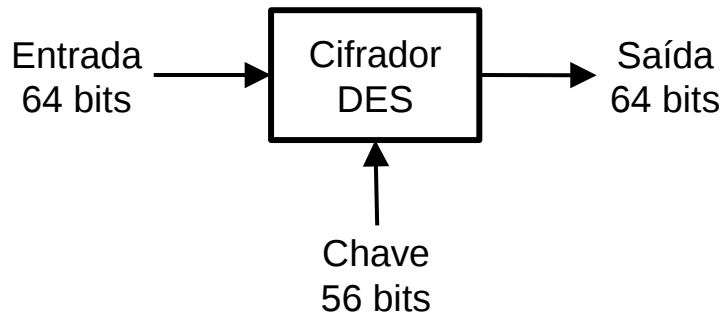


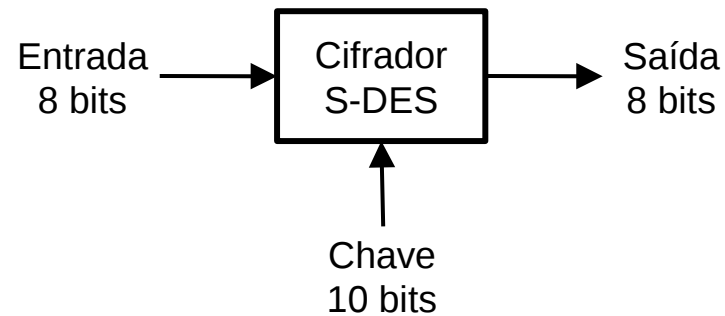
DES Simplificado

S-DES

DES Simplificado



Versão Simplificada



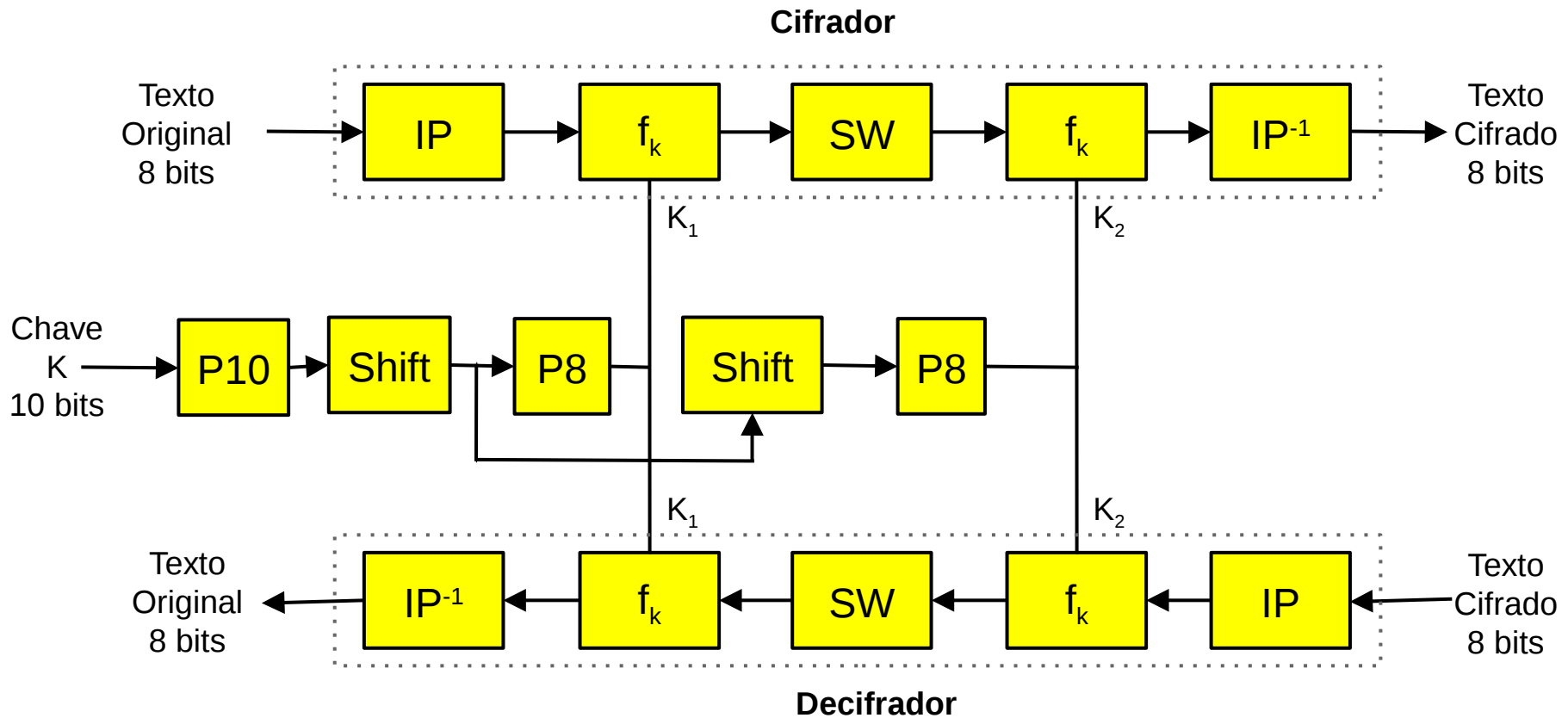
DES Simplificado

Legenda

IP - Initial Permutation

P - Permutation

SW - Switch



Geração de Sub-chaves

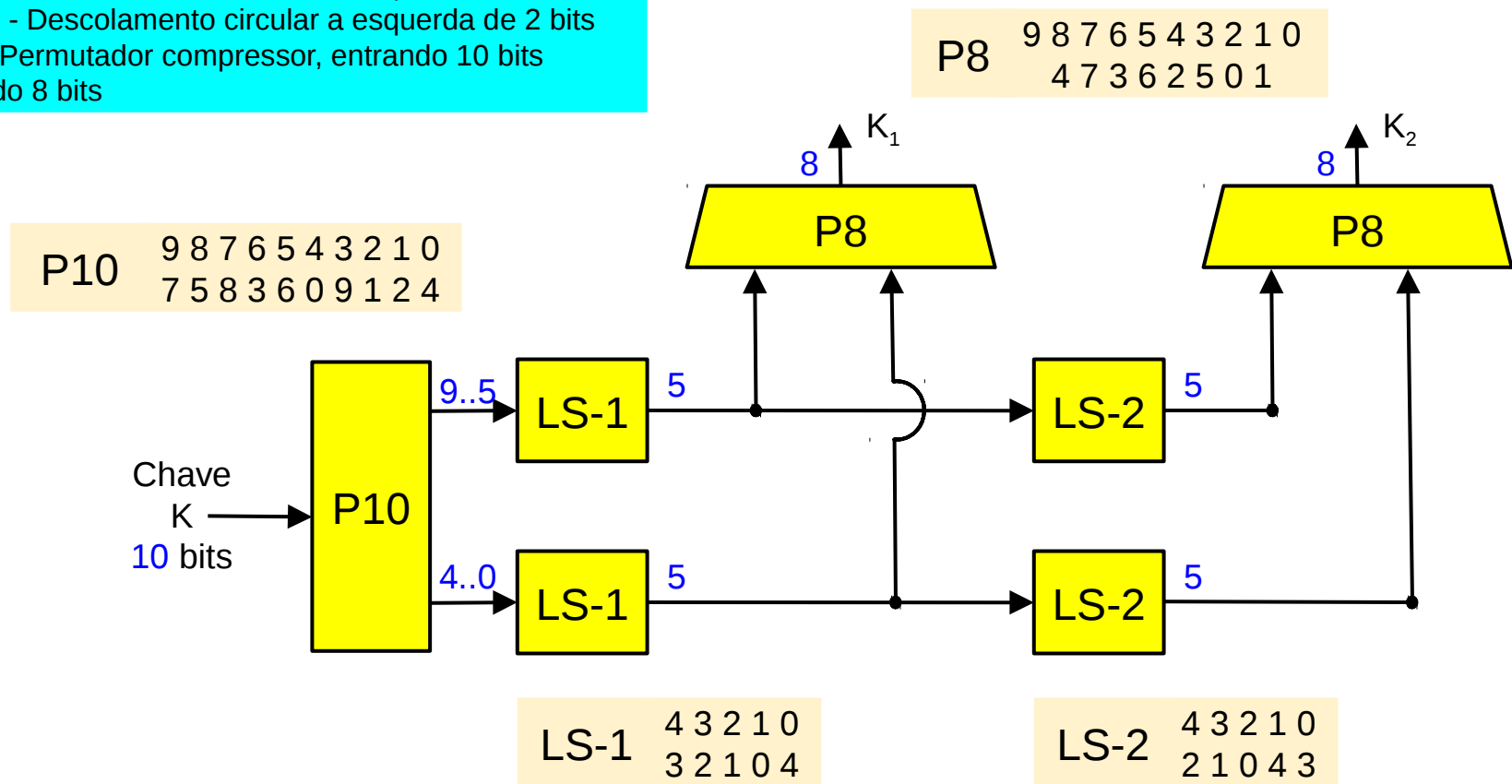
Legenda

P10 - Permutador de 10 bits

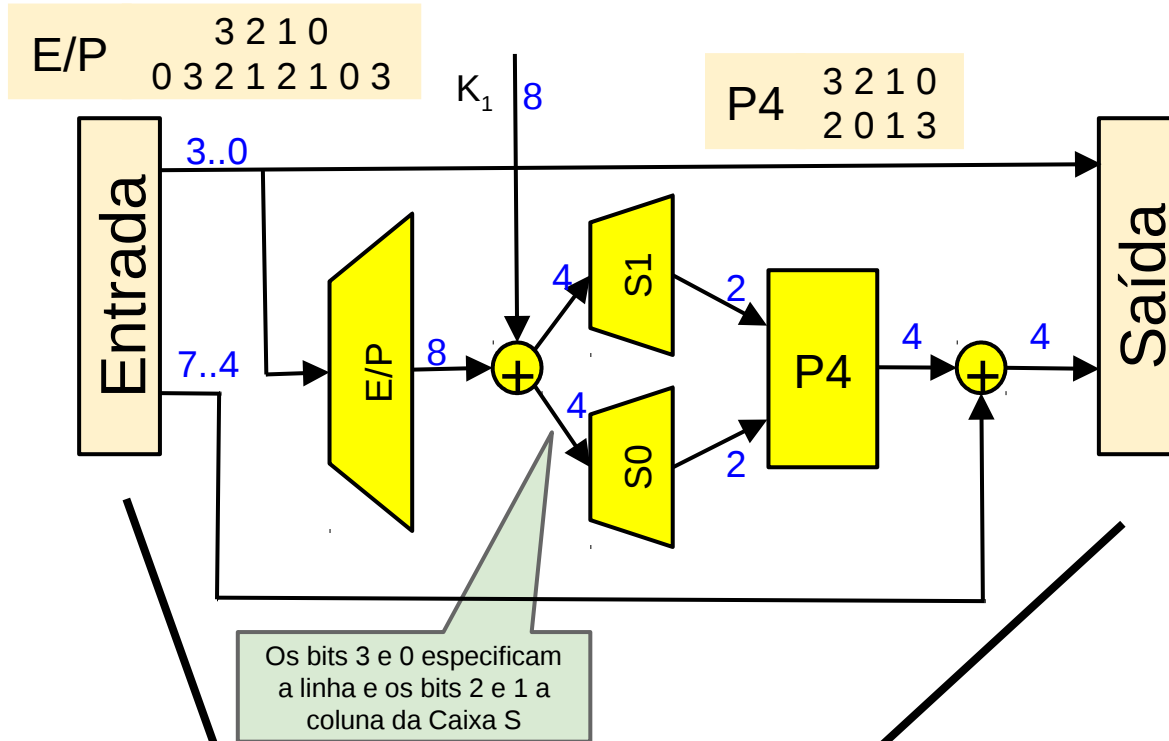
LS-1 - Descolamento circular a esquerda de 1 bit

LS-2 - Descolamento circular a esquerda de 2 bits

P8 - Permutador compressor, entrando 10 bits saindo 8 bits



Função f_k



S0

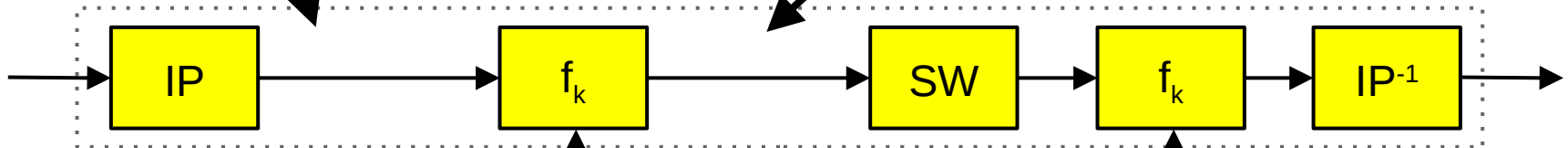
01	00	11	10
11	10	01	00
00	10	01	11
11	01	11	10

S1

00	01	10	11
10	00	01	11
11	00	01	00
10	01	00	11

XOR

Cifrador



IP

7	6	5	4	3	2	1	0
6	2	5	7	4	0	3	1

SW

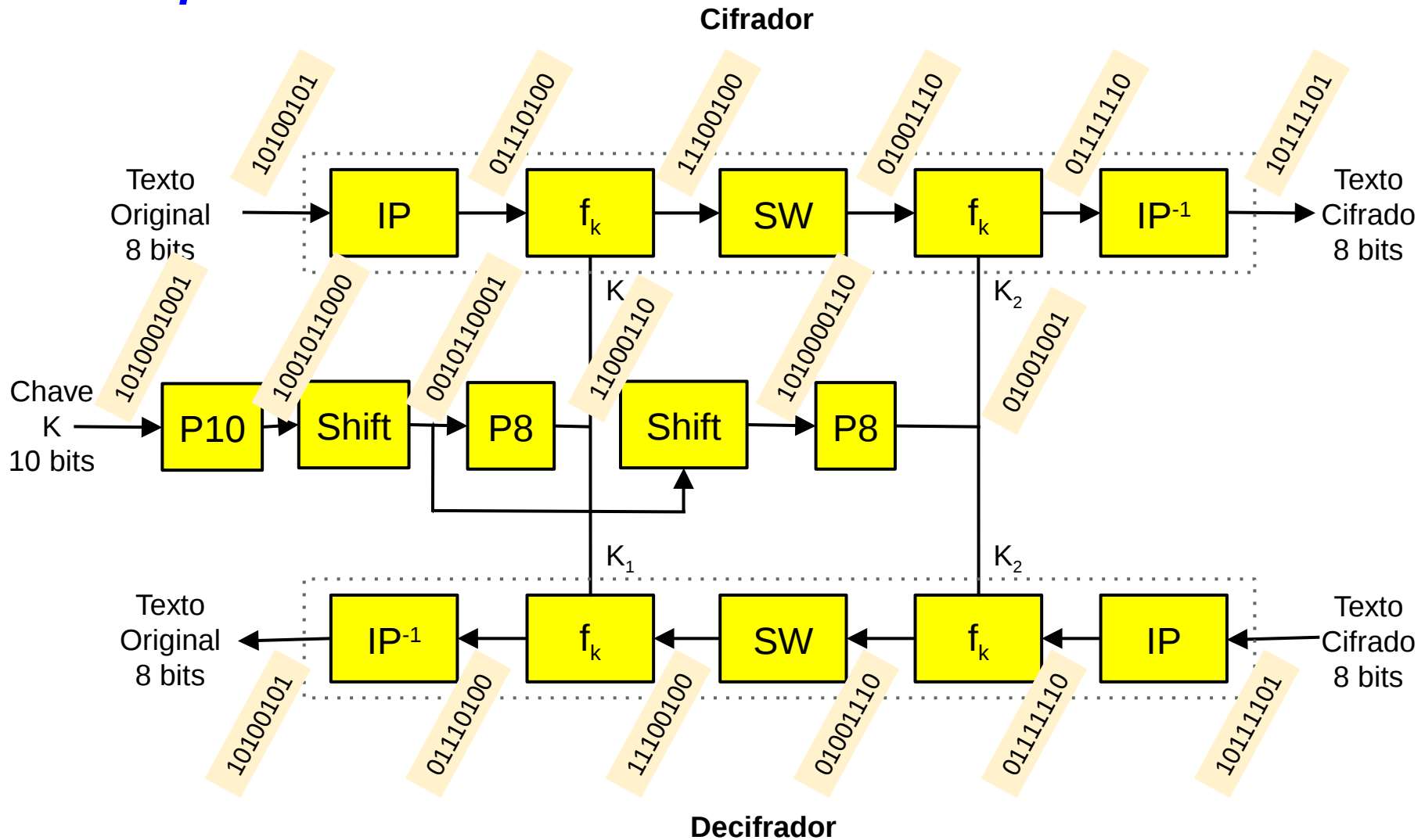
7	6	5	4	3	2	1	0
3	2	1	0	7	6	5	4

IP⁻¹

7	6	5	4	3	2	1	0
4	7	5	3	1	6	0	2

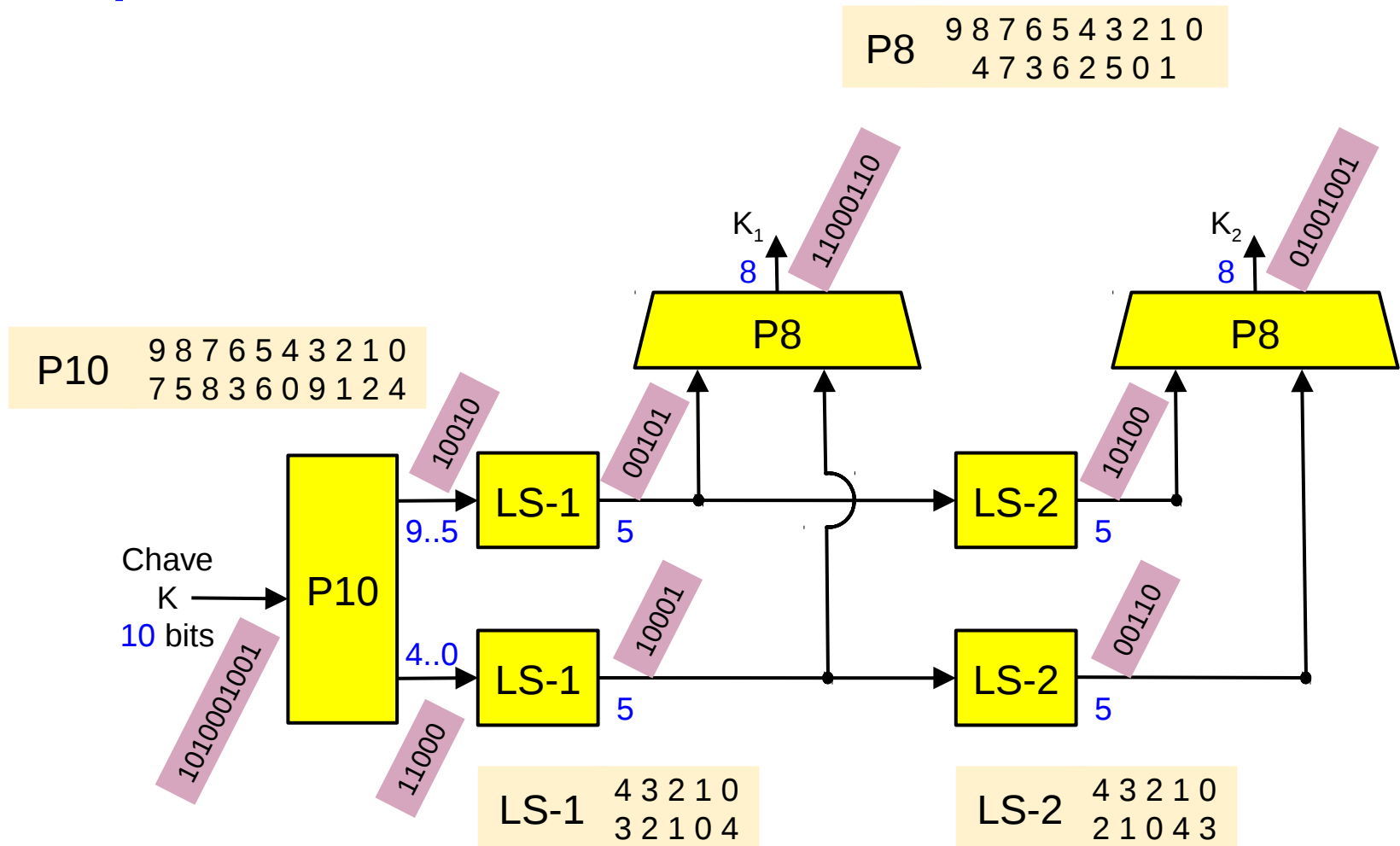
DES Simplificado

Exemplo

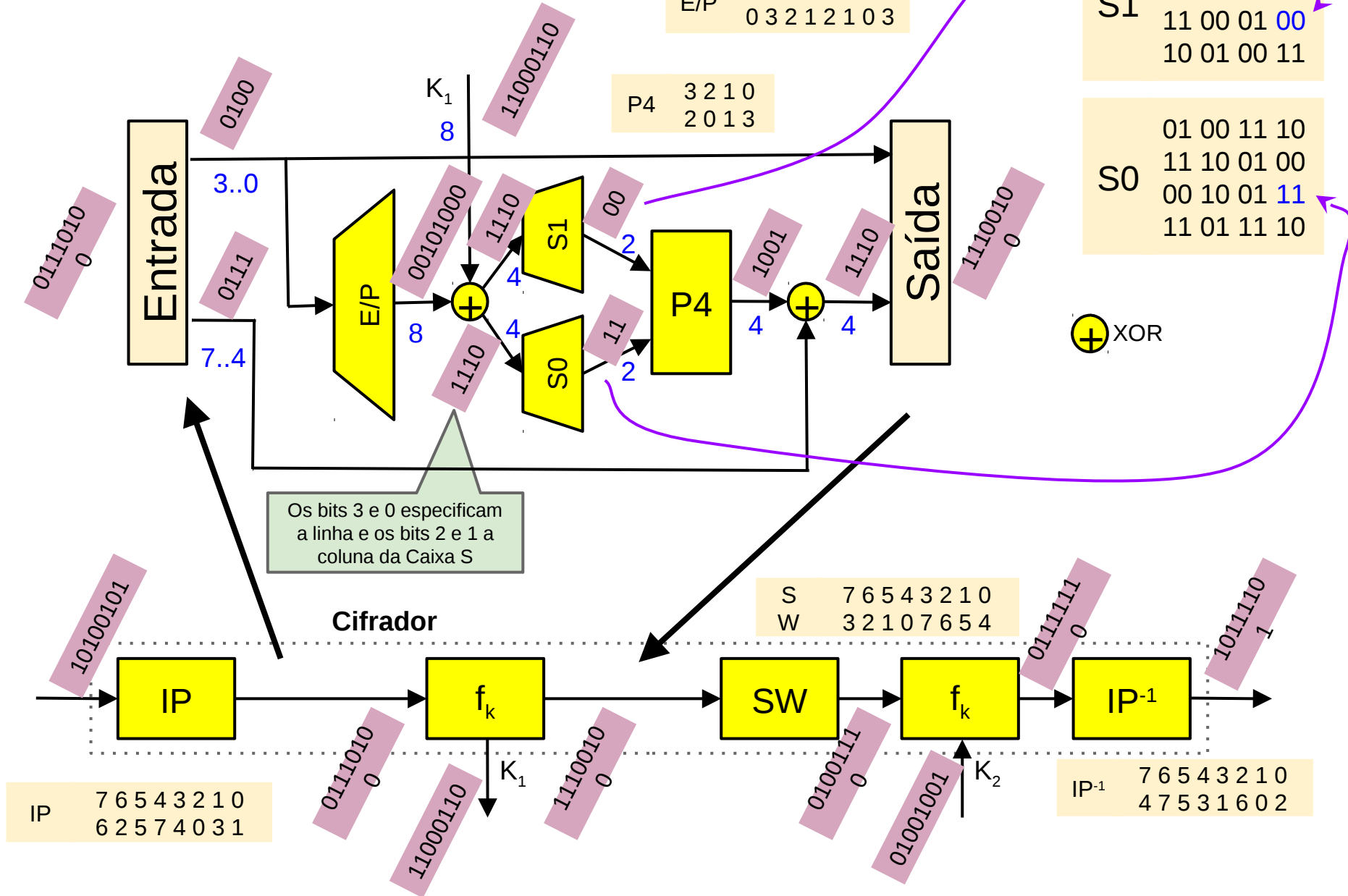


Geração de Sub-chaves

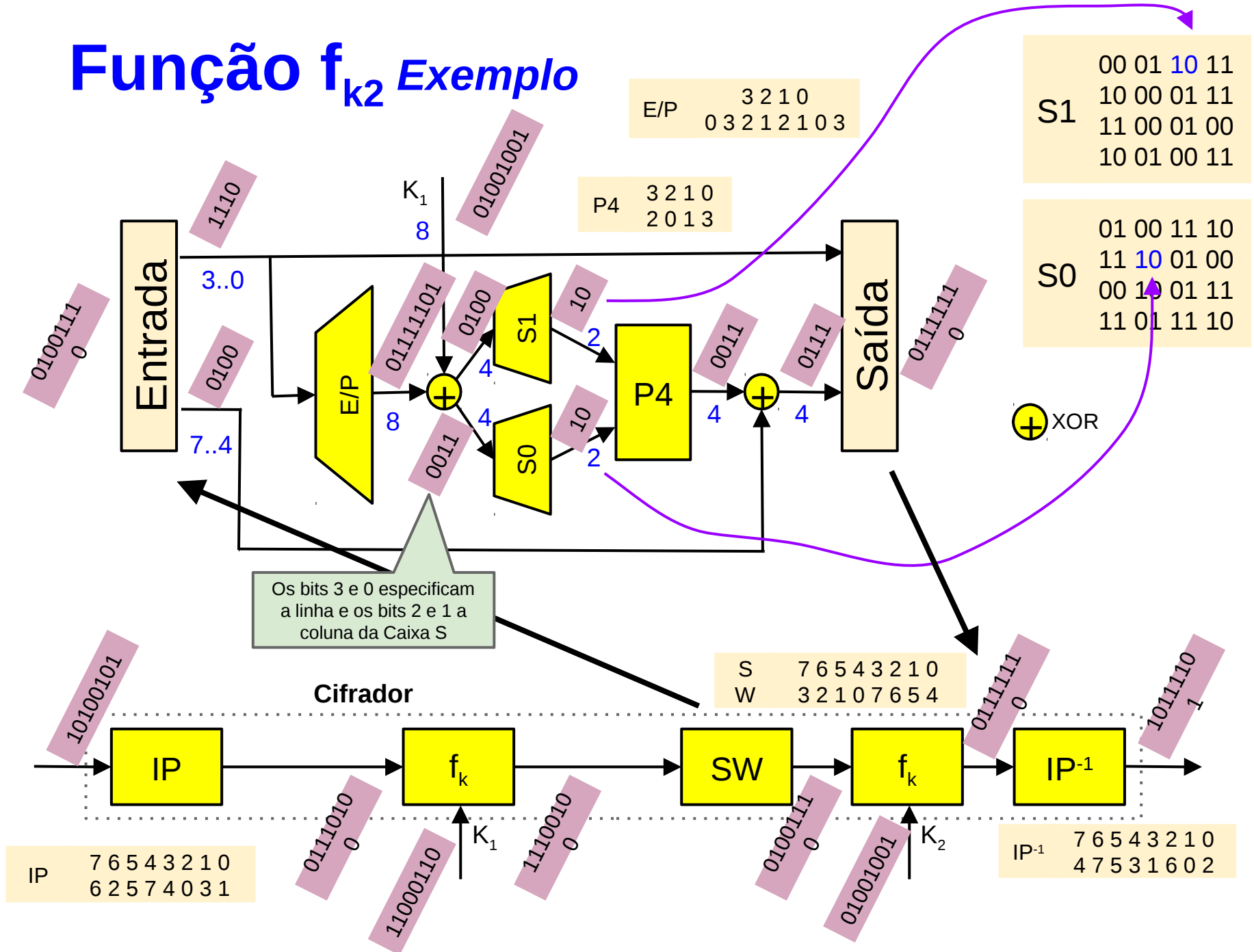
Exemplo



Função f_{k1} Exemplo



Função f_{k2} Exemplo



DES Simplificado

Exercício

Converta o seu número de matrícula para binário e tome como chave os primeiros 10 bits (da esquerda).

1 - Cifre os últimos 8 bits (da direita) utilizando S-DES. Mostre todos os passos.

2 – Decifre a cifra obtida no passo anterior utilizando a mesma chave. Mostre todos os passos.

Exemplo: N° de matrícula: “123456123456”

Conversão para binário: **1110010111110100011101111001001000000**

Modo	Chave	Entrada	Saída
Ciframento	1110010111	01000000	?
Deciframento	1110010111	?	01000000

