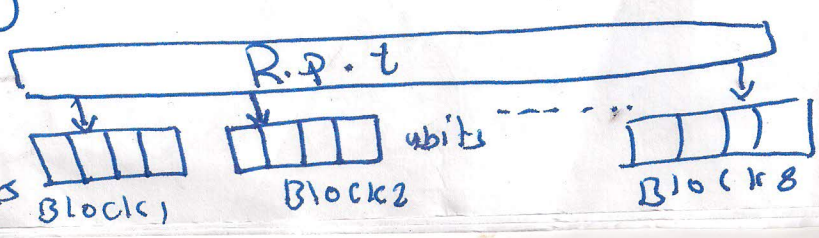
y these swapped bits are transposition
cording to inverse- initial transposition
and obtaining 64 bit of cipher text.

هذا المفهوم الذي يوضح كيف يدور.

→ In each round the 32 bits of Ri-1 فقط البيت يخضع للتوسع
is being expanded to 48-bits by using
(expansion permutation table) which generates
48-bits which are being X-ORed with
48-bit of secret key. 4

→ these 48 bit are divided into 8 groups.
(6 bit each) which are being ~~8 bit~~
substituted as 4 bits into 8 groups.
by using 8 S-boxes, thus, 32 bits are
being generated which are permuted by
using P-Box and X-ORed with Ci-1
generating 32 bits of Ri.



8 x 4 = 32

*Left circulare Shift:-

each round key is generated after left circular shift of 28-bit each, for two seperate blocks. (Ci-1, Di-1).

these Left circular shift bits are taken as,

1- Input to the PC-2 which generates 48 bits of round key.

2- these bits are also taken as input bits for next round (Ci-1, Di-1).

التبديل الابتدائي

...itial Permutation table:- 6

+8, +2

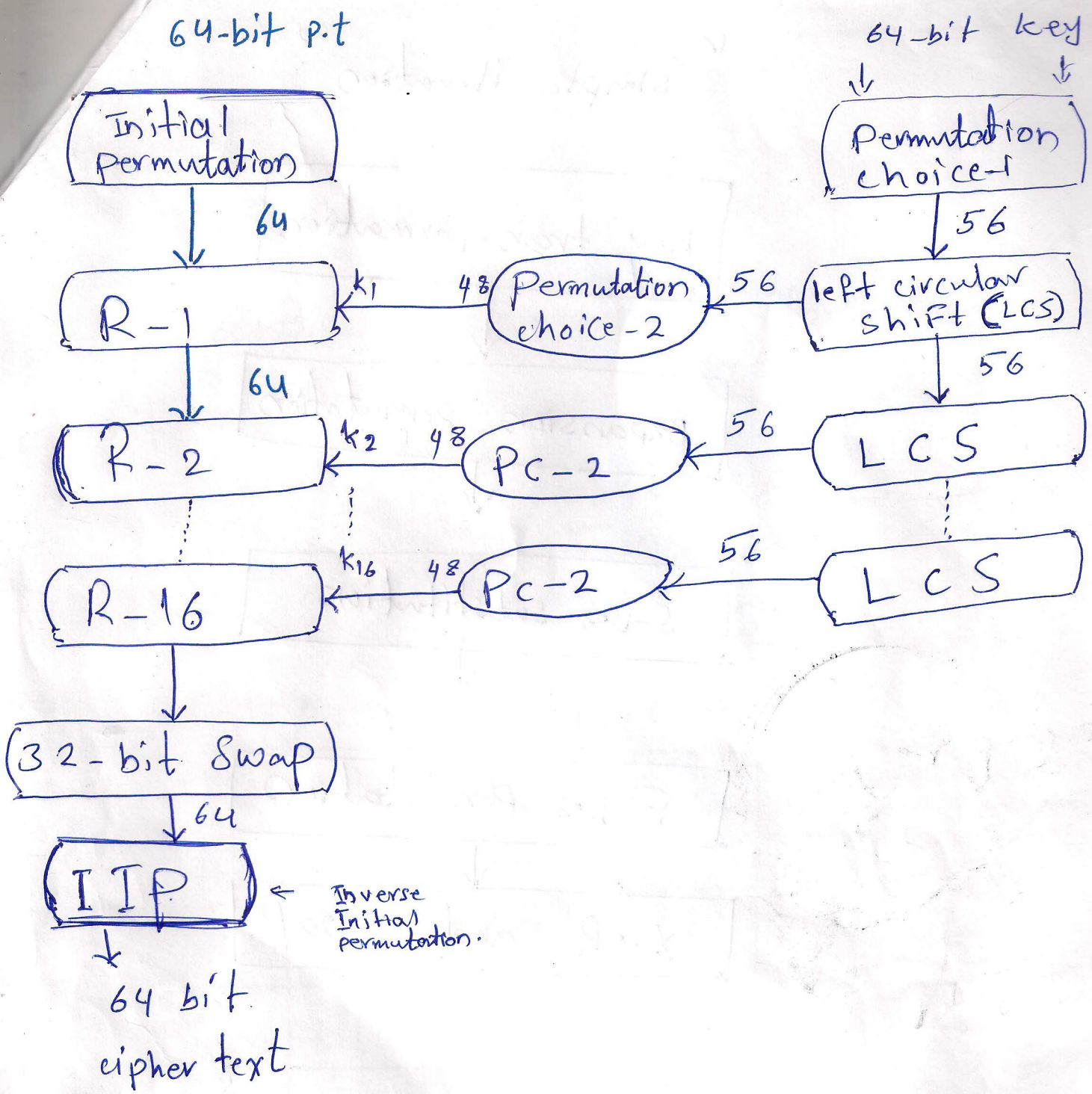
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

الواحد موقعه ← 5x8 =40

* Inverse initial permutation table:-

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

حيث اخذ العناصر حسب الموقع في المصفوفة السابقة.



ملاحظة: تكون عدد مدخلات PC أكثر من المخرجات.

"DES algorithm"

simple iteration