22	11	4	25			+
	35	0	0														+
	36	1	0														

	37	0	1								Р	C1							
	38	1	1					57	49	41	33	25	17	9	1				
4	39	0	1	F				58	50	42	34	26	18	10	2				
	40	0	1	1 1				59	51	43	35	27	19	11	3				
	41	0	1					60	52	44	36	63	55	47	39				
	42	0	0	1				31	23	15	7	62	54	46	38				
3	43	1	1	A				30	22	14	6	61	53	45	37				
	44	1	0	1 1				29	21	13	5	28	20	12	4				
	45	0	0								_				-				
	46	0	1	1															
2	47	1	0	5							Р	C2							
	48	0	1	1 1				14	17	11	24	1	5	3	28				
	49	0	1					15	6	21	10	23	19	12	4				
	50	0	0	1				26	8	16	7	27	20	13	2				
1	51	0	0	8				41	52	31	37	47	55	30	40				
	52	1	0					51	45	33	48	44	49	39	56				
	53	0	0					34	53	46	42	50	36	29	32				
	54	0	1	1 _ 1															
0	55	0	1	7															
	56	0	1	1 1															
	57	1	0																
_	58	1	0	1 . 1															
Е	59	1	1	2															
	60	0	0	1 1															
	61	1	1																
_	62	1	0	1 , [
D	63	0	1	A															
	64	1	0																
							No. o	of Shifts =	1 bit										
													145 =			\		-	
			PC1	L-Shift		Round		Sr. No	Key	L0	R0	EP box	XOR	S Box	Straigh		Hex.		
	1	1	1	1	1			1	1	1	1	0	1	0	1	0			
Е	2	1	1	1	1	Е		2	1	0	0	1	0	1	0	0	3		
-	3	1	1	1	1	-		3	1	0	0	0	1	1	1	1			
	4	0	1	1	0			4	0	1	0	0	0	0	0	1			
	5	1	1	1	1			5	1	0	1	0	1	0	0	0			
D	6	1	1	1	1	F		6	1	0	1	1	0	0	1	1	4		
_	7	0	1	1	1	·		7	1	1	1	0	1	0	1	0			
	8	1	1	1	1			8	1	1	1	1	0	0	1	0			
	9	1	1	1	1			9	1	0	1	1	0	0	0	0			

	10	1	1	1	1	1		10	1	1	0	1	0	0	1	0			
С	11	0	1	1	1	F		11	1	1	1	1	0	1	1	0	0		
	12	0	1	1	1	1		12	1	1	0	1	0	1	1	0			
	13	1	1	1	1			13	1	0	0	1	0	1	0	0			
	14	0	1	1	1	1		14	1	0	1	1	0	0	1	1			
В	15	1	1	1	1	F		15	1	0	0	0	1	1	0	0	4		
	16	1	1	0	1	-		16	1	0	1	1	0	1	0	0			
	17	1	0	1	0			17	0	1	1	0	0	1	1	0			
	18	1	1	0	1	1		18	1	0	0	0	1	1	0	0			
Е	19	1	0	1	0	6		19	0	0	0	0	0	1	1	1	3		
	20	0	1	0	1	-		20	1	1	0	0	1	1	0	1			
	21	1	0	1	0			21	0	1	0	1	1	0					
		1	1	0		1		22	0	0	1	0	0	0	1	0			
D	22 23		0	1	0	3		23	1	0	1	1	0	1	1	1	7		
	23	0		$\overline{}$		-							0		0				
	25	1	1	0	1			24 25	1	1	1	1		1		1		 	
			0	0	1	-		25 26	1	1	0	1	0	1	1	0			
С	26	1	0	0	0	9			0	0	0		0	1			6		
	27	0	0	0	0			27	0	0	1	0		1	1	1			
	28	0	0	1	1			28	1	0	0	0	1	1	0	0			
	29	1	1	0	1			29	1	1	1	0	1	0		1			
В	30	0	0	1	0	Α		30	0	1	0	0	0	1	1	0	Α		
	31	1	1	0	1			31	1	1	1	0	1	0	0	1			
	32	1	0	1	0			32	0	1	0	0	0	1	1	0			
	33	1	1	0	1			33	1			1	0						
Е	34	1	0	1	1	D		34	1			1	0						
_	35	1	1	0	0			35	0			1	1						
	36	0	0	0	1			36	1			0	1						
	37	1	0	1	1			37	1			1	0						
D	38	1	1	0	1	F		38	1			0	1						
	39	0	0	1	1] '		39	1			0	1						
	40	1	1	0	1			40	1			1	0						
	41	1	0	1	1]		41	1			0	1						
С	42	1	1	0	0	A		42	0			1	1						
	43	0	0	1	1] ^		43	1			0	1						
	44	0	1	1	0			44	0			1	1						
	45	1	1	1	1			45	1			0	1						
D I	46	0	1	1	0			46	0			1	1						
В	47	1	1	1	0	9		47	0			0	0						
	48	1	1	1	1			48	1			1	0						
	49	1	1	1															
_	50	1	1	1															
E	51	1	1	1															
	52	0	1	0															

	53	1	0	0	1													T
	54	1	0	0														1
D	55	0	0	0														+
_	56	1	0	1														
	57	1		•													-	-
	58	1																+
С	59	0																+
_	60	0			1													+
	61	1																+
	62	0																
В	63	1																
	64	1																
					No. o	f Shifts =	1 bit											
Sr. N	o Binary	L-Shift	PC2	Round	Sr. No	Key	L1	R1	EP box	XOR	S Box	Straigh	XOR	Hex.				
1	1	1	1	1	1	1	1	0	0	1	0	1	0					
2	1	1	0	1.	2	0	0	0	0	0	0	1	1	1 .				
3	1	1	1	A	3	1	0	1	0	1	0	1	1	6				
4	1	1	0	1	4	0	0	1	1	1	1	0	0	1				
5	1	1	1		5	1	1	0	1	0	1	1	0					
6	1	1	1	1 _	6	1	1	1	0	1	0	0	1	1 ,				
7	1	1	1	⊢ F	7	1	1	0	1	0	1	0	1	6				
8	1	1	1	1	8	1	1	0	0	1	1	1	0	1				
9	1	1	0		9	0	1	0	1	1	0	0	1					
10	1	1	1	٦ ,	10	1	0	0	0	1	1	1	1					
11	1	1	0	5	11	0	1	0	0	0	1	1	0	С				
12	1	1	1		12	1	0	0	0	1	0	0	0					
13	1	1	0		13	0	0	0	0	0	1	1	1					
14	1	1	0	3	14	0	1	1	0	0	0	1	0					
15	1	0	1	`	15	1	0	0	0	1	1	0	0	8				
16	0	1	1		16	1	1	0	0	1	1	1	0					
17	1	0	0		17	0	1	0	0	0	1	0	1					
18	0	1	1	7	18	1	0	0	0	1	1	1	1	С				
19	1	0	1	」 ′	19	1	0	1	0	1	0	0	0					
20	0	1	1		20	1	0	1	0	1	1	0	0					
21	1	0	1	_	21	1	0	0	1	0	0	0	0					
22	0	1	1	F	22	1	1	1	0	1	1	0	1	7				
23	1	0	1	」 '	23	1	1	1	0	1	1	0	1					
24	0	0	1		24	1	1	1	0	1	0	0	1					
25	0	0	0		25	0	0	0	0	0	1	0	0					
															•		1	1
26 27	0	0	0	2	26 27	0	0	1	0	0	0	1	1	4				

				-													 		_
28	1	1	0			28	0	0	0	1	1	0	0	0					
29	0	1	1			29	1	1	1	1	0	1	1	0					
30	1	0	1	D		30	1	0	0	0	1	1	1	1	_				
31	0	1	0	ן די		31	0	1	1	1	1	0	1	0	- 5				Т
32	1	0	1	1		32	1	0	0	0	1	0	1	1					T
33	0	1	0			33	0			1	1								T
34	1	0	1	1		34	1			1	0								T
35	0	0	1	7		35	1			1	0								†
36	0	1	1	†		36	1			0	1								+
37	1	0	1			37	1			1	0								+
38	0	1	1	1		38	1			0	1								\top
39	1	0	0	C		39	0			1	1								\top
40	0	1	0	1		40	0			1	1								+
41	1	0	0			41	0			0	0								+
42	0	1	0	1		42	0			1	1					1			\dagger
43	1	1	1	3		43	1			0	1								+
44	1	1	1	1		44	1			1	0								+
45	1	1	1			45	1			0	1								+
46	1	1	1	†		46	1			1	0								+
47	1	1	1	E		47	1			0	1						+	+	+
48	1	1	0	1		48	0			0	0								+
49	1	1	_			40					,								+
50	1	1																	+
51	1	0																	+
52	0	0																	+
53	0	0																	+
54	0	0																	+
55	0	1																	+
56	1	0																	+
30	l	U																	+
						No. of	Shifts =	2 hito											+
						140. 01	Jillito -	Z DILO											+
Sr No	Binary	L-Shift	PC2	Round		Sr. No	Key	L2	R2	EP box	XOR	S Boy	Straigh	XOR	Hex.	Ī			+
1	1	1	1	I	-	1	1	0	0	1	0	0	1	1		-			+
2	1	1	0	1	-	2	0	0	1	0	0	1	0	0					+
3	1	1	1	A		3	1		1	1	0	0		0	8				+
4	1	1	0	+		4	0	1	0	1	1	0	1	0					+
4	'			1									0						+
-	4	1	1	+		5	1	0	0	0	1	1		0					+
5	1					6	1	1	1	0	1	0	1	0	3				+
6	1	1	1	F			1	0	1	0	1	0	1	1					
6 7	1	1	1	F		7													
6 7 8	1 1 1	1	1	F		8	1	0	0	0	1	1	1	1					1
6 7	1	1	1	F							1 1 0	0	0 1	0					1

11	1	1	0	د ا	11	0	0	0	0	0	1	1	1	ס ן			
12	1	1	1	l	12	1	0	0	1	0	1	0	0	-			
13	1	0	0		13	0	0	1	0	0	0	1	1				
14	1	1	0	İ	14	0	1	0	1	1	1	1	0	1			
15	0	0	1	3	15	1	0	0	1	0	1	0	0	9			
16	1	1	1	İ	16	1	0	0	0	1	1	1	1	1			
17	0	0	1		17		0	1	0	1	1	1	1				
18	1	1	1	i _	18	1	0	1	1	0	1	1	1	1 _			
19	0	0	1	F	19	1	1	0	0	1	1	1	0	С			
20	1	1	1	İ	20	1	1	0	1	0	1	1	0	1			
21	0	0	1		21	1	0	0	0	1	1	1	1				
22	1	0	1		22	1	1	1	0	1	0	0	1	1 _			
23	0	0	0	D	23	0	1	1	0	0	1	0	1	F			
24	0	0	1	İ	24	1	1	1	1	0	1	0	1				
25	0	1	1		25	1	0	0	0	1	1	1	1				
26	0	1	0	1 ,	26	0	1	1	1	1	0	0	1				
27	1	1	1	A	27	1	1	0	1	0	0	1	0	С			
28	1	1	0		28	0	0	0	0	0	1	0	0				
29	1	1	1		29	1	1	0	0	1	0	0	1				
30	0	0	1	D	30	1	0	1	0	1	1	1	1	F			
31	1	1	0		31	0	1	0	0	0	0	0	1				
32	0	0	1		32		0	1	0	1	1	1	1				
33	1	0	0		33				1	1							
34	0	1	1	5	34	1			1	0							
35	0	0	0]	35	0			1	1							
36	1	1	1		36				0	1							
37	0	0	1	[37				1	0							
38	1	1	0	8	38	0			0	0							
39	0	0	0]	39				1	1							
40	1	1	0		40				0	0							
41	0	1	1	ļ	41				0	1							
42	1	1	1	F	42				0	1							
43	1	1	1	ļ .	43	_			0	1							
44	1	1	1		44	1			0	1							
45	1	1	0	ļ	45				1	1							
46	1	1	1	6	46	1			0	1			ļ				
47	1	1	1	•	47				1	0							
48	1	1	0		48	0			0	0							
49	1	0															
50	1	0															
51	0	0															
52	0	0															
53	0	1															

54	0	0														
55	1	1														
56	0	0														
					 No. of	Shifts =	2 bits									
		-		<u></u>												
_	Binary		PC2	Round	Sr. No	Key	L3	R3	EP box	XOR	S Box	Straigh		Hex.		
1 2	1	1	0	-	2	0	0	0	1	0	0	1	1			
3	1	1	0	9	3	0	1	0	0	0	1	1	0	9		
4	1	1	1	1	4	1	0	0	0	1	1	1	1	-		
5	1	1	1		5	1	0	0	0	1	0	1	1			
6	1	1	<u>'</u> 1	1	6	1	1	0	0	1	1	0	1			
7	1	1	<u>·</u> 1	∮ F	7	1	1	1	0	1	1	0	1	3		
8	1	1	1	1	8	1	0	1	0	1	0	1	1			
9	1	1	0		9	0	1	0	0	0	0	1	0			
10	1	1	1	1 _	10	1	1	1	1	0	0	1	0			
11	1	0	0	5	11	0	0	1	1	1	0	1	1	3		
12	1	1	1	1	12	1	0	0	0	1	0	1	1			
13	0	0	1		13	1	1	1	1	0	1	0	1			
14	1	1	0	В	14	0	0	0	0	0	0	1	1	С		
15	0	0	1] B	15	1	0	0	1	0	1	0	0			
16	1	1	1		16	1	0	1	1	0	1	0	0			
17	0	0	1	1	17	1	1	1	0	1	1	0	1			
18	1	1	1	l F	18	1	1	1	1	0	1	0	1	E		
19	0	0	1	1 .	19	1	0	0	0	1	0	1	1			
20	1	0	1	ļ	20	1	0	0	1	0	1	0	0			
21	0	0	1	1	21	1	0	1	0	1	1	1	1			
22	0	0	0	9	22	0	1	1	0	0	1	0	1	D -		
23	0	1	0	4	23	0	1	1	1	1	1	1	0			
24	0	1	1	-	24	11	1	1	1	0	1	0	1			
25 26	1	1	0	1	25 26	0	0	1	1	0	1		0			
26	1	1	0	8	26	0	0	0	1	1	0	0	0	1		
28	1	1	0	1	28	0	0	0	0	0	0	1	<u>0</u> 1			
29	1	1	0		29	0	0	1	0	0	1	1	1			
30	0	0	1	1	30	1	1	1	1	0	0	0	1			
31	1	0	0	5	31	0	0	1	0	0	0	1	1	E		
32	0	1	1	1	32	1	1	1	1	0	1	1	0			
33	0	0	1		33	1			1	0						
34	1	1	1	1 _	34	1			1	0						
35	0	0	0	C	35	0			1	1						
36	1	1	0	1	36	0			1	1						

37	0	0	1	_	37	1			1	0							
38	1	1	0		38	0			1	1							
39	0	1	1	A	39	1			1	0							
40	1	1	0	1	40	0			0	0							
41	1	1	1		41	1	1		0	1							
42	1	1	1	†	42	1	<u> </u>		1	0							
43	1	1	1	F	43	1	<u> </u>		0	1							
44				}	44	1	<u> </u>		1								-
	1	1	1				ļ			0					-		
45	1	1	0	-	45	0	ļ		1	1					-		+
46	1	1	1	7	46	1	ļ		1	0							-
47	1	0	1	ļ	47	1	ļ		1	0							
48	1	0	1		48	1			1	0							
49	0	0															
50	0	0															
51	0	1															
52	0	0															
53	1	1															
54	0	0															
	1	1															
55				 													
55		0															
	0	0															
55		0			No. of	Shifts =	2 hits										
55		0			No. of	Shifts =	2 bits										
55 56	0		PC2	Round				R4	I EP box	XOR	S Box	Straigh	XOR	Hex.			
55 56 Sr. No	0 Binary	L-Shift	PC2	Round	Sr. No	Key	L4	R4	EP box	XOR		Straigh	XOR	Hex.			
55 56 Sr. No	Binary	L-Shift	1	Round	Sr. No	Key	L4 1	1	0	1	1	1	0	Hex.			
55 56 Sr. No 1	0 Binary 1 1	L-Shift 1 1	1	Round	Sr. No 1 2	Key 1 0	L4 1 0	1 0	0	1	1 0	1	0	Hex.			
55 56 Sr. No 1 2 3	0 Binary 1 1 1	L-Shift 1 1 1	1 0 0		Sr. No 1 2 3	Key 1 0 0	1 0 0	1 0 0	0 1 0	1 1 0	1 0 0	1 1 0	0 1 0				
55 56 Sr. No 1 2 3 4	Binary 1 1 1 1	L-Shift 1 1 1	1 0 0 1		Sr. No 1 2 3 4	Key 1 0 0 1	L4 1 0 0	1 0 0	0 1 0 0	1 1 0 1	1 0 0	1 1 0 1	0 1 0 1				
55 56 Sr. No 1 2 3 4 5	Binary 1 1 1 1 1	L-Shift 1 1 1 1 1	1 0 0 1		Sr. No	Key 1 0 0 1 1	L4 1 0 0 0	1 0 0 1 1	0 1 0 0	1 1 0 1 0	1 0 0 1	1 1 0 1	0 1 0 1				
55 56 Sr. No 1 2 3 4 5 6	Binary 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1	1 0 0 1 1 1	9	Sr. No 1 2 3 4 5	Key 1 0 1 1 1 1	L4 1 0 0 0 0	1 0 0 1 1	0 1 0 0 1 1	1 1 0 1 0	1 0 0 1 1	1 1 0 1 1	0 1 0 1 1	5			
55 56 Sr. No 1 2 3 4 5 6 7	Binary 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1	1 0 0 1 1 1 1		Sr. No 1 2 3 4 5 6 7	Key 1 0 0 1 1 1 1	L4 1 0 0 0 0 0	1 0 0 1 1 1	0 1 0 0 1 1	1 1 0 1 0 0	1 0 0 1	1 1 0 1 1 0	0 1 0 1 1 0 0				
55 56 Sr. No 1 2 3 4 5 6 7	Binary 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 0 1 1 1 1 1	9	Sr. No 1 2 3 4 5 6 7	Key 1 0 0 1 1 1 1 1	L4 1 0 0 0 0 0 0	1 0 0 1 1 1 1	0 1 0 0 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 0	5			
55 56 Sr. No 1 2 3 4 5 6 7	Binary 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 0 1 1 1 1	9	Sr. No 1 2 3 4 5 6 7	Key 1 0 0 1 1 1 1	L4 1 0 0 0 0 0	1 0 0 1 1 1	0 1 0 0 1 1	1 1 0 1 0 0 0 0	1 0 0 1 1 1	1 1 0 1 1 0	0 1 0 1 1 0 0	5			
55 56 Sr. No 1 2 3 4 5 6 7	Binary 1 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 0 1 1 1 1 1	- 9 - F	Sr. No 1 2 3 4 5 6 7	Key 1 0 0 1 1 1 1 1 1	L4 1 0 0 0 0 0 0	1 0 0 1 1 1 1	0 1 0 0 1 1 1	1 0 1 0 0 0 0	1 0 0 1 1 1 1	1 0 1 1 0 1 0	0 1 0 1 1 0 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9	Binary 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 1 0	1 0 0 1 1 1 1 1 1	9	Sr. No 1 2 3 4 5 6 7 8 9	Key 1 0 0 1 1 1 1 1 0 0	L4 1 0 0 0 0 0 0 1 1	1 0 0 1 1 1 1 1 1	0 1 0 0 1 1 1 1	1 1 0 1 0 0 0 0	1 0 0 1 1 1 1 1 0	1 0 1 1 0 1 0	0 1 0 1 1 0 0 1	5			
55 56 Sr. No 1 2 3 4 5 6 7 8 9	Binary 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 0 1	1 0 0 1 1 1 1 1 0	- 9 - F	Sr. No 1 2 3 4 5 6 7 8 9	Key 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L4 1 0 0 0 0 0 0 1 1	1 0 0 1 1 1 1 1 0	0 1 0 0 1 1 1 1 1	1 0 1 0 0 0 0 0 0	1 0 0 1 1 1 1 1 0	1 1 0 1 1 0 1 0 1	0 1 0 1 1 0 0 0 1 1	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11	Binary 1 1 1 1 1 1 1 1 1 1 0	L-Shift 1 1 1 1 1 1 1 1 1 0 1 0	1 0 0 1 1 1 1 1 0 1	- 9 - F	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12	Key 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L4 1 0 0 0 0 0 0 1 1 1	1 0 0 1 1 1 1 1 1 0	0 1 0 0 1 1 1 1 1	1 1 0 1 0 0 0 0 0	1 0 0 1 1 1 1 1 0 1	1 1 0 1 1 0 1 0 1 1 1	0 1 0 1 1 0 0 0 1 1 1 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Binary 1 1 1 1 1 1 1 1 1 1 1 0 1 0	L-Shift 1 1 1 1 1 1 1 1 1 1 1 0 1 0 1 0	1 0 0 1 1 1 1 1 0 1 1 1	9 - F - 7	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Key 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L4 1 0 0 0 0 0 1 1 0 1 1	1 0 0 1 1 1 1 1 0 0	0 1 0 0 1 1 1 1 1 1 1 1 0	1 1 0 1 0 0 0 0 0 0 1 0 0 0	1 0 0 1 1 1 1 1 0 1 1 0	1 1 0 1 1 0 1 0 1 1 1 1 1	0 1 0 1 1 0 0 1 1 0 0 0 1 1 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Binary 1 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1	L-Shift 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 0 1 1 1 1 1 0 1 1 1 1 1 0	- 9 - F	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Key	L4 1 0 0 0 0 0 1 1 1 0 1 0	1 0 0 1 1 1 1 1 0 0 0 1 1	0 1 0 0 1 1 1 1 1 1 1 1 0 0	1 0 1 0 0 0 0 0 1 0 0 0 1 0 0	1 0 0 1 1 1 1 0 1 1 0 0	1 1 0 1 1 0 1 0 1 1 1 1 1	0 1 0 1 1 0 0 1 1 0 0 1 1 0 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Binary 1 1 1 1 1 1 1 1 0 1 0 1 0	L-Shift 1 1 1 1 1 1 1 1 0 1 0 1 0 1 0	1 0 0 1 1 1 1 1 0 1 1 1 1 1 0 1	9 - F - 7	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Key 1 0 0 1 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1	L4 1 0 0 0 0 0 1 1 1 0 1 0 0 0 0 0 0 0 0	1 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1	0 1 0 0 1 1 1 1 1 1 1 1 0 0	1 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 0 1	1 0 0 1 1 1 1 0 1 1 0 0 1	1 0 1 1 0 1 0 1 1 1 1 1 1 1	0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 0 1 0 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Binary 1 1 1 1 1 1 1 1 0 1 0 1 0 1	L-Shift 1 1 1 1 1 1 1 0 1 0 1 0 1 1	1 0 0 1 1 1 1 1 0 1 1 1 1 0 1 1 1 1 1 1	9 - F - 7	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Key	L4 1 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 0 0 0 0 1 0	1 0 0 1 1 1 1 1 0 0 1 1 1 1 1 1 0 0	0 1 0 0 1 1 1 1 1 1 1 0 0	1 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0	1 0 0 1 1 1 1 0 1 1 0 0 1 1 1	1 0 1 1 0 1 0 1 1 1 1 1 1 1 1	0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Binary 1 1 1 1 1 1 1 1 0 1 0 1 0 1 0 0	L-Shift 1 1 1 1 1 1 1 0 1 0 1 0 1 0 1 0	1 0 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1	9 - F - 7	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Key 1 0 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1	L4 1 0 0 0 0 0 1 1 1 0 1 0 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1	1 0 0 1 1 1 1 1 0 0 1 1 1 1 1 1 0 0 0 1 1 1 1 0 0 1 1 1 0 0 0 1	0 1 0 0 1 1 1 1 1 1 1 0 0 1 0	1 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0	1 0 0 1 1 1 1 0 1 1 0 0 1 1 1 1 0	1 1 0 1 1 0 1 1 1 1 1 1 1 1 0	0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	9			
55 56 Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Binary 1 1 1 1 1 1 1 1 0 1 0 1 0 1	L-Shift 1 1 1 1 1 1 1 0 1 0 1 0 1 1	1 0 0 1 1 1 1 1 0 1 1 1 1 0 1 1 1 1 1 1	9 - F - 7	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Key	L4 1 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0 1 0	1 0 0 1 1 1 1 1 0 0 1 1 1 1 1 1 0 0	0 1 0 0 1 1 1 1 1 1 1 0 0	1 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0	1 0 0 1 1 1 1 0 1 1 0 0 1 1 1	1 0 1 1 0 1 0 1 1 1 1 1 1 1 1	0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	9			

23	20	0	0	1	1	20	1	0	0	1	0	0	1	1	1			
222																		
23		+			1										1			
24					9										7			
25					1										-			
28																		
27 1 1 0 0 9 27 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0					1										-			
28 1 1 1 1 1 2 28 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1					9										5			
29 1 1 0 0 0 1 1 7 30 1 1 1 0 0 0 1 1 0 1 0 1 0 1 0 1 0 1					1										-			
30											0			0				
31					1					_								
32					7										1			
33					1							1	0	1	1			
34																		
35 0 0 0 0 8 35 0 0 1 1 1 1 0 36 36 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0					1 .					+								
36					1 8													
37 0 1 1 1 38 1 0 1 38 1 0 1 38 1 0 1 38 1 0 1 38 1 0 1 38 1 0 1 39 1 1 1 1 1 1 1 1 1			1	0	1					0								
38 1 1 1 1 1 1 40 40 0 1 1 0 0 1 1 1 1 42 1 1 1 1 42 1 1 1 1 0 1 1 43 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		0	1							1	0							
39			1		1 _					0	1							
41	39	1	1	1	j	39	1			0	1							
42	40	1	1	0	1	40	0			0	0							
43	41	1	1	1		41	1			1	0							
43 1 1 0 0 444 1 1 1 1 0 444 1 1 0 0 0 0 0	42	1	1	1] _	42	1			1	0							
45 1 0 0 0 45 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	43	1	1	0] ^D	43	0			1	1							
46 1 0 1 0	44	1		1	1		1			1								
47	45	1	0	0		45	0			1	1							
47	46	1		1			1			1								
49			0]	47				0	0							
50			0	1		48	1			1	0							
51 1 1 1 52 0	_																	
52 0 0	_																	
53																		
54																		
55																		
No. of Shifts = 2 bits No. of Shifts = 2 bits Sr. No Binary L-Shift PC2 Round Sr. No Key L5 R5 EP box XOR S Box Straigh XOR Hex.																		
No. of Shifts = 2 bits Sr. No Binary L-Shift PC2 Round Sr. No Key L5 R5 EP box XOR S Box Straigh XOR Hex.																		
Sr. No Binary L-Shift PC2 Round Sr. No Key L5 R5 EP box XOR S Box Straigh XOR Hex. 1 1 1 1 1 0 1 1 0 2 1 1 0 1 0 0 0 0 0	56	1 0	0															
Sr. No Binary L-Shift PC2 Round Sr. No Key L5 R5 EP box XOR S Box Straigh XOR Hex. 1 1 1 1 1 0 1 1 0 2 1 1 0 1 0 0 0 0 0								0.1.11										
1 1 1 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0						No. o	Shifts =	2 bits										-
1 1 1 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0	0.11	I Di	1.00.00	BOG	Bound	0.11	14.		D.F.	ED how	VOR	0.0	Ctroigh	VOR	Цох	1		-
2 1 1 0 0 0 0 0 0 0	_	+			Round										пех.			
		+			-													-
	2	1 1	1	U	ه ل	<u> 2</u>	U	U	1	0	0	0	U	Ü	1			

3	1	1	0	ا ا		3	0	0	0	1	1	1	0	0				
4	1	1	1			4	1	1	1	0	1	1	0	1				
5	1	1	1			5	1	1	1	1	0	1	0	1				
6	1	1	1			6	1	1	0	1	0	0	0	1	1			
7	1	0	1	F		7	1	1	0	1	0	0	0	1	E			
8	1	1	1			8	<u>'</u> 1	1	1	1	0	0	1	0				
9	0	0	0			9	0	0	1	0	0	0	1	1				
10	1	1	1			10	1	0	0	0	1	1	0	0				
11	0	0	1	7		11	1	1	0	1	0	1	0	1	В			
12	1	1	1			12	1	1	1	1	0	0	0	1				
13	0	0	1			13	1	1	0	1	0	1	1	0				
14	1	1	1			14	1	1	1	1	0	0	1	0				
15	0	0	1	F		15	1	0	0	0	1	0	0	0	1			
16	1	0	1			16	1	0	0	0	1	1	1	1				
17	0	0	1			17	1	1	1	1	0	1	0	1				
18	0	0	1		7	18	1	1	0	0	1	1	0	1	1 _			
19	0	1	0	С		19	0	1	0	1	1	0	0	1	E			
20	0	1	0		2	20	0	0	1	0	0	0	0	0	1			
21	1	1	1		2	21	1	1	0	1	0	0	0	1				
22	1	1	1		2	22	1	1	1	0	1	1	0	1				
23	1	1	0	D	2	23	0	0	1	0	0	0	1	1	F			
24	1	1	1		2	24	1	1	1	1	0	0	0	1				
25	1	1	1		2	25	1	0	0	0	1	0	0	0				
26	1	1	0	9	2	26	0	0	1	1	1	0	0	1 0	5			
27	1	1	0	9		27	0	0	0	0	0	0	0					
28	1	1	1		2	28	1	1	1	0	1	0	0	1				
29	0	0	1			29	0	1	0	1	0	0	1	0				
30	1	1	0	В		30	1	1	0	0	0	0	1	0	0			
31	0	0	1			31	1	1	0	1	0	0	1	0				
32	1	1	1			32	1	0	1	0	1	0	0	0				
33	0	0	1			33	1			1	0							
34	1	1	0	8		34	0			1	1							
35	0	1	0			35	0			1	1							
36	1	1	0			36	0			0	0							
37	1	1	0			37	0			1	1							
38	1	1	1	7		38	1			0	1							
39	1	1	1	•		39	1			1	0							
40	1	1	1			10	1			0	1							
41	1	1	1			11	1			1	0							
42	1	1	1	D		12	1			0	1							
43	1	0	0	_		13	0			1	1							
44	1	0	1			14	1			0	1							
45	0	0	0			1 5	0			0	0							

		_		7	- 10		1	1				1	l	l	1	1		
46	0	0	1	5	46	1	ļ		0	1								
47	0	1	0	1	47	0	ļ		1	1								
48	0	0	1		48	1			0	1								
49	1	1																
50	0	0																
51	1	1																
52	0	0																
53	1	1																
54	0	0																
55	1	0																
56	0	1																
					No. o	f Shifts =	2 bits											
Sr. No	Binary	L-Shift	PC2	Round	Sr. No	Key	L6	R6	EP box	XOR	S Box	Straigh	XOR	Hex.				
1	1	1	0		1	0	0	0	0	0	1	1	1					
2	1	1	1	1 _	2	1	1	0	0	1	1	1	0					
3	1	1	0	5	3	0	0	0	0	0	0	0	0	8				
4	1	1	1	1	4	1	1	1	0	1	0	1	0	1				
5	1	0	1		5	1	1	1	1	0	1	1	0					
6	1	1	0	1 _	6	0	0	1	1	1	0	0	0	1				
7	0	0	1	В	7	1	0	1	1	0	1	0	0	1				
8	1	1	1	1	8	1	1	0	1	0	1	0	1	1				
9	0	0	0		9	0	1	1	1	1	0	1	0					
10	1	1	1	1 _	10	1	0	0	1	0	1	0	0	1 .				
11	0	0	1	7	11	1	0	1	0	1	1	0	0	0				
12	1	1	1	1	12	1	1	1	1	0	0	1	0	1				
13	0	0	1		13	1	0	0	0	1	1	1	1					
14	1	0	1	1 _	14	1	1	0	1	0	1	1	0	1 _				
15	0	0	1	┥ F	15	1	0	0	0	1	0	1	1	В				
16	0	0	1	1	16	1	0	1	1	0	1	1	1					
17	0	1	1		17	1	1	1	1	0	0	1	0					
18	0	1	1	1 _	18	1	0	1	0	1	1	1	1					
19	1	1	0	C	19	0	0	1	1	1	0	1	1	6				
20	1	1	0	1	20	0	1	0	0	0	0	1	0					
21	1	1	1		21	1	0	1	0	1	1	0	0					
22	1	1	1	1 _	22	1	1	1	0	1	0	1	0					
23	1	1	0	D	23	0	1	1	1	1	0	0	1	3				
24	1	1	1	1	24	1	1	1	1	0	1	0	1					
25	1	1	0		25	0	0	0	1	1	0	0	0					
26	1	1	0	1 .	26	0	1	1	1	1	1	1	0					
27	1	1	0	1	27	0	0	0	1	1	1	1	1	3				
28	1	1	1	1	28	1	1	1	1	0	0	0	1					

	29	0	0	1		29	1	0	0	0	1	1	0	0				
	30	1	1	0	1	30	0	0	0	1	1	1	1	1				
	31	0	0	1	В	31	1	0	0	0	1	1	0	0	5			
	32	1	1	1	1	32	1	1	0	1	0	0	0	1				
	33	0	1	1		33	1			1	0							
	34	1	1	1	1 _	34	1			1	0							
	35	1	1	1	E	35	1			1	0							
	36	1	1	0	1	36	0			0	0							
	37	1	1	0		37	0			1	1							
	38	1	1	1	1 _	38	1			0	1							
	39	1	1	1	7	39	1			1	0							
	40	1	1	1	1	40	1			0	1							
	41	1	0	1		41	1			1	0							
	42	1	0	0	1	42	0			0	0							
	43	0	0	0	8	43	0			1	1							
	44	0	0	0	1	44	0			0	0							
	45	0	1	0		45	0			0	0							
	46	0	0	1] _	46	1			0	1							
	47	1	1	0	5	47	0			0	0							
	48	0	0	1]	48	1			0	1							
	49	1	1															
	50	0	0															
	51	1	1															
	52	0	0															
	53	1	0															
	54	0	1															
	55	0	0															
	56	1	1															
						No. o	f Shifts =	2 bits										
											V05			V05			-	
	Sr. No		L-Shift	PC2	Round	Sr. No	Key	L7	R7	EP box	XOR		Straigh		Hex.			
	1	1	1	0	1	1	0	0	1	1	1	1	1	1			-	
	2	1	1	1	5	2	1	0	0	1	0	0	1	1	E		-	
	3	1	0	0	1	3	0	0	0	0	0	0	1	1			-	
	4	1	1	1		4	1	1	0	0	1	0	1	0			-	
	5	0	0	1	1	5	1	1	0	0	1	1	0	1			-	
	6	1	1	0	9	6	0	1	0	0	0	0	1	0	В		-	
	7	0	0	0	1	7	0	1	0	0	0	1	0	1			-	
	8	1	1	1		8	1	0	1	0	1	1	1	1			-	
	9	0	0	11	1	9	1	1	0	0	1	0	1	0			-	
-	10	1	1	1	F	10	1	0	0	0	1	1	0	1	7		-	
	11	0	0	1]	11	1	1	U	1	0	T	U	T				

12	1	0	1	i	12	,	1	1	0	0	1	1	0	1				
13	0	0	1		13		1	0	1	1	0	0	1	1				
14	0	0	1	İ	14		1	0	0	0	1	1	0	0	1			
15	0	1	0	D	15		0	0	1	0	0	1	1	1	A			
16	0	1	1		16		1	1	1	0	1	1	1	0	1			
17	1	1	1		17		1	1	0	0	1	1	0	1				
18	1	1	1	İ	18		1	1	1	1	0	0	1	0	1			
19	1	1	1	E	19		1	1	1	0	1	0	1	0	9			
20	1	1	0	İ	20		0	0	0	1	1	1	1	1	1			
21	1	1	1		21		1	1	0	0	1	1	0	1				
22	1	1	1	i _	22		1	1	0	1	0	0	1	0	_			
23	1	1	0	D	23		0	1	1	1	1	0	0	1	В			
24	1	1	1	1	24		1	1	1	0	1	1	0	1				
25	1	1	0		25		0	0	0	1	1	1	0	0				
26	1	1	1	۱ ـ	26	;	1	1	0	0	1	0	0	1	1 _			
27	1	1	1	7	27	,	1	0	1	1	0	1	0	0	- 5			
28	1	1	1	İ	28	3	1	1	1	1	0	0	0	1				
29	0	0	1		29)	1	0	0	0	1	0	0	0				
30	1	1	0	1	30)	0	0	1	0	0	0	1 0	0	5			
31	0	1	1	A	31		1	0	0	0	1	1	0	0] 3			
32	1	1	0		32		0	0	1	0	0	0	1	1				
33	1	1	0		33		0			0	0							
34	1	1	1	6	34		1			1	0							
35	1	1	1		35		1			1	0							
36	1	1	0		36		0			0	0							
37	1	1	0		37		0			1	1							
38	1	1	1	5	38		1			0	1							
39	1	0	0]	39		0			0	0							
40	1	0	1		40		1			1	0							
41	0	0	1	ļ	41		1			1	0							
42	0	0	0	8	42		0			0	0							
43	0	1	0		43		0			1	1							
44	0	0	0		44		0			0	0							
45	1	1	0		45		0			1	1							
46	0	0	1	5	46		1			0	1							
47	1	1	0	ļ -	47		0			1	1							
48	0	0	1		48	5	1			1	0							
49	1	1																
50	0	0																
51	1	0																
52	0	1																
53	0	0																
54	1	1																

55	0	0														П
56	1	1														
		ı			No. o	f Shifts =	= 1 bit									
Sr. No	Binary	L-Shift	PC2	Round	Sr. No	Key	L8	R8	EP box	XOR	S Box	Straigh	XOR	Hex.		_
1	1	1	1		1	1	1	1	1	0	1	0	1			_
2	1	0	1	1	2	1	0	1	1	0	1	0	0			_
3	0	1	0	D	3	0	0	1	1	1	1	1	1	A		_
4	1	0	1	1	4	1	0	0	1	0	1	0	0			
5	0	1	1		5	1	0	1	0	1	1	1	1			_
6	1	0	1	F	6	1	0	0	1	0	1	1	1			
7	0	1	1] 「	7	1	0	1	0	1	0	0	0	С		
8	1	0	1		8	1	1	1	1	0	1	1	0			
9	0	1	1		9	1	0	0	0	1	1	1	1			
10	1	0	0	A	10	0	0	1	1	1	1	1	1	F		
11	0	0	1	」 ′`	11	1	0	1	1	0	1	1	1	'		
12	0	0	0		12	0	0	1	0	0	1	1	1			_
13	0	0	1	1	13	1	1	1	1	0	0	1	0			_
14	0	1	1	l c	14	1	0	0	0	1	1	0	0	2		_
15	1	1	0	4	15	0	1	1	1	1	1	0	1			_
16	1	1	0		16	0	1	0	1	1	0	1	0			_
17	1	1	1	4	17 18	0	0	1	1	0	1	1	1			_
18 19	1	1	0 1	В	19	1	1	0	1	0	0	1	0	9		-
20	1	1	1	1	20	1	0	1	1	0	1	1	1			-
21	1	1	1		21	1	0	1	0	1	0	0	0			-
22	1	1	1	1	22	1	0	0	1	0	0	0	0			-
23	1	1	0	C	23	0	1	1	0	0	1	1	0	0		_
24	1	1	0	1	24	0	1	1	1	1	1	1	0			-
25	1	1	0		25	0	0	0	0	0	0	0	0			-
26	1	1	0	1	26	0	0	1	1	1	1	0	0			_
27	1	1	1	3	27	1	1	0	0	1	0	1	0	0		
28	1	1	1	1	28	1	1	1	0	1	0	1	0			
29	0	1	0		29	0	0	0	1	1	1	0	0			
30	1	1	1	6	30	1	1	1	1	0	1	1	0	3		
31	1	1	1] "	31	1	0	0	1	0	0	1	1	3		
32	1	1	0		32	0	1	1	1	1	0	0	1			
33	1	1	1		33	1			0	1						_
34	1	1	0	В	34	0			1	1						
35	1	1	1	ຸ ່	35	1			1	0						
36	1	1	1		36	1			0	1						
37	1	1	1	1	37	1			1	0						

39 0 0 0 0 0 8					7									1		
39 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	38	1	0	0	۾ ا		38	0			0	0				
41	39	0	0	0	_ °		39	0			1	1				
42	40	0	0	0			40	0			0	0				
43	41	0	0	1			41	1			1	0				
43 1 0 1 1	42	0	1	1] _		42	1			0	1				
46	43	1	0	1	1 -		43	1			1	0				
46	44	0	1	1	1		44	1			0	1				
47	45	1	0	0			45	0			1	1				
47	46	0	1	1	1 _		46	1			0	1				
48	47	1	0	1	7		47	1			1	0				
49	48	0	1	1	1		48	1			1					
Signature Sign	49	1	0													
State Stat		0	0													
Standard Standard																
Signary C-Shift PC2 Round																
State Stat																
St. No Shifts = 2 bits St. No Shifts S																
No. of Shifts = 2 bits No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No. of Shifts No																
No. of Shifts = 2 bits In. No Binary L-Shift PC2 Round						_										
Sr. No Binary L-Shift PC2 Round Sr. No Key L9 R9 EP box XOR S Box Straigh XOR Hex.		,									-					
Sr. No Binary L-Shift PC2 Round Sr. No Key L9 R9 EP box XOR S Box Straigh XOR Hex.	30															
1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 1 0	30						No of	Chifte -	2 hite							
1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 1 0	30						No. of	Shifts =	2 bits							
2 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0		Rinany	L-Shift	PC2	Round					Pa	FP hox	XOR	S Box	Straigh	XOR	Hex
3 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0	Sr. No				Round		Sr. No	Key	L9		_					Hex.
4 0 0 1 0	Sr. No	1	1	1	Round		Sr. No	Key 1	L9 1	1	1	0	0	0	1	
5 1 1 1 1 0 1 0 1 0 1 0	Sr. No 1 2	1 0	1	1			Sr. No 1 2	Key 1	L9 1	1 0	1	0	0	0 1	1	
6 0 0 1 1 1 1 0	Sr. No 1 2 3	1 0 1	1 0 1	1 1 0			Sr. No 1 2 3	Key 1 1 0	L9 1 1	1 0 1	1 1 0	0 0 0	0 1 0	0 1 1	1 0 0	
7 1 1 1 1 0 0 1 1 1 0	Sr. No 1 2 3 4	1 0 1 0	1 0 1 0	1 1 0			Sr. No 1 2 3 4	1 1 0	L9 1 1 1 0	1 0 1 0	1 1 0 1	0 0 0	0 1 0 0	0 1 1 0	1 0 0 0	
8 0 0 0 1 0 1 1 0 1 0	Sr. No 1 2 3 4 5	1 0 1 0	1 0 1 0	1 1 0 1	D		Sr. No 1 2 3 4 5	Key 1 1 0 1 1	L9 1 1 1 0	1 0 1 0	1 1 0 1 0	0 0 0 0	0 1 0 0	0 1 1 0	1 0 0 0	
9 1 0 1 0	Sr. No 1 2 3 4 5	1 0 1 0 1 0	1 0 1 0 1	1 1 0 1 1	D		5r. No 1 2 3 4 5	Key 1 1 0 1 1 1	L9 1 1 1 0 1	1 0 1 0 1	1 0 1 0 1	0 0 0 0 1	0 1 0 0 0	0 1 1 0 1 0	1 0 0 0 0	8
10 0 0 0 0 1 1 0 0 1 1 0	Sr. No 1 2 3 4 5 6 7	1 0 1 0 1 0	1 0 1 0 1 0	1 0 1 1 1 1	D		Sr. No 1 2 3 4 5 6 7	Key 1 1 0 1 1 1 1 1 1	L9 1 1 1 0 1 0	1 0 1 0 1 1 1	1 1 0 1 0 1	0 0 0 0 1	0 1 0 0 0 1	0 1 1 0 1 0	1 0 0 0 0 0	8
11 0 0 1 0 1 0 1 0 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0	Sr. No 1 2 3 4 5 6 7 8	1 0 1 0 1 0 1	1 0 1 0 1 0 1	1 0 1 1 1 1 1 0	D		Sr. No 1 2 3 4 5 6 7	Key 1 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0	L9 1 1 1 0 1 0 1	1 0 1 0 1 1 1 0	1 1 0 1 0 1	0 0 0 0 1 0	0 1 0 0 0 1 1	0 1 1 0 1 0 1	1 0 0 0 0 0 0	8
12 0 1 0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 </td <td>Sr. No 1 2 3 4 5 6 7 8 9</td> <td>1 0 1 0 1 0 1 0</td> <td>1 0 1 0 1 0 1 0</td> <td>1 0 1 1 1 1 1 0</td> <td>D</td> <td></td> <td>Sr. No 1 2 3 4 5 6 7 8 9</td> <td>Key 1 1 0 1 1 1 0 1 1 1 1 1 1</td> <td>L9 1 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0</td> <td>1 0 1 0 1 1 1 0 0</td> <td>1 1 0 1 0 1 0</td> <td>0 0 0 0 1 0 1 1</td> <td>0 1 0 0 0 1 1 1 0</td> <td>0 1 1 0 1 0 1 1 1</td> <td>1 0 0 0 0 0 0 0</td> <td>8</td>	Sr. No 1 2 3 4 5 6 7 8 9	1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0	1 0 1 1 1 1 1 0	D		Sr. No 1 2 3 4 5 6 7 8 9	Key 1 1 0 1 1 1 0 1 1 1 1 1 1	L9 1 1 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0	1 0 1 0 1 1 1 0 0	1 1 0 1 0 1 0	0 0 0 0 1 0 1 1	0 1 0 0 0 1 1 1 0	0 1 1 0 1 0 1 1 1	1 0 0 0 0 0 0 0	8
13 0 1 1 14 1 1 1 0 0 1 1 0 0 0 15 1 1 1 1 0 0 0 0 0 0 0 0 16 1 1 0 0 0 0 1 1 0 1 1 0	Sr. No 1 2 3 4 5 6 7 8 9 10	1 0 1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0 0	1 0 1 1 1 1 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10	Key 1 1 0 1 1 1 1 0 1 1 0 1 0 0 0 0 0 0	L9 1 1 1 0 1 0 1 1 0 1 1 1 1 1 1 1 1 1 1	1 0 1 0 1 1 1 0 0	1 0 1 0 1 0 1 0	0 0 0 0 1 0 1 1 0	0 1 0 0 0 1 1 1 0	0 1 1 0 1 0 1 1 0	1 0 0 0 0 0 0 0 0	0
14 1 1 1 1 1 0 </td <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11</td> <td>1 0 1 0 1 0 1 0 1 0</td> <td>1 0 1 0 1 0 1 0 0 0 0 0</td> <td>1 0 1 1 1 1 1 0 1 0</td> <td>D E</td> <td></td> <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11</td> <td>Key 1 1 0 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1</td> <td>L9 1 1 1 0 1 0 1 1 0 1 1</td> <td>1 0 1 0 1 1 1 0 0 1 1 1 1 0</td> <td>1 0 1 0 1 0 1 0 1 0</td> <td>0 0 0 0 1 0 1 1 0 0</td> <td>0 1 0 0 0 1 1 1 0 0</td> <td>0 1 1 0 1 0 1 1 0 1 1</td> <td>1 0 0 0 0 0 0 0 0</td> <td>0</td>	Sr. No 1 2 3 4 5 6 7 8 9 10 11	1 0 1 0 1 0 1 0 1 0	1 0 1 0 1 0 1 0 0 0 0 0	1 0 1 1 1 1 1 0 1 0	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11	Key 1 1 0 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1	L9 1 1 1 0 1 0 1 1 0 1 1	1 0 1 0 1 1 1 0 0 1 1 1 1 0	1 0 1 0 1 0 1 0 1 0	0 0 0 0 1 0 1 1 0 0	0 1 0 0 0 1 1 1 0 0	0 1 1 0 1 0 1 1 0 1 1	1 0 0 0 0 0 0 0 0	0
15	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12	1 0 1 0 1 0 1 0 1 0 1 0 0	1 0 1 0 1 0 1 0 0 0 0 0	1 0 1 1 1 1 1 0 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12	Key 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 0 0 0	L9 1 1 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 1 0 1 1 1 0 0 0 1 1 1 1	1 0 1 0 1 0 1 0 1 0 1	0 0 0 0 1 0 1 1 0 0 1 1	0 1 0 0 0 1 1 1 0 0 0	0 1 1 0 1 0 1 1 0 1 1 0	1 0 0 0 0 0 0 0 0 0	0
15 1 1 1 1 1 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 </td <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13</td> <td>1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0</td> <td>1 0 1 0 1 0 1 0 0 0 0 0 0</td> <td>1 0 1 1 1 1 0 1 0 1 0 1</td> <td>D E</td> <td></td> <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13</td> <td>Key 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 1 1 1 0 1</td> <td>L9 1 1 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1</td> <td>1 0 1 0 1 1 1 0 0 0 1 1 1 1 0</td> <td>1 0 1 0 1 0 1 0 1 1 0 0 1</td> <td>0 0 0 0 1 0 1 1 0 0 1 1 1 0</td> <td>0 1 0 0 0 1 1 1 0 0 1 0</td> <td>0 1 1 0 1 0 1 1 0 1 1 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0</td> <td>0</td>	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 0 1 0 1 0 0 0 0 0 0	1 0 1 1 1 1 0 1 0 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Key 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 1 1 1 0 1	L9 1 1 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1	1 0 1 0 1 1 1 0 0 0 1 1 1 1 0	1 0 1 0 1 0 1 0 1 1 0 0 1	0 0 0 0 1 0 1 1 0 0 1 1 1 0	0 1 0 0 0 1 1 1 0 0 1 0	0 1 1 0 1 0 1 1 0 1 1 1 0	1 0 0 0 0 0 0 0 0 0 0	0
17 1 1 1 1 1 1 0 1 1 0 </td <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14</td> <td>1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0</td> <td>1 0 1 0 1 0 1 0 0 0 0 0 0</td> <td>1 0 1 1 1 1 0 1 0 1 0 1</td> <td>D E</td> <td></td> <td>Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14</td> <td>Key 1 1 0 1 1 1 1 0 1 1 1 0 1 1 1 1 1 1 1</td> <td>L9 1 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 0 0 0</td> <td>1 0 1 0 1 1 0 0 0 1 1 1 1 0 0 0</td> <td>1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 0 1 0 0 1</td> <td>0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 1 0</td> <td>0 1 0 0 0 1 1 1 0 0 0 1 0</td> <td>0 1 1 0 1 0 1 1 1 0 1 1 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0 0</td> <td>0</td>	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0	1 0 1 0 1 0 1 0 0 0 0 0 0	1 0 1 1 1 1 0 1 0 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14	Key 1 1 0 1 1 1 1 0 1 1 1 0 1 1 1 1 1 1 1	L9 1 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 0 0 0	1 0 1 0 1 1 0 0 0 1 1 1 1 0 0 0	1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 0 1 0 0 1	0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 1 0	0 1 0 0 0 1 1 1 0 0 0 1 0	0 1 1 0 1 0 1 1 1 0 1 1 1 0	1 0 0 0 0 0 0 0 0 0 0 0	0
18 1 1 0 19 1 1 1 18 0 0 0 0 0 0 19 1 0 0 1 0 0 1 18 0 0 0 0 0 0 0 19 1 0 0 1 0 0 1 1	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0	1 0 1 0 1 0 1 0 0 0 0 0 1 1 1 1	1 0 1 1 1 1 0 1 0 1 0 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Key 1 1 0 1 1 1 1 0 1 1 1 0 1 1 1 1 1 1 1	L9 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 1 1	1 0 1 0 1 1 0 0 0 1 1 1 1 0 0 0 1 1 1 1	1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 0 1 0 0 1 0 0 1 0 0 0 0 0 1	0 0 0 0 1 1 0 1 1 1 0 0 0 1 1 1 1 0 0	0 1 0 0 0 1 1 0 0 1 0 0 1	0 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 0 1	1 0 0 0 0 0 0 0 0 0 0 0	0
19 1 1 1 1 B 19 1 0 0 1 0 0 1 1 3	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0	1 0 1 0 1 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1	1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Key 1 1 0 1 1 1 1 0 1 1 0 1 1 1 0 1 0 1 1 0 0 1 1 0 0 0 1 0	L9 1 1 1 0 1 0 1 1 1 0 1 1 0 1 1 1 0 1 0	1 0 1 0 1 1 0 0 0 1 1 1 1 0 0 0 1 1 1 1	1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1	0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 1 0 0	0 1 0 0 0 1 1 0 0 1 0 0 1 0	0 1 1 0 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 0 1 0 0 1 1	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
19 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 1 1 0	1 0 1 0 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1	1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Key 1 1 0 1 1 1 0 1 1 1 0 1 1	L9 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 1 1	1 0 1 0 1 1 0 0 0 1 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0 0 0 1 1 0 0 0 1	1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 1	0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 1 0 0 1 1 1 0 0 1 1 0 0 0 1 1 0	0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 1 0	0 1 1 0 1 0 1 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 0 0 0 0 1	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0
20 1 1 1 20 1 1 1 0 1 1 0 1	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 1 1 1 0	1 0 1 0 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1	1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	Key 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 1 1	L9 1 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 0 1 0 1 0 0 1 0 0 1 0	1 0 1 0 1 1 0 0 0 1 1 1 1 1 0 0 0 1 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0	1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 0 1 0 1	0 0 0 0 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0	0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0	0 1 1 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 0 0 1 1 0 0 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0
	Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19	1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 1 1 1 1 0 0 1 1 0	1 0 1 0 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1	1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 0 1 1 1 0 1 1 1 1 0 1 1 1 0 1	D E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19	Key 1 1 0 1 1 1 0 1 1 0 1 0 1 0 1 0 1 1	L9 1 1 1 0 1 0 1 1 1 0 1 1 0 1 1 1 0 1 0	1 0 1 1 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 1 1 1 0 0 0 1 1 0	1 0 1 0 1 0 1 1 0 0 1 0 1 1 0 1 0 1 0 1	0 0 0 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 0 1 0	0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0	0 1 1 0 1 0 1 1 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 0 0 1 1 1 1 0 0 1 1	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0

22	21	1	1	1		21	1	1	0	0	1	0	0	1				T
23					†													
24					E										F			 _
25					1													 -
28																		-
27					1										1			
28					2								0	0	0			
29					1													 -
30			-							_								 -
31					†													
32					7									0	С			+
33 1 1 1 0 A 33 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0					†													+
34																		+
35					†													
36 1 0 0 0 37 1 0 1 38 1 0 0 1 38 1 0 0 1 38 1 0 0 1 38 1 0 0 1 38 1 0 0 1 38 1 0 0 1 38 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0					A													
37					†													
38																		
39					1													
40					† P						0							
41				1	1					0								
42		0	0															
43	42	1	1	1	1 _		1			0	1							
45		0	0		1 -					0	1							
46	44	1	1	1	1	44	1			0	1							
47	45	0	0	0		45	0			0	0							
47 0 0 1 48 1 1 0 1 48 1 1 0 1 48 1 1 0 1 48 1 1 0 1 48 1 1 0 1 48 1 1 0 1 48 1 1 0 1 1 1 1 1 1 1	46	1	1	0	1	46	0			1	1							
49	47	0	0	1	3	47	1			1	0							
Sr. No Binary L-Shift PC2 Round Sr. No Key L10 R10 EP box XOR S Box Straigh XOR Hex.	48	1	0	1	1	48	1			1	0							
51 1	49	0	1															
52		0	0															
53		1	1															
54 0 0		0	0															
Sr. No Binary L-Shift PC2 Round Sr. No Key L10 R10 EP box XOR S Box Straigh XOR Hex.																		
No. of Shifts = 2 bits No. of Shifts = 2 bits No. of Shifts = 2 bits																		
No. of Shifts = 2 bits No. of Shifts = 2 bits																		
Sr. No Binary L-Shift PC2 Round Sr. No Key L10 R10 EP box XOR S Box Straigh XOR Hex. 1 1 1 1 1 1 0 1 0 0 1 2 0 0 1 0 0 1	56	0	1															
Sr. No Binary L-Shift PC2 Round Sr. No Key L10 R10 EP box XOR S Box Straigh XOR Hex. 1 1 1 1 1 1 0 1 0 0 1 2 0 0 1 0 0 1																		
1 1 1 1 1 1 1 0 1 0 0 1 0 1 1 1 1 1 1 1						No. of	Shifts =	2 bits										
1 1 1 1 1 1 1 1 0 1 0 0 1 1 1 1 1 1 1 1	Sr. No	Binary	L-Shift	PC2	Round	Sr. No	Key	L10	R10	EP box	XOR	S Box	Straigh	XOR	Hex.	Ī		
					1			1		0	1							
	2	0	0	1	1 _	2	1	0	0	1	0	1	1	1				
3 1 1 1 3 1 1 0 0 1 1 1 0	3	1	1	1	F	3	1	1	0	0	1	1	1	0	U			

4	0	0	1	İ		4	1	0	0	0	1	1	1	1				
5	1	1	1			5	1	1	0	0	1	1	1	0				
6	0	0	1			6	1	1	0	0	1	1	1	0	1			
7	1	0	1	E		7	1	0	0	0	1	1	1	1	2			
8	0	0	0			8	0	0	0	0	0	1	0	0	1			
9	0	0	1			9	1	1	0	0	1	1	0	1				
10	0	1	0	_		10	0	1	0	0	0	0	0	1	1 _			
11	0	1	1	В		11	1	1	0	0	1	1	1	0	D			
12	1	1	1			12	1	1	0	0	1	1	0	1	1			
13	1	1	1			13	1	0	1	0	1	1	1	1				
14	1	1	1	_		14	1	0	0	0	1	0	1	1] _			
15	1	1	1	E		15	1	1	0	0	1	0	1	0	С			
16	1	1	0			16	0	0	1	0	0	0	0	0				
17	1	1	0			17	0	1	0	0	0	0	1	0				
18	1	1	0	2		18	0	0	0	1	1	1	1	1	- 5			
19	1	1	1	_		19	1	0	1	0	1	1	0	0]			
20	1	1	0			20	0	1	1	1	1	1	0	1				
21	1	1	1			21	1	0	1	0	1	1	1	1				
22	1	1	1	E		22	1	0	1	0	1	0	0	0	В			
23	1	1	1	_		23	1	0	1	1	0	1	1	1				
24	1	1	0			24	0	0	1	0	0	0	1	1				
25	1	1	0			25	0	0	0	1	1	1	1	1				
26	1	0	0	2		26	0	0	0	0	0	0	1	1	F			
27	1	1	1	_		27	1	0	0	0	1	0	1	1				
28	0	0	0			28	0	0	0	1	1	1	1	1				
29	1	1	1			29	1	0	1	1	0	1	0	0	-			
30	1	1	1	F		30	1	0	1	1	0	1	1	0	4			
31	1	1	1			31	1	1	0	1	0	1		0	-			
32	1	1	1			32	1	1	0	1	0	1	1	U				
33	1	1	1			33 34	1			1	0							
34 35	1	0	0 1	Α		35	0			1	1							
36	0	0	0			36	0			0	0		-		-			
37	0	0	1			37	1			1	0							
38	0	1	1			38	1			0	1							
39	0	0	0	D		39	0			0	0							
40	1	1	1			40	1			0	1							
41	0	0	0			41	0			0	0				+			
42	1	1	1			42	1			1	0							
43	0	0	0	5		43	0			0	0							
44	1	1	1			44	1			1	0							
45	0	0	0			45	0			1	1							
46	1	0	0			46	0			0	0							
				1 3		. •				Ţ								

47	0	1	1	٦٥		47	1			0	1							Т
48	0	0	1	1		48	1			1	0							
49	1	1																
50	0	0																
51	1	1																Т
52	0	0																Т
53	1	1																Т
54	0	1																
55	1	1																
56	1	1																
																		L
				1		No. of	Shifts =	2 bits		I		1						L
Sr. No	Rinany	L-Shift	PC2	Round		Sr. No	Key	L11	R11	EP box	XOR	S Box	Straigh	XOR	Hex.	Ī		H
1	1	1	1	Round		31. NO	1	1	1	0	1	0	1	0	TIOX.			H
2	0	0	1	†		2	1	0	1	1	0	1	0	0				+
3	1	1	1	E		3	1	0	0	1	0	0	0	0	1			t
4	0	0	0	†		4	0	0	1	0	0	0	1	1				t
5	1	0	1	<u> </u>		5	1	0	0	1	0	0	1	1				t
6	0	0	0	1 .		6	0	0	0	0	0	1	0	0				T
7	0	0	1	A		7	1	0	1	1	0	0	0	0	9			T
8	0	1	0	1		8	0	0	0	0	0	0	1	1				T
9	0	1	1			9	1	0	1	0	1	0	0	0				T
10	1	1	0	1 .		10	0	0	1	1	1	1	0	0				T
11	1	1	1	В		11	1	0	0	0	1	1	0	0	1			Т
12	1	1	1	1		12	1	0	1	1	0	0	1	1				Г
13	1	1	1			13	1	1	1	0	1	0	0	1				Г
14	1	1	1	E		14	1	0	1	1	0	1	0	0				Г
15	1	1	1] -		15	1	0	0	1	0	0	1	1	Α			
16	1	1	0			16	0	1	0	0	0	1	1	0				
17	1	1	0			17	0	0	0	1	1	1	1	1				Ĺ
18	1	1	1	6		18	1	0	1	1	0	0	0	0	Α			L
19	1	1	1	」		19	1	1	0	1	0	0	0	1	^			L
20	1	1	0			20	0	1	1	1	1	0	1	0				L
21	1	1	1	1		21	1	1	1	1	0	1	1	0				L
22	1	1	1	E		22	1	1	0	0	1	1	0	1	7			L
23	1	1	1	↓ ¯		23	1	1	1	0	1	0	0	1				L
24	1	0	0			24	0	1	1	0	0	0	0	1				L
25	1	1	0	1		25	0	0	1	0	0	0	0	0				L
26	0	0	1	6		26	1	0	1	0	1	1	0	0	1			L
27	1	1	1	↓		27	1	0	1	1	0	0	0	0				1
28 29	0	0	0	1		28	0	0	1	0	0	0	1	1				1
	1 1	1	1	1	1	29	1	1	0	1	0	1 1	1 1	0		I		

31	30	n I	1	1	1	1	30	1	1	1	1	0	0	1	0			T		1	
32				1		F								0	0	0					
33						1										1		-			
34													,		U						
35						+			 	 											
36						С			+	 								-			
37						1			 			_						-	-		
38									 	 											
39		-				1				 											
40						5				 											
41				-		1			 	 											
42									 	 											
43 0 0 0 0 0 1 44 1 1 0 1 1 1 45 0 1 1 1 45 0 1 1 45 0 1 1 1 45 0 1 1 1 1 1 1 1 1 1						†					+							+			
44						5											1				
45						1			\vdash									+			
46									\vdash												
47						†												+			
48						6	_					_						1			
49						1	_		+									1			
Sr. No Binary L-Shift PC2 Round							1.4	-	-		-							+			
St. No Binary L-Shift PC2 Round																					
Sr. No Binary L-Shift PC2 Round Sr. No Key L12 R12 EP box XOR S Box Straigh XOR Hex.																					
Sr. No Binary L-Shift PC2 Round																					
St. No Binary L-Shift PC2 Round																					
Sr. No Binary L-Shift PC2 Round Sr. No Key L12 R12 EP box XOR S Box Straigh XOR Hex.		-	1	1																	
Sr. No Binary L-Shift PC2 Round Sr. No Key L12 R12 EP box XOR S Box Straigh XOR Hex.		-	1	1																	
No. of Shifts = 2 bits No. of Shifts = 2 bits Sr. No Key L12 R12 EP box XOR S Box Straigh XOR Hex.			1	1																	
Sr. No Binary L-Shift PC2 Round Sr. No Key L12 R12 EP box XOR S Box Straigh XOR Hex.																					
1 1 1 1 1 1 1 2 2 0 0 0 1 1 2 2 1 1 1 0 0 0 1 1 0 1 0							No. of	Shifts =	2 bits												
1 1 1 1 1 1 1 2 2 0 0 0 1 1 2 2 1 1 1 0 0 0 1 1 0 1 0																					
2 0 0 1 0 1 0 1 0 1 0 0 1 0 0 0 0 1 0	Sr.	No	Binary	L-Shift	PC2	Round	Sr. No	Key	L12	R12	EP box	XOR	S Box	Straigh	XOR	Hex.					
3 1 0 1 4 0 0 0 0 1 4 0 1 1 0 0 0 0 1 1 0 0 0 1 0 1	1	1	1	1	1		1	1	1	0	0	1	1	1	0						
3 1 0 1 1 0 0 0 1 1 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0	2	2	0	0	1		2	1	1	0	0	1	0	1	0						
5 0 0 1 6 0 1 0 1 1 0 0 7 0 1 0 <td>3</td> <td>3</td> <td>1</td> <td>0</td> <td>1</td> <td></td> <td>3</td> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>1</td> <td>1</td> <td>0</td> <td>0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	3	3	1	0	1		3	1	0	0	0	1	1	0	0						
6 0 1 0 0 1 1 1 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 <td>4</td> <td>4</td> <td>0</td> <td>0</td> <td>0</td> <td></td> <td>4</td> <td>0</td> <td>1</td> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td></td> <td>0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	4	4	0	0	0		4	0	1	1	0	0	0		0						
7 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0	5	5	0	0	1		5	1	0	1		0	1	0	0						
7 0 1 0 1 0 8 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 0 1	6	6	0	1	0		6	0	0	0	1	1	1								
8 1 1 0 8 0 0 1 1 1 0 1 1 9 1 1 1 1 0 0 1 0 1 0 1 0 0 1 0 0 1 0 <td>7</td> <td>7</td> <td>0</td> <td>1</td> <td>0</td> <td>ľ</td> <td>7</td> <td>0</td> <td>1</td> <td>0</td> <td>1</td> <td>1</td> <td>1</td> <td>0</td> <td>1</td> <td>,</td> <td></td> <td></td> <td></td> <td></td> <td></td>	7	7	0	1	0	ľ	7	0	1	0	1	1	1	0	1	,					
10 1 1 1 F 10 1 1 0 0 1 1 0 0 1 1 1 1 0 1 1 1 1	8	8	1	1	0	<u> </u>	8	0		1			0	1	1						
10 1 1 1 F 10 1 1 0 0 1 1 0 0 1 1 1 1 0 1 1 1 1	9	9	1	1	1		9	1	1	0	0	1	0	1	0						
	10	0	1	1		_ [10	1	1	0			1	1	0	4					
12 1 1 1 1 1 1 0 1 0 0 1													_		_		1				
			1	1	11			1	0	0		0	0	0	0						

13	1	1	1			13	1	1	1	1	0	1	1	0				
14	1	1	1	ł		14	1	1	0	0	1	1	1	0	1			
15	1	1	1	E		15	1	0	1	0	1	1	1	1	3			
16	1	1	0	l		16	0	0	0	0	0	1	1	1	1			
17	1	1	0			17	0	0	1	1	1	1	0	0				
18	1	1	1	l		18	1	1	0	1	0	1	0	1	1			
19	1	1	1	7		19	1	0	1	1	0	0	1	1	6			
20	1	1	1			20	1	1	0	1	0	0	1	0	1			
21	1	1	1			21	1	1	0	0	1	1	0	1				
22	1	0	1	İ		22	1	0	1	1	0	1	0	0				
23	1	1	1	E		23	1	1	1	0	1	0	1	0	9			
24	0	0	0	İ		24	0	1	1	1	1	1	0	1				
25	1	1	0			25	0	1	0	0	0	0	0	1				
26	0	0	1			26	1	1	0	1	0	0	1	0				
27	1	1	0	4		27	0	1	0	0	0	0	0	1	Α			
28	0	0	0	1		28	0	1	1	1	1	0	1	0				
29	1	1	1			29	1	0	0	0	1	0	1	1				
30	1	0	1			30	1	1	0	0	1	0	0	1] _			
31	1	0	0	D		31	0	0	0	0	0	1	0	0	С			
32	0	0	1			32	1	0	0	0	1	0	0	0				
33	0	0	1			33	1			1	0							
34	0	1	1	С		34	1			1	0							
35	0	0	0			35	0			1	1							
36	1	1	0			36	0			0	0							
37	0	0	0	[37	0			1	1							
38	1	1	1	5		38	1			0	1							
39	0	0	0]		39	0			0	0							
40	1	1	1			40	1			0	1							
41	0	0	1			41	1			1	0							
42	1	0	1	С		42	1			0	1							
43	0	1	0	ļ		43	0			1	1							
44	0	0	0			44	0			0	0							
45	1	1	1			45	1			0	1							
46	0	0	1	E		46	1			0	1							
47	1	1	1			47	1			0	1							
48	0	0	0			48	0			0	0							
49	1	1																
50	0	1																
51	1	1																
52	1	1																
53	1	1																
54	1	1																
55	1	1		<u> </u>														

56	1	1														I
																 +
				1	No. 01	Shifts =	2 bits		1		1					 +
Sr No	Binary	I -Shift	PC2	Round	Sr. No	Key	L13	R13	EP box	XOR	S Box	Straigh	XOR	Hex.		 +
1	1	0	1		1	1	0	0	0	1	1	0	0			 +
2	0	0	1	1 _	2	1	0	0	0	1	0	1	1			T
3	0	0	1	d E	3	1	0	0	0	1	1	1	1	6		T
4	0	1	0	1	4	0	1	0	0	0	0	1	0			T
5	0	1	0		5	0	1	0	0	0	1	0	1			
6	1	1	1	4	6	1	0	0	0	1	1	1	1	E		
7	1	1	0]	7	0	0	1	0	0	1	1	1	_		
8	1	1	0		8	0	1	1	0	0	1	1	0			
9	1	1	1	1	9	1	0	0	0	1	0	1	1			
10	1	1	1	l F	10	1	0	0	1	0	0	0	0	A		
11	1	1	1	1 '	11	1	0	0	1	0	0	1	1			 1
12	1	1	1		12	1	1	1	0	1	1	1	0			
13	1	1	1	1	13	1	1	0	1	0	0	1	0			_
14	1	1	1	l F	14	1	0	0	0	1	1	0	0	0		4
15	1	1	1	ļ '	15	1	1	1	0	1	0	1	0			4
16	1	1	1		16	1	0	1	0	1	0	0	0			 4
17	1	1	0	4	17	0	1	0	1	1	1	0	1	_		 +
18	1	1	1	7	18	1	0	1	0	1	0	1	1	D		 +
19	1	1	1	4	19	1	1	1	1	0	0	1	0			+
20	1	0	1	-	20	1	0	0	0	1	1	1	1			 +
21 22	1 0	1	0	1	21	0	0	0	0	1	0	0	0			+
23	1	0 1	1	A	23	1	1	0	1	0	1	0	0	5		+
24	0	0	0	1	24	0	1	1	0	0	1	0	1			 +
25	1	1	1	-	25	1	0	1	1	0	1	0	0			 +
26	0	0	1	1	26	1	0	0	0	1	1	0	0			 +
27	1	1	0	C	27	0	0	1	1	1	0	1	1	2		 +
28	0	0	0	1	28	0	1	0	1	1	1	1	0			 +
29	1	0	1		29	1	0	1	0	1	0	0	0			 +
30	0	0	1	1 _	30	1	0	1	1	0	1	0	0			\dagger
31	0	0	0	C	31	0	0	0	0	0	1	0	0	1		+
32	0	1	0	1	32	0	0	0	1	1	0	1	1			\dagger
33	0	0	1		33	1			0	1						+
34	1	1	1	1 .	34	1			0	1						T
35	0	0	0	D	35	0			1	1						\top
36	1	1	1	1	36	1			1	0						T
37	0	0	0		37	0			1	1						
38	1	1	1] 4	38	1			1	0						

				7 4											1			
39	0	0	0	_ ~		39	0			0	0							
40	1	0	0			40	0			1	1							
41	0	1	1			41	1			0	1							
42	0	0	1	С		42	1			1	0							
43	1	1	0			43	0			0	0							
44	0	0	0	1		44	0			1	1							
45	1	1	1			45	1			1	0							
46	0	0	1	1 _		46	1			0	1							
47	1	1	0	D		47	0			0	0							
48	0	1	1	1		48	1			0	1							
49	1	1																
50	1	1																
51	1	1																
52	1	1																
53	1	1																
54	1	1																
55	1	1																
56	1	0																
- 00																		
																1	-	
						No of	Shifts =	2 hits										
						No. of	Shifts =	2 bits				1						
Sr No	Rinary	L-Shift	PC2	Round					R14	EP box	XOR	S Box	Straigh	XOR	Hex.			
	_	L-Shift		Round		Sr. No	Key	L14	R14	EP box			Straigh		Hex.			
1	0	0	1	Round		Sr. No	Key	L14	0	1	0	0	1	1	Hex.			
1 2	0	0	1	Round		Sr. No 1 2	Key 1	L14 0 0	0	0	0	0	1 0	1 0	Hex.			
1 2 3	0 0	0 1 1	1 1 1			Sr. No 1 2 3	Key 1 1 1	L14 0 0	0 1 1	0 1	0 1 0	0 1 1	0 0	0 0				
1 2 3 4	0 0 0	0 1 1 1	1 1 1 0			Sr. No 1 2 3 4	Key 1 1 1 0	L14 0 0 0	0 1 1 0	1 0 1 1	0 1 0 1	0 1 1 0	1 0 0 0	1 0 0				
1 2 3 4 5	0 0 0 1 1	0 1 1 1	1 1 1 0			Sr. No 1 2 3 4 5	Key 1 1 1 0 0	L14 0 0 0 0	0 1 1 0	1 0 1 1 0	0 1 0 1	0 1 1 0	1 0 0 0	1 0 0 0				
1 2 3 4 5	0 0 0 1 1	0 1 1 1 1	1 1 1 0 0			Sr. No 1 2 3 4 5 6	1 1 1 0 0 0 1	L14 0 0 0 0 0 0	0 1 1 0 1	1 0 1 1 0	0 1 0 1 0	0 1 1 0 1	1 0 0 0 1	1 0 0 0 1				
1 2 3 4 5 6 7	0 0 0 1 1 1	0 1 1 1 1 1	1 1 1 0 0 1	E		Sr. No 1 2 3 4 5 6 7	Key 1 1 1 0 0 1 1 1	L14 0 0 0 0 0 0 0	0 1 1 0 1 1	1 0 1 1 0 1	0 1 0 1 0 0	0 1 1 0 1 0	1 0 0 0 1 1 0	1 0 0 0 1 0	- 8			
1 2 3 4 5 6 7 8	0 0 0 1 1 1 1	0 1 1 1 1 1 1	1 1 0 0 1 1	E		Sr. No 1 2 3 4 5 6 7 8	Key 1 1 1 0 0 1 1 1 0 0	L14 0 0 0 0 0 0 0 1	0 1 1 0 1 1 1 0	1 0 1 1 0 1	0 1 0 1 0 0 0	0 1 1 0 1 0 0	1 0 0 0 1 0 0	1 0 0 0 1 0 1 0	- 8			
1 2 3 4 5 6 7 8 9	0 0 0 1 1 1 1 1	0 1 1 1 1 1 1 1	1 1 0 0 1 1 0	E		Sr. No 1 2 3 4 5 6 7 8 9	Key 1 1 1 0 0 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 0 1 1	0 1 1 0 1 1 1 0	1 0 1 1 0 1 0	0 1 0 1 0 0 1 1 1	0 1 1 0 1 0 0 0	1 0 0 0 1 0 0 1 0	1 0 0 0 1 0 1 0	- 8			
1 2 3 4 5 6 7 8 9	0 0 0 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1	1 1 0 0 1 1 0 1	E		Sr. No 1 2 3 4 5 6 7 8 9 10	Key 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 0 1 1 0	0 1 1 0 1 1 1 0 1 0	1 0 1 1 0 1 0 1 0	0 1 0 1 0 0 1 1 0	0 1 1 0 1 0 0 0 0	1 0 0 0 1 0 0 1 0	1 0 0 0 1 0 1 0 0	- 8			
1 2 3 4 5 6 7 8 9 10	0 0 0 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 0 1 1	- E		Sr. No 1 2 3 4 5 6 7 8 9 10 11	Key 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0	0 1 1 0 1 1 1 1 0 1 0	1 0 1 1 0 1 0 1 1 0	0 1 0 1 0 0 1 1 0 0	0 1 1 0 1 0 0 0 0	1 0 0 0 1 1 0 0 1 0	1 0 0 0 1 0 1 0 0 0	8 - A			
1 2 3 4 5 6 7 8 9 10 11	0 0 0 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 0 1 1 1 1	- E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12	Key 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 1	0 1 1 0 1 1 1 1 0 1 0 1 0	1 0 1 1 0 1 0 1 1 1 0	0 1 0 1 0 0 1 1 1 0 0	0 1 1 0 1 0 0 0 0 0 1 1	1 0 0 0 1 1 0 0 1 0 0	1 0 0 0 1 0 1 0 0 0 0	8 - A			
1 2 3 4 5 6 7 8 9 10 11 12 13	0 0 0 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 0 1 1 1	- E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13	Key 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 1 1 0 0	0 1 1 0 1 1 1 1 0 1 0 1 0	1 0 1 1 0 1 0 1 1 0 1 1 0 1	0 1 0 1 0 0 1 1 1 0 0	0 1 1 0 1 0 0 0 0 0 1 1 1	1 0 0 0 1 1 0 0 1 0 0 1 1	1 0 0 0 1 0 1 0 0 0 0 1 0	8 - A			
1 2 3 4 5 6 7 8 9 10 11 12 13 14	0 0 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 0 1 1 1 1 1 1	6 - 6		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14	Key 1 1 0 0 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 0 1 0 1 0 1 0 0	1 0 1 1 0 1 0 1 1 0 1 1 0 1 1 0 1	0 1 0 1 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0	1 0 0 0 1 1 0 0 1 0 0 1 1 1 0	1 0 0 0 1 0 1 0 0 0 0 0 1 0	8 A 2			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	0 0 0 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 0 1 1 1 1 1 1	- E		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Key 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 0 1 0 1 0	0 1 0 1 0 0 1 1 1 0 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0	1 0 0 0 1 0 0 1 0 0 1 1 0 0 0 1 1 0 0	1 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1	8 - A			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 1 1 1 1 1 1	6 - 6		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	Key 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1	0 1 0 1 0 0 1 1 0 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0 0 0 1 0	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0	1 0 0 0 1 0 0 1 0 0 1 1 1 0 0 0 1 1	1 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0	8 A 2			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 1 1 1 1 1 1 1	6 - 6		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Key 1 1 0 0 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1	0 1 0 1 0 0 1 1 0 0 1 0 1 0 1 0 0 1 1 0 0 0 1 0	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0	1 0 0 0 1 0 0 1 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1	1 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1	8 A 2			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	- 6 - 6 - F		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	Key 1 1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1	0 1 0 1 0 0 1 1 0 0 1 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0 0 0 1 0	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0	1 0 0 0 1 0 0 1 0 0 1 1 1 0 0 0 1 1	1 0 0 0 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 1 0	8 A 2			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 1 1 1 1 1 1 1	6 - 6		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Key 1 1 0 0 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 1 0 1 1 0 1 1 0 1 0 1	0 1 0 1 0 0 1 1 0 0 1 0 1 0 1 0 0 1 1 0 0 0 1 0	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0	1 0 0 0 1 0 0 1 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1	1 0 0 0 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 1 0 1 0 1	8 A 2			
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	- 6 - 6 - F		Sr. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	Key 1 1 0 0 1 1 1 1 1 1 1 1 1	L14 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1 0 1 1 0 1	0 1 1 0 1 1 1 0 1 0 1 0 0 0 0 0 0 0 0 0	1 0 1 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0	0 1 0 1 0 0 1 1 0 0 1 0 1 0 0 1 0 0 1 0 0 1 0	0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0	1 0 0 0 1 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0	1 0 0 0 1 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 1 1 1 1 1 1	8 A 2			

2	22	0	0	0	1		22	0	0	1	0	0	0	0	0				
	23	1	1	1	3		23	1	0	0	0	1	1	1	1	3			
	24	0	0	1	-		24	1	1	1	1	0	0		1				
	25						25							0	0				-
		1	1	1	1			1	1	0	0	1	1	0				-	-
	26	0	0	1	С		26	1	0	0	1	0	1		0	0			-
	27	1	0	0	4		27	0	1	1	1	1	0	1	0				-
	28	0	0	0			28	0	0	0	0	0	0					-	-
	29	0	0	1	4		29	1	1	0	1	0	1	0	1				-
	30	0	1	0	A		30	0	1	0	0	0	1	0	0	9		-	-
	31	0	0	1	1		31	1	0	0	1	0	0	0					-
	32	1	1	0			32	0	0	1	0	0	1	1	1				
	33	0	0	1	1		33	1			1	0							
	34	1	1	1	D		34	1			0	1							
	35	0	0	0	ļ -		35	0			1	1							
	36	1	1	1			36	1			0	1							
	37	0	0	0	1		37	0			1	1							
	38	1	0	1	6		38	1			0	1							
	39	0	1	1]		39	1			0	1							
4	40	0	0	0			40	0			1	1							
	41	1	1	1	_		41	1			0	1							
	42	0	0	1	E		42	1			0	1							
4	43	1	1	1] -		43	1			0	1							
4	44	0	0	0			44	0			0	0							
4	45	1	1	1			45	1			0	1							
4	46	0	1	1			46	1			0	1							
4	47	1	1	0	D		47	0			1	1							
4	48	1	1	1	1		48	1			0	1							
4	49	1	1																
5	50	1	1																
5	51	1	1																
5	52	1	1																
5	53	1	1		İ														
	54	1	0																
5	55	1	0																
5	56	0	0																
							No. o	f Shifts =	1 bit										
Sr.	. No	Binary	L-Shift	PC2	Round		Sr. No	Key	L15	R15	EP box	XOR	S Box	Straigh	XOR	Hex.			
1	1	0	1	1			1	1	0	1	1	0	0	0	0				
2	2	1	1	0			2	0	1	0	1	1	1	0	1				
3	3	1	1	1	В		3	1	1	0	0	1	1	1	0	4			
4	4	1	1	1	1		4	1	0	0	0	1	1	0	0				

5	1	1	1	1		5	1	1	1	0	1	0	0	1				
6	1	1	1	1		6	1	1	0	1	0	0	0	1	1			
				E		7								1	E			
7	1	1	1	1			1	1	1	0	1	0	0	0	-			
8	1	1	0			8	0	0	0	1 0	1	0						
9	1	1	1	-		9	1	1	0			0	0	1	-			
10	1	1	1	D		10	1	0	0	1	0	1	1	1	F			
11	1	1	0			11	0	1	1	0	0	1	0	1				
12	1	1	1			12	1	0	0	0	1	0	1	1				
13	1	1	0	<u> </u>		13	0	0	1	0	0	0	0	0				
14	1	1	0	3		14	0	0	0	0	0	1	0	0	1			
15	1	1	1			15	1	0	1	0	1	1	0	0] '			
16	1	1	1			16	1	0	0	1	0	0	1	1				
17	1	0	0			17	0	1	1	0	0	0	1	0				
18	0	1	1	7		18	1	1	1	1	0	0	0	1				
19	1	0	1] ′		19	1	0	1	0	1	0	0	0	4			
20	0	1	1	1		20	1	1	0	1	0	1	1	0	1			
21	1	0	0			21	0	0	0	0	0	0	0	0				
22	0	1	1	1 _		22	1	1	0	1	0	0	1	0]			
23	1	0	1	7		23	1	0	1	0	1	0	1	1	3			
24	0	1	1	1		24	1	1	1	1	0	0	0	1				
25	1	0	0			25	0	0	0	0	0	1	0	0				
26	0	0	1	1		26	1	0	0	1	0	1	0	0				
27	0	0	1	6		27	1	1	0	1	0	1	1	0	0			
28	0	0	0	†		28	0	0	0	1	1	0	0	0	1			
29	0	1	1			29	1	0	1	0	1	0	0	0				
30	1	0	0	†		30	0	0	0	0	0	1	1	1	-			
31	0	1	0	9		31	0	0	0	0	0	0	1	1	6			
32	1	0	1	†		32	1	1	1	0	1	0	1	0	1			
33	0	1	1		_	33	1	•		0	1	V	·					
34	1	0	1	†		34	1			1	0							
35	0	1	1	F		35	1			1	0		-					
36	1	0	1	1		36	1			0	1							
37	0	0	1			37	1			1	0		-			-		
38	0	1	1	1		38	1			0	1							
39	1	0	0	С		39	0			0	0		-					
		1		1		40							-					
40	0		0				0			0	0		-					
41	1	0	0	1		41	0			0	0		-	1				
42	0	1	0	3		42	0			1	1							
43	1	0	1	1		43	1			0	1							
44	0	1	1			44	1			1	0			ļ				
45	1	1	1			45	1			0	1			ļ				
46	1	1	0	A		46	0			0	0							
47	1	1	1] ^`		47	1			1	0							

40	-1	4	_	1			48	_			1	4			1	1	1		
48	1	1	0	ļ			46	0			1	1							
49	1	1		ļ															
50	1	1																	
51	1	1																	
52	1	1																	
53	1	0																	
54	0	0																	
55	0	0																	
R16L16 -	4	Е	F	1	4	3	0	6	8	Α	2	Α	Е	3	0	9			
							IP INV	/ERSE											
				40	8	48	16	56	24	64	32								
				39	7	47	15	55	23	63	31								
				38	6	46	14	54	22	62	30								
				37	5	45	13	53	21	61	29								
				36	4	44	12	52	20	60	28								
				35	3	43	11	51	19	59	27								
				34	2	42	10	50	18	58	26								
				33	1	41	9	49	17	57	25								
						S.No	R16L16	IP Inv.	Hex.										
						1	0	0											
						2	1	0	1										
						3	0	0	1										
						4	0	1	1										
						5	1	1											
						6	1	1											
						7	1	1	E										
						8	0	0	1										
						9	1	1											
						10	1		-	-									
		-		-	-	11		1	E										
							1		-										
						12	1	0											
						13	0	1											
						14	0	1	D										
						15	0	0	_										
						16	1	1											
						17	0	0											
						18	1	1											

			4				1	I		
19	0	0								
20	0	0								
21	0	0								
22	0	0	1							
23	1	0	' '							
24	1	1								
25	0	1								
26	0	1	1 _							
27	0	1	E							
28	0	0	1							
29	0	0								
30	1	0	1							
31	1	0 1	2							
32	0	0								
33	1	0								
34	0	0	1 .							
35	0	0	1							
36	0	1								
37	1	0								
38	0	0								
39	1	0	0							
40	0	0								
41	0	0								
42	0	0	1							
43	1	1	3							
44	0	1								
45	1	1								
46	0	0	1							
47	1	0	8							
48	0	0	1							
49	1	0								
50	1	1								
51	1	0	5							
52	0	1								
53	0	1								
54	0	1	1							
55	1	0	С							
56	1	0								
	0	1								
57 58	0	0								
	0		9							
59		0								
60	0	1								
61	1	1								

						62	0	0											_
						63	0	0	8										-
						64	1	0	-										
						04	'	U											
																			_
						Ci	phertext :	- 1EED41	E210385	C98									
Char:	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F			
Compl:	F	Е	D	С	В	Α	9	8	7	6	5	4	3	2	1	0			
Cipher:	1	Е	Е	D	4	1	Е	2	1	0	3	8	5	С	9	8			
Compl:	Е	1	1	2	В	Е	1	D	Е	F	С	7	Α	3	6	7			_
				0		of Oimbo	44 > 0	-ii1 Oi		> F440D	E4DEE03	4007					-		_
	1	1	1	Con	npiement	of Cipne	rtext -> O	riginai C	pnertext	-> E112B	E1DEFC/	A36/			1				_
																			_
							Orig	ginal			Comp	lement							
				K	Cey		12341234	1234123	4	E	DCBEDCE	BEDCBED	СВ						
				Plai	ntext	Original 12341234 12341234 12345678ABCDEF12 E112BE1DEFC7A367					EDCBA98	7543210E	D						
				Ciph	ertext		-112RF1Γ	FFC7A36	§7		1EED41E	210385C9	8	1					_