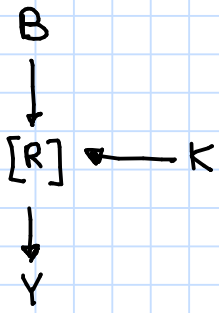
Es 1

Consider the following Feistel scheme



B = 1100 1111

K = 1111

Y?

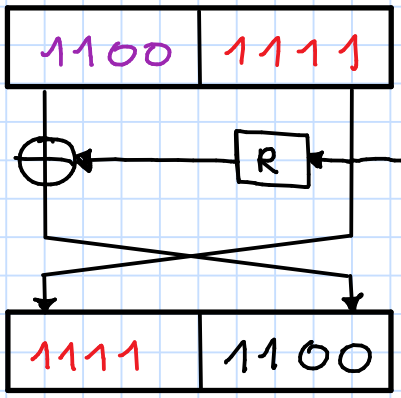
a) Y = 1111 1111

b) Y = 1100 1111

c) Y = 1111 1100 ✓

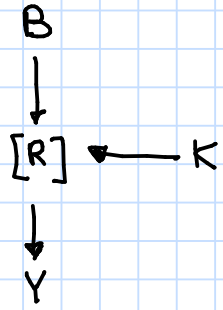
d) Y = 0000 0000

Solution: R is a XOR operation. The Feistel network works this way:



Es 1 other version

Consider the following Feistel scheme



B = 0100 1111

K = 1111

Y?

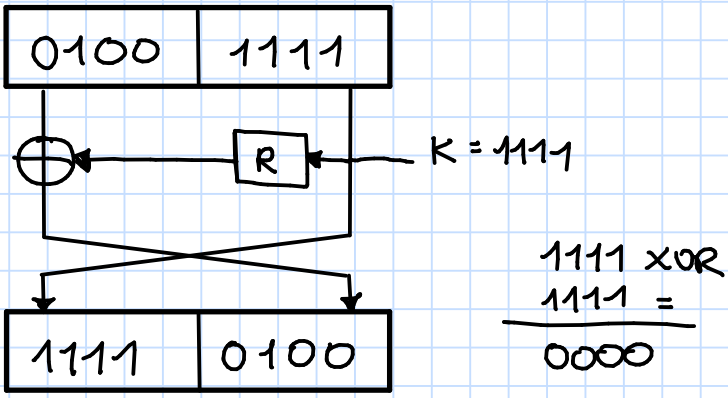
a) Y = 1111 1111

b) Y = 1100 1111

c) Y = 1111 0100

d) Y = 0000 0000

Solution: R is a XOR operation. The Feistel network works this way:



1111 XOR
1111 =
0000

Es 2

Compute the value of $S_1(22)$ in DES algorithm

Here is S_1:

S_1	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

a) $S_1(22) = 14$

b) $S_1(22) = 11$

c) $S_1(22) = 12$ ✓

d) $S_1(22) = 7$

Solution

First of all we transform 22 in binary using 6 bit

$22|_{10} = 2^4 + 2^2 + 2^1 = 010110$

row = 0

col = 11

Compute the value of S(55)

$55 = 32+16+4+2+1 = 2^5+2^4+2^2+2^1+2^0 = 110111$

col 11

row 3

S(55) = 14

Es 3

Here the tables of DES permutations IP and its inverse

ble 3.1 Initial permutation *IP*

IP							
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

Table 3.2 Final permutation IP^{-1}

IP^{-1}							
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

Compute the first row of the table corresponding to the composition

$IP^2 = IP \circ IP$

Solution: in the first position we put the value "pointed" by the value of the first position of IP and so on

$IP(0,0) = 58$ => go to the 58^{th} position => 55

$IP^2(0,0) = 55$

...

55	53	51	49	56	54	52	50