Algoritmo Simplified Data Encryption Standard (SDES)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

SDES

- Definición
- Características
- Proceso SDES
- Descifrado

Definición

Es una versión simple del algoritmo DES.

Similar al algoritmo DES pero es un algoritmo más pequeño y tiene menos parámetros que DES.

Se creó con fines educativos para que la comprensión de DES fuera más sencilla.

Se necesita un bloque de 8 bits.

Características

Cifrado de bloque.

Llave de 10 bits. (2 bits de paridad)

Utiliza permutaciones como DES

Utiliza desplazamiento de bits como DES

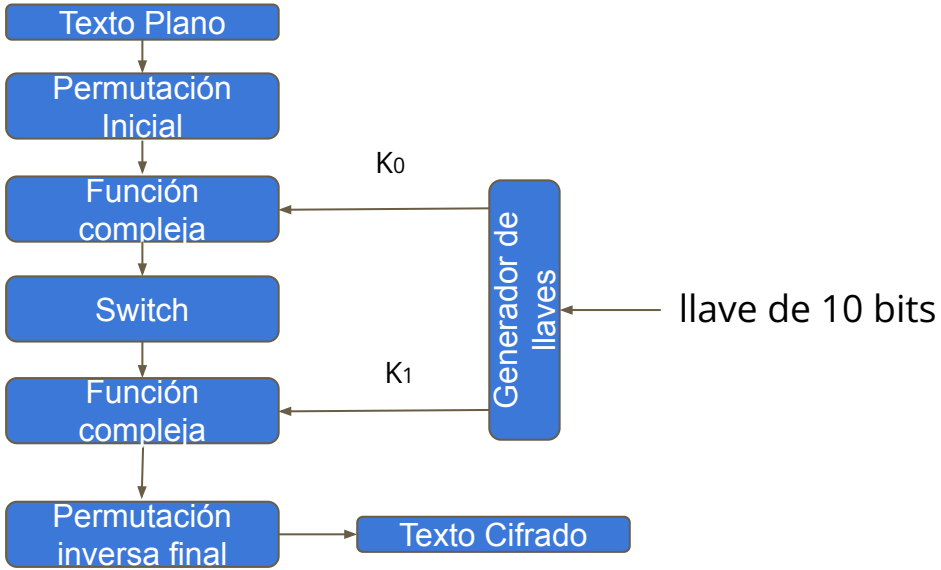
S-BOX mas pequeña

XOR

INPUT		OUTPUT
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Proceso SDES

Proceso SDES



Proceso SDES

Mensaje (M): m (8 bits)

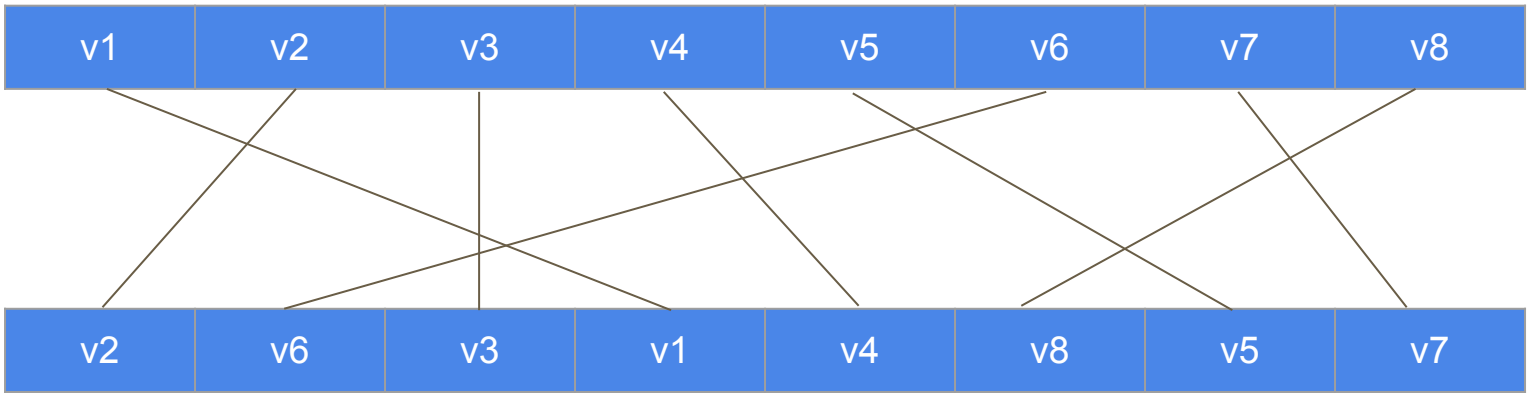
0110 1100

llave (K): a (10 bits)

11000 00101

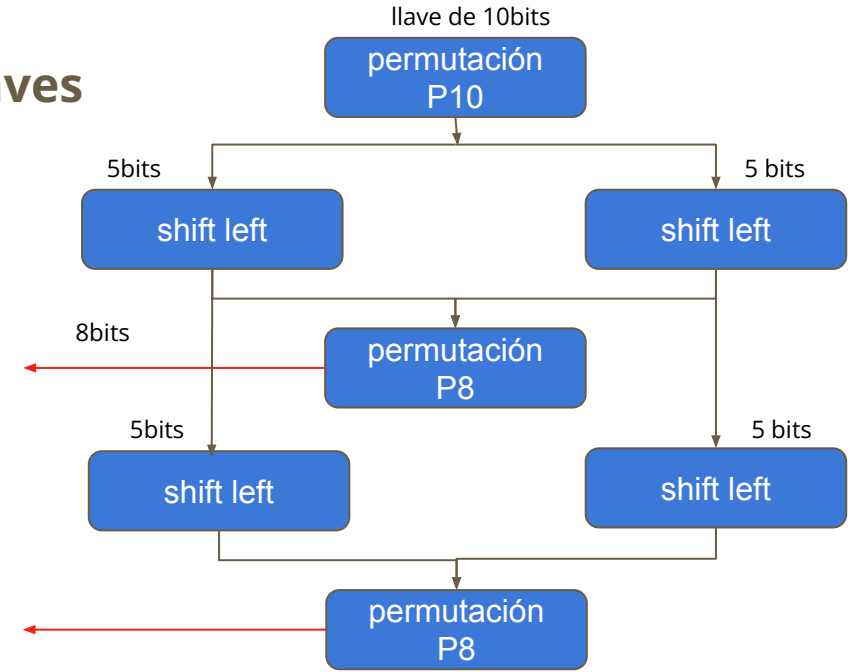
Proceso SDES

Permutación Inicial



Proceso SDES

Generador de llaves

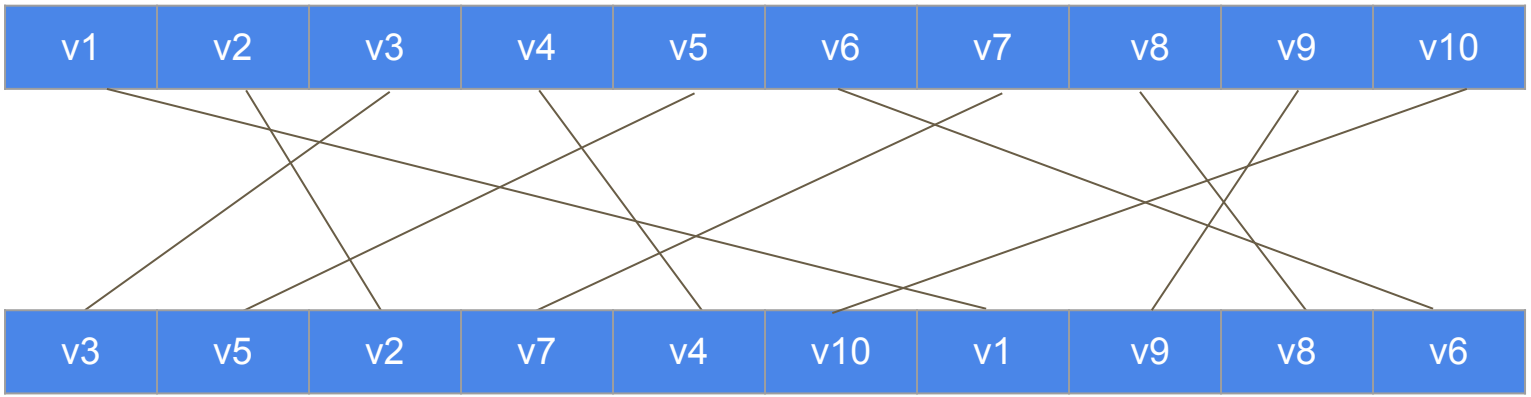


K1: Ronda 1

K2: Ronda 2

Proceso SDES

Permutación
P10



Proceso SDES

llave (K): ar (10 bits)

11000 00101

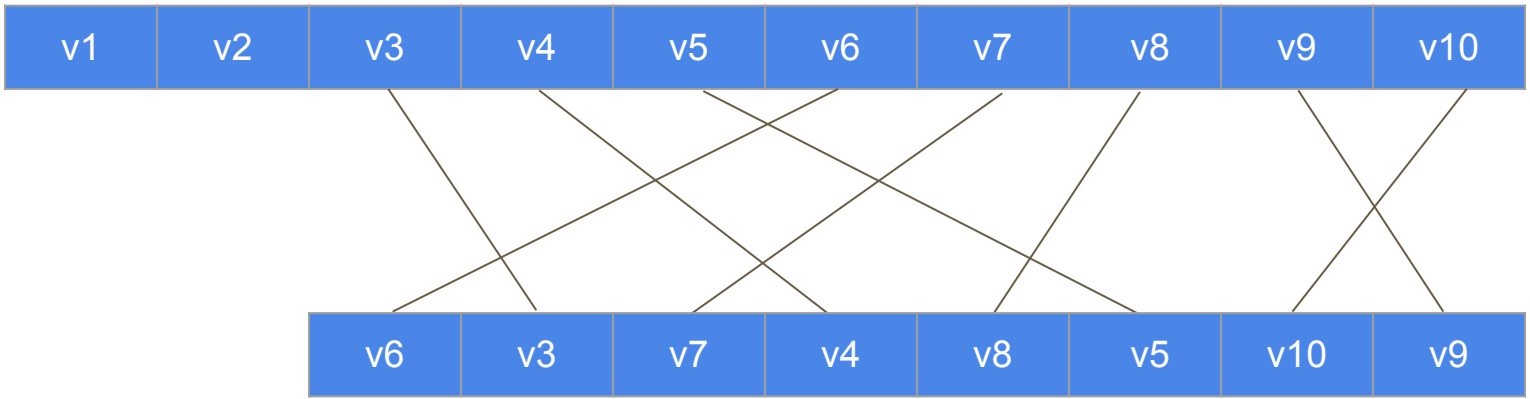
P10:

00100 11010

Proceso SDES

Proceso SDES

Permutación P8



Proceso SDES

0100010101

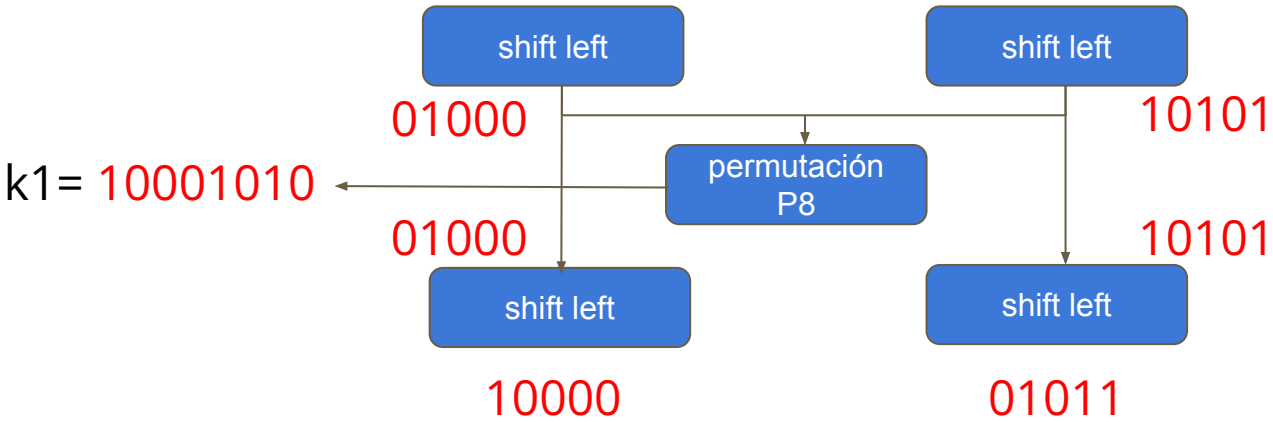
P8:

10001010

entonces

k1= 10001010

Proceso SDES



Proceso SDES

1000001011

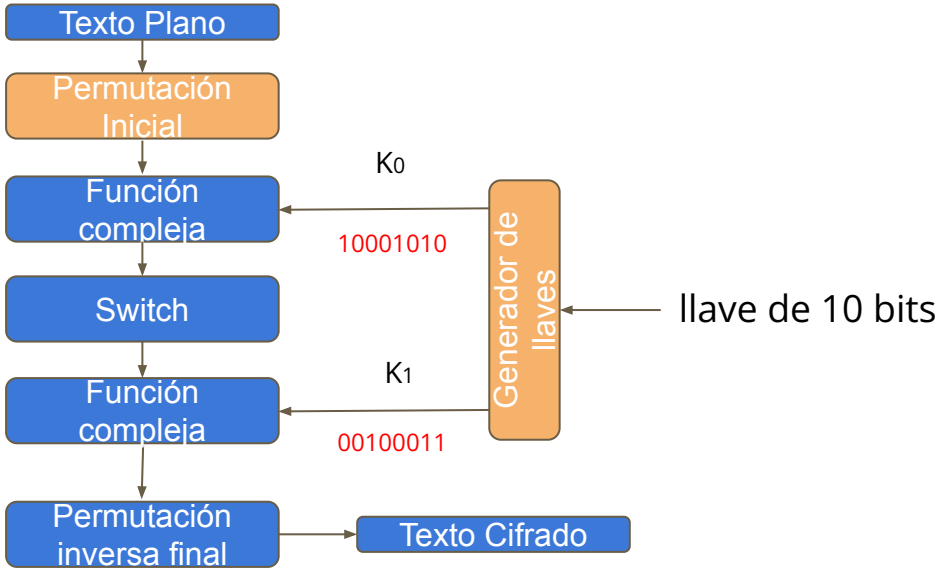
P8:

00100011

entonces

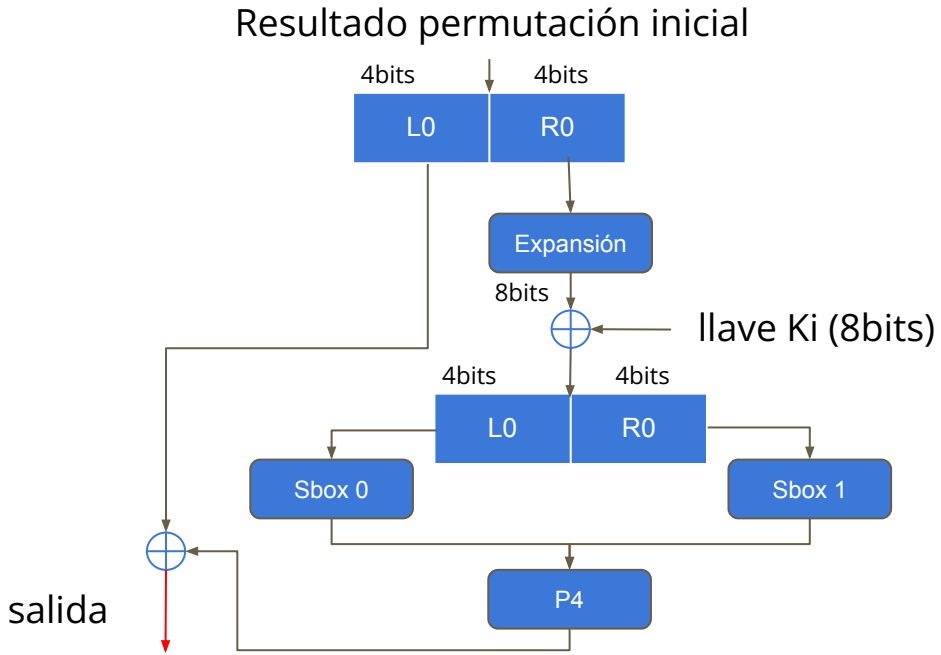
k2= 00100011

Proceso SDES



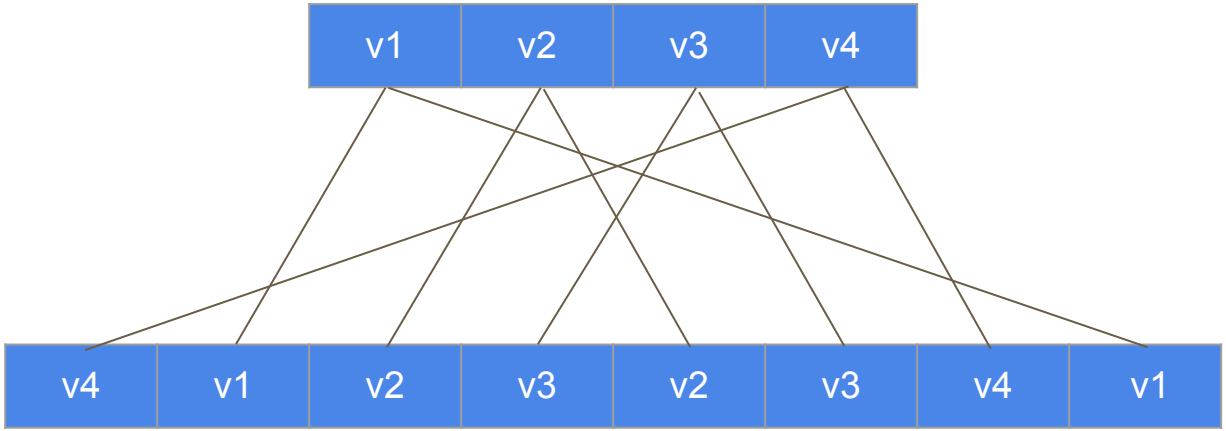
Proceso SDES

función compleja (fw)



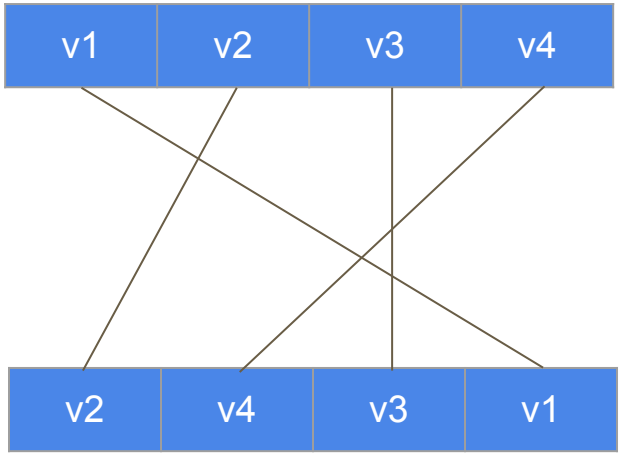
Proceso SDES

Expansión



Proceso SDES

P4



Proceso SDES

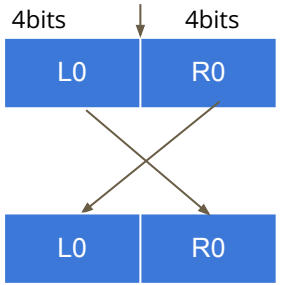
Sbox

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

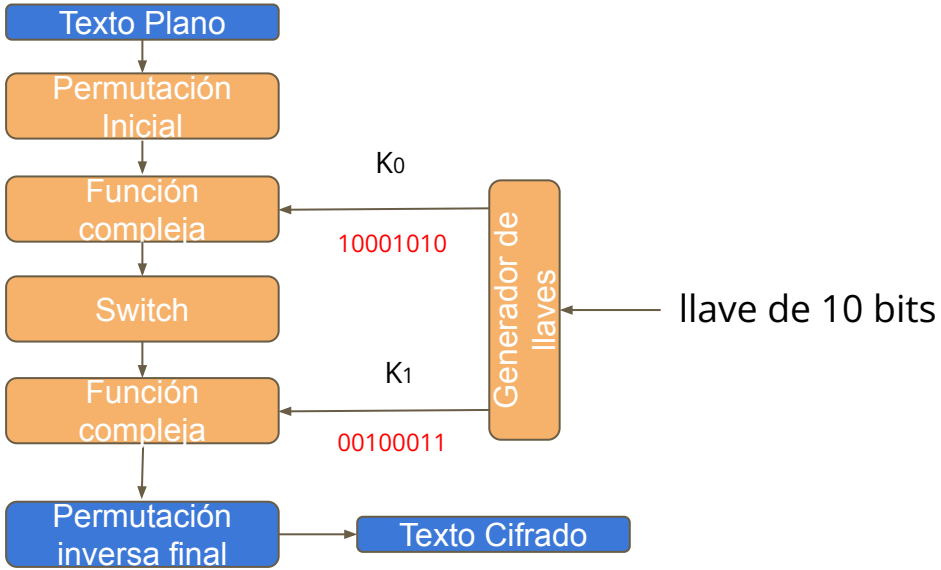
Proceso SDES

Switch

Resultado función compleja

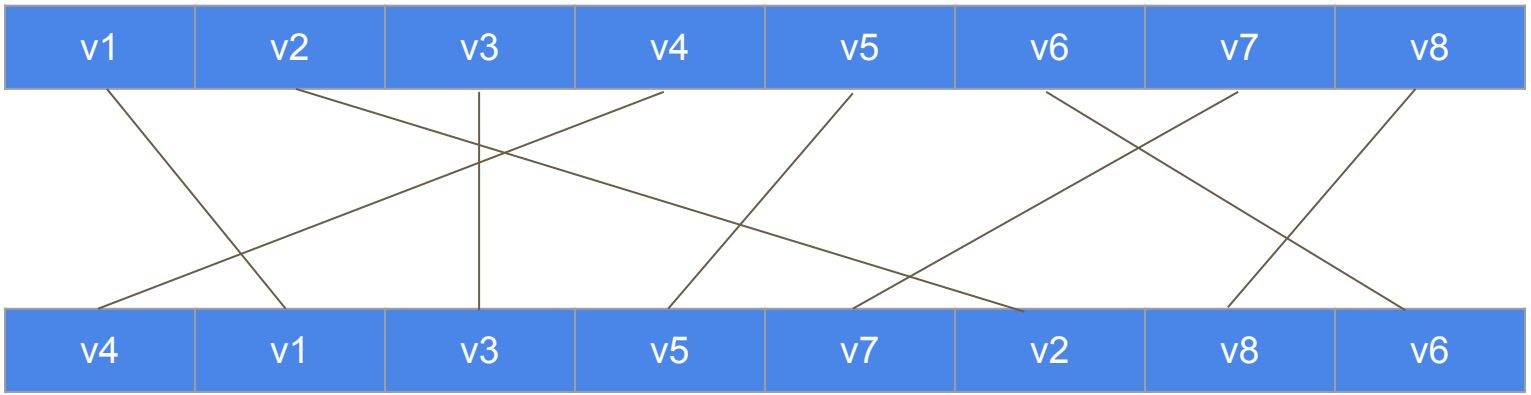


Proceso SDES

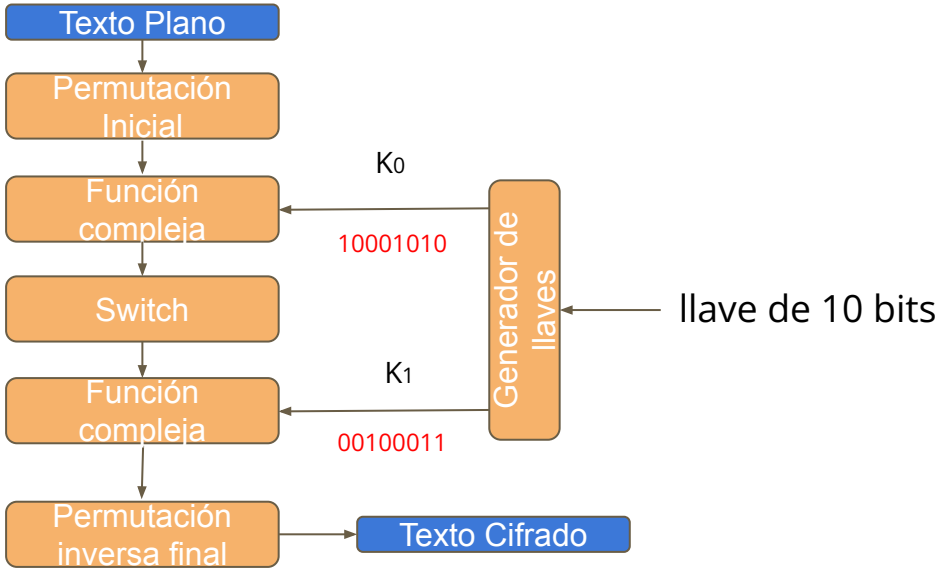


Proceso SDES

Permutación inversa final



Proceso SDES



Proceso SDES

Descifrado