Algoritmo Data Encryption Standard (DES)

Ing. Max Alejandro Antonio Cerna Flores

Agenda

DES

- Definición
- Características
- Cifrado Feistel
- Proceso Feistel
- S-BOX
- Proceso DES

Definición

Es el nombre del documento FIPS (Federal Information Processing Standard), del Departamento de Comercio de Estados Unidos. Fue publicado en 1977. En este documento se describe el DES.

Es un algoritmo de cifrado por bloques de 64 bits de tamaño. Emplea una llave de 56 bits durante la ejecución.

En la llave se eliminan 8 bits de paridad del bloque de 64 bits.

Definición

Aunque el DES era un algoritmo computacionalmente seguro, esto ha dejado de ser cierto, ya que con hardware específico es posible realizar ataques por fuerza bruta que descubran una clave en pocos días.

El problema principal es que el tamaño de la clave (56 bits) es demasiado pequeño para la potencia de cálculo actual.

El DES dejó de ser el algoritmo empleado por el gobierno norteamericano en Noviembre de 1998.

Características

Cifrado de bloque.

Llave de 56 bits. (8 bits de paridad)

Número de rondas: 16

Cifrado de Feistel.

Operaciones XOR.

S-BOX

Sub-llaves de 48 bits por ronda

XOR

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

Cifrado Feistel

Debe su nombre al criptógrafo Horst Feistel quien trabajó en IBM.

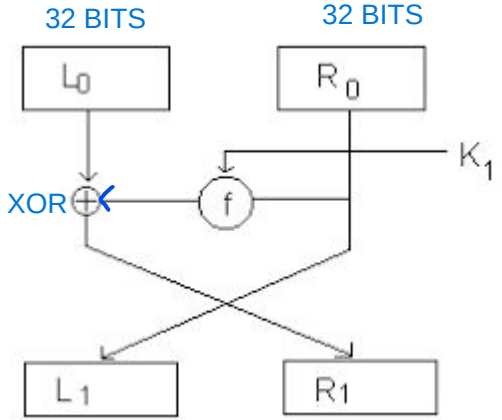
También es conocida comúnmente como Red de Feistel o Cadena de Feistel.

Presentan la ventaja de ser reversible para las operaciones de cifrado y descifrado, requiriendo únicamente invertir el orden de las subclaves utilizadas.

Se denomina simétrico por rondas.

Proceso Feistel

Se descompone el texto plano en dos piezas iguales, (L0 , R0)

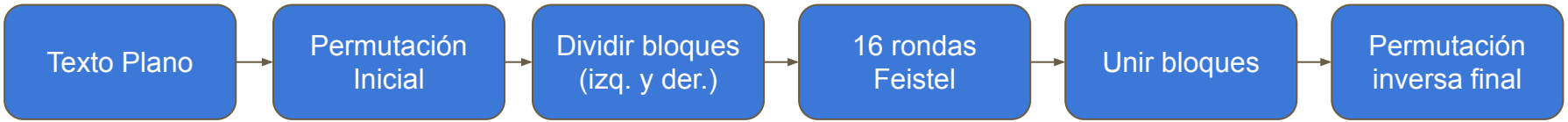


S-BOX

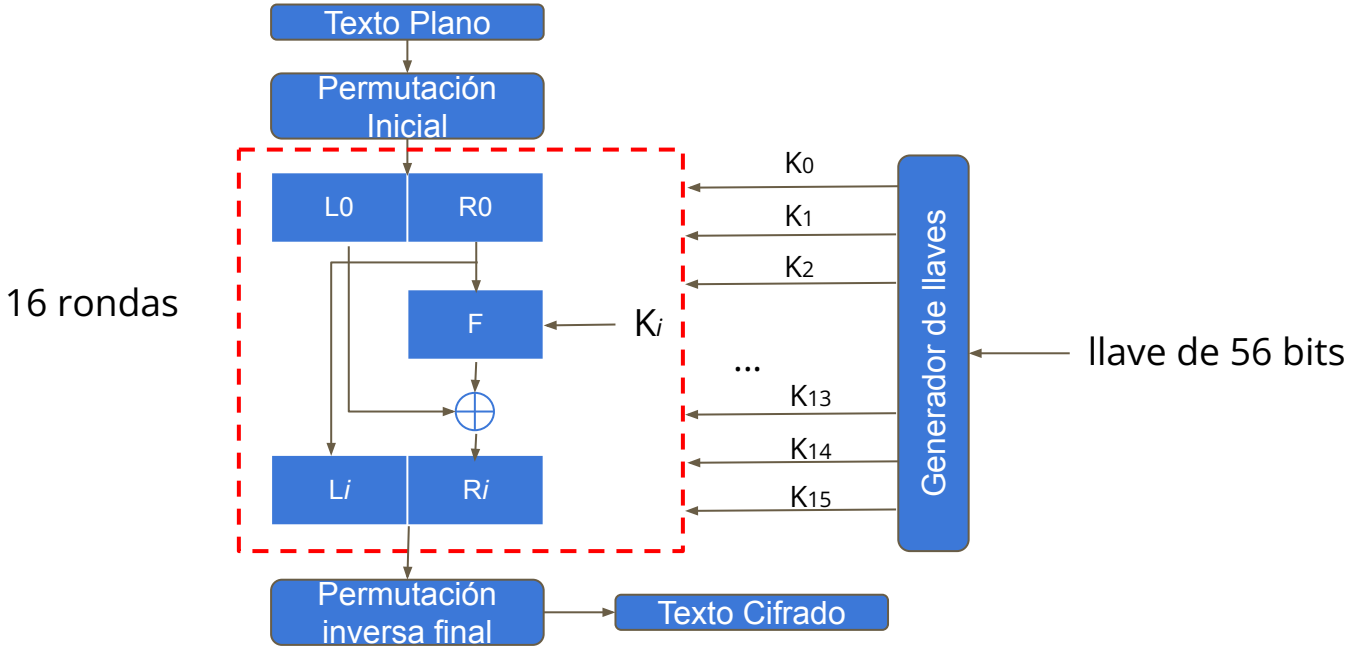
Tabla de Permutación:

i	S_i															
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Proceso DES


Texto Plano
Permutación Inicial
Dividir bloques (izq. y der.)
16 rondas Feistel
Unir bloques
Permutación inversa final

Proceso DES


Texto Plano
Permutación Inicial
L0
R0
F
Ki
Li
Ri
16 rondas
K0
K1
K2
...
K13
K14
K15
Generador de llaves
llave de 56 bits
Permutación inversa final
Texto Cifrado

Proceso DES

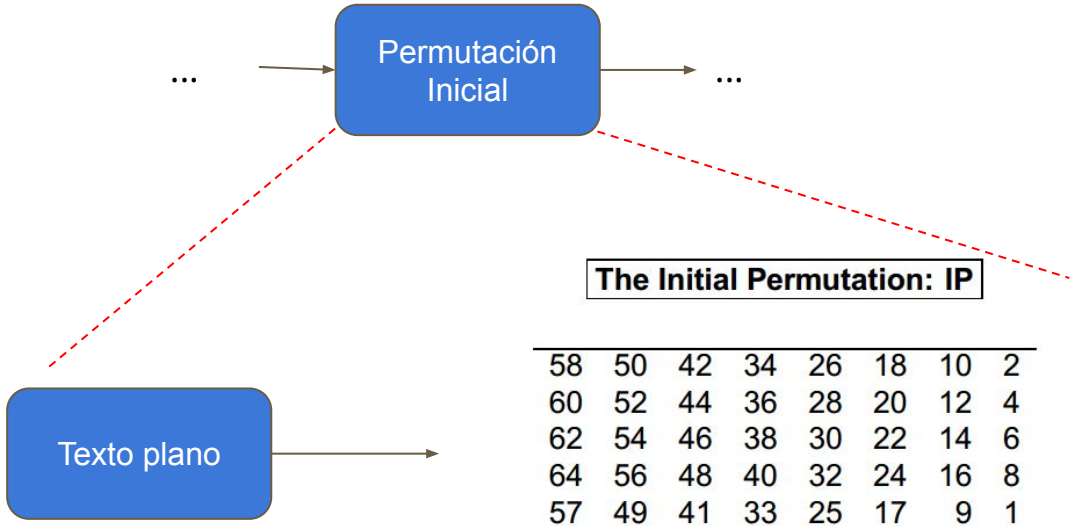
Mensaje (M): mensajes (64 bits)

0110 1101 0110 0101 0110 1110 0111 0011 0110 0001 0110 1010 0110 0101 0111 0011

llave (K): arbustos (64 bits)

1100 0010 1110 0101 1100 0100 1110 1010 1110 0110 111 01001 1101 1111 1110 0110

Proceso DES



The Initial Permutation: 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

Proceso DES

0110 1101 0110 0101 0110 1110 0111 0011 0110 0001 0110 1010 0110 0101 0111 0011

The Initial Permutation: 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

nuevo orden:
1

Proceso DES

0110 1101 0110 0101 0110 1110 0111 0011 0110 0001 0110 1010 0110 0101 0111 0011

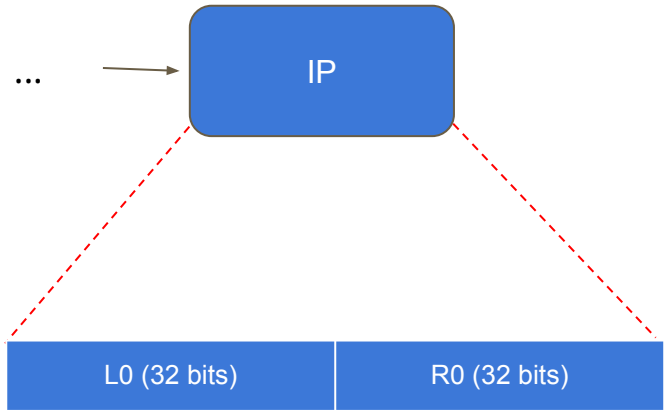
The Initial Permutation: IP

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

nuevo orden:
11

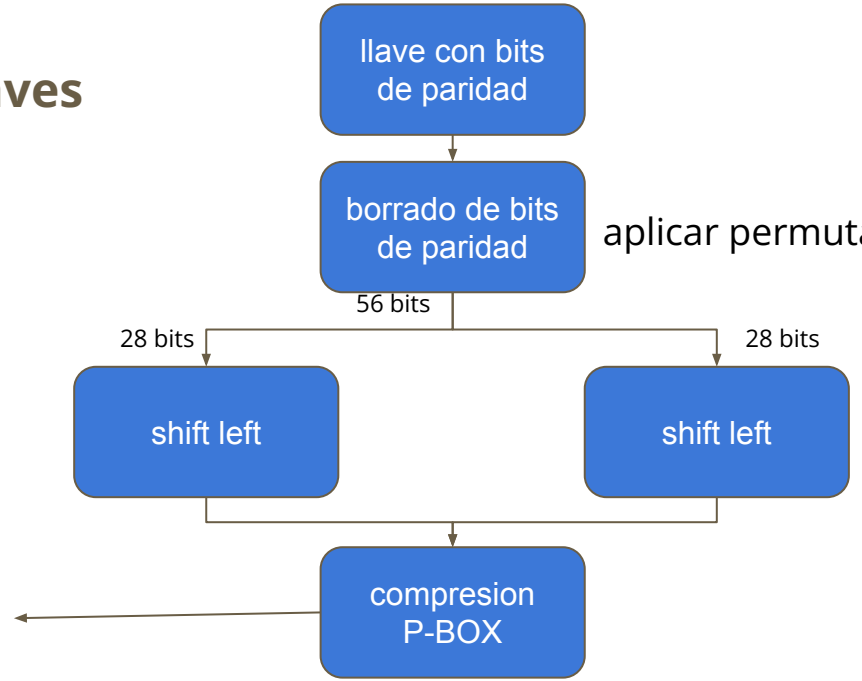
...

Proceso DES



Proceso DES

Generador de llaves

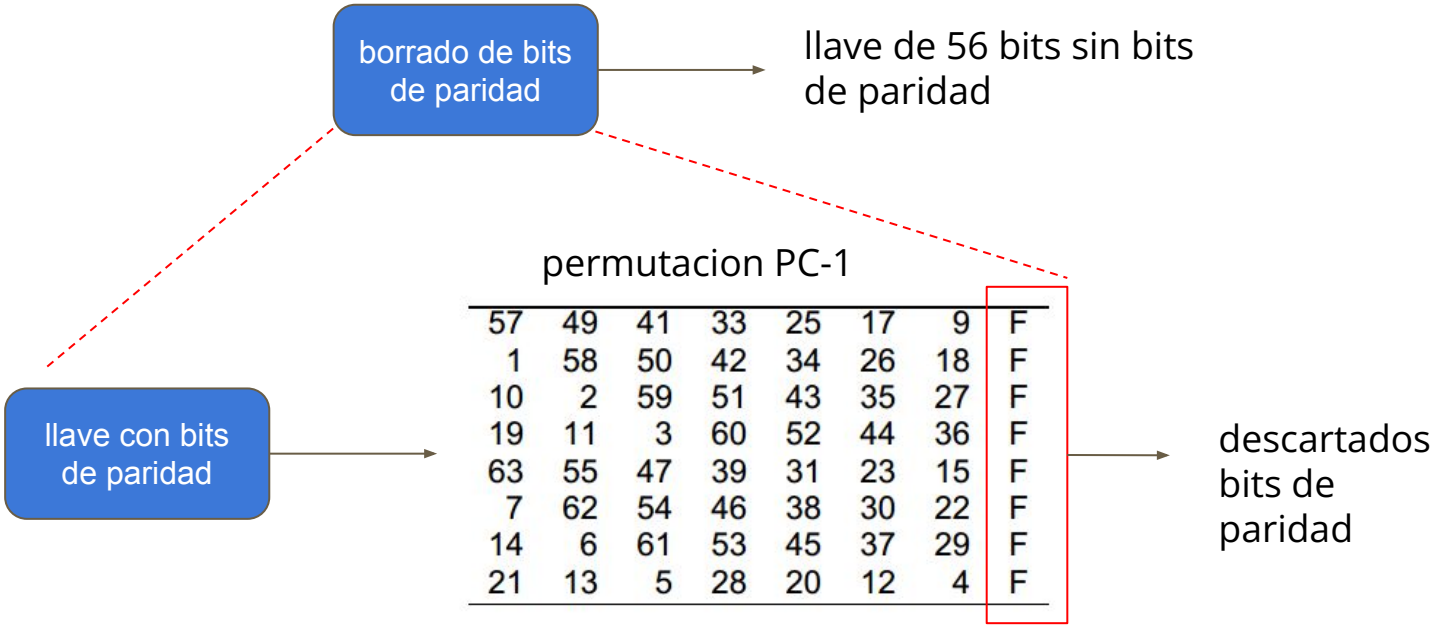


aplicar permutación PC-1

K1: Ronda 1

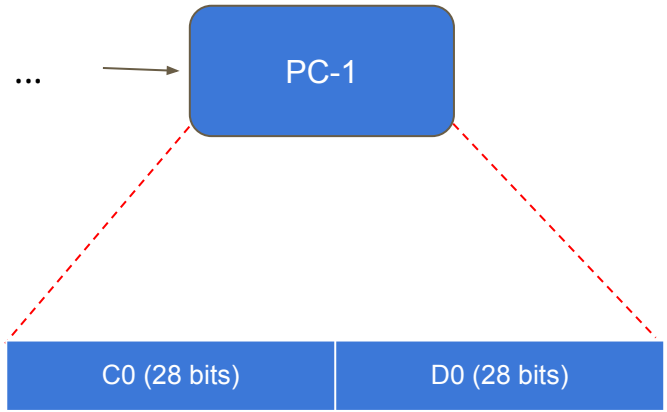
Repetir 16 veces para las 16 rondas.

Proceso DES



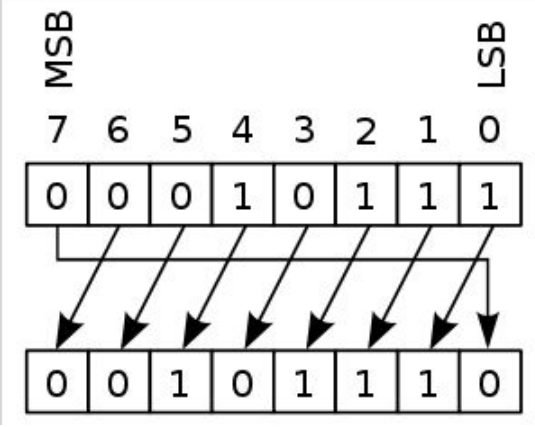
57	49	41	33	25	17	9	F
1	58	50	42	34	26	18	F
10	2	59	51	43	35	27	F
19	11	3	60	52	44	36	F
63	55	47	39	31	23	15	F
7	62	54	46	38	30	22	F
14	6	61	53	45	37	29	F
21	13	5	28	20	12	4	F

Proceso DES



Proceso DES

Desplazamientos (shift left)



C0 (28 bits)	D0 (28 bits)

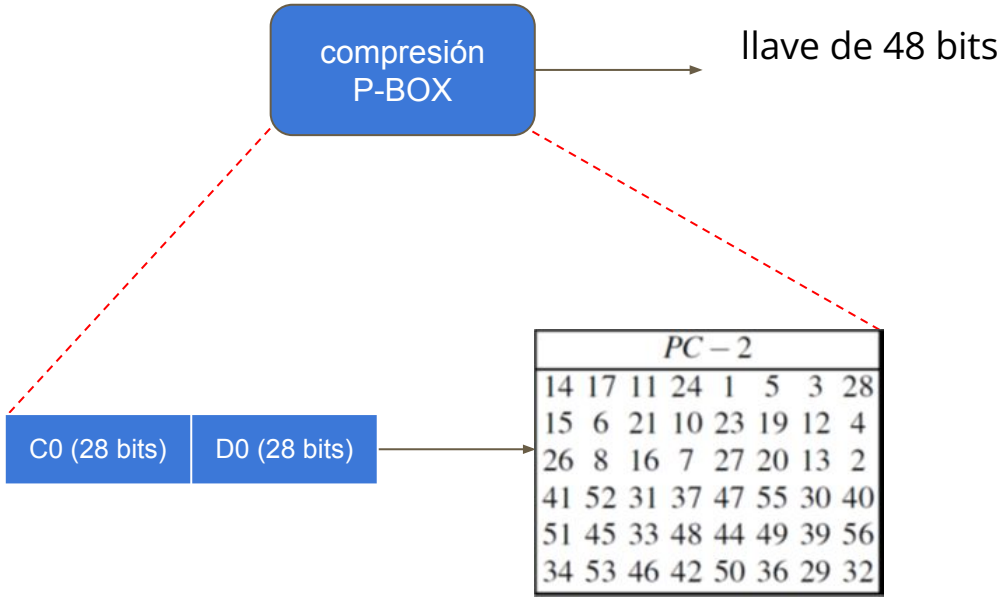
aplicar el desplazamiento para cada una de las mitades.

Proceso DES

Desplazamientos (shift left)

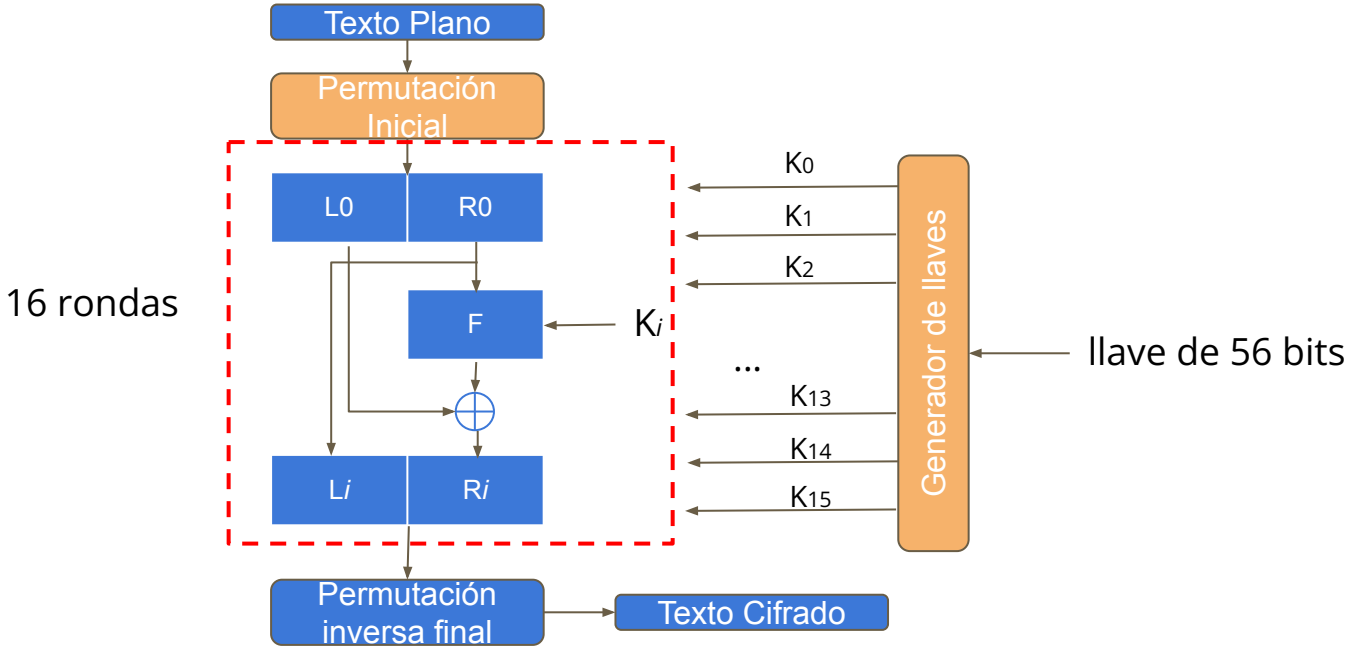
Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Proceso DES



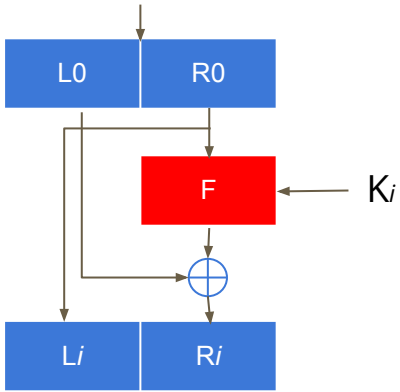
$PC-2$							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Proceso DES


Texto Plano
Permutación Inicial
L0
R0
F
Ki
Li
Ri
16 rondas
K0
K1
K2
...
K13
K14
K15
Generador de llaves
llave de 56 bits
Permutación inversa final
Texto Cifrado

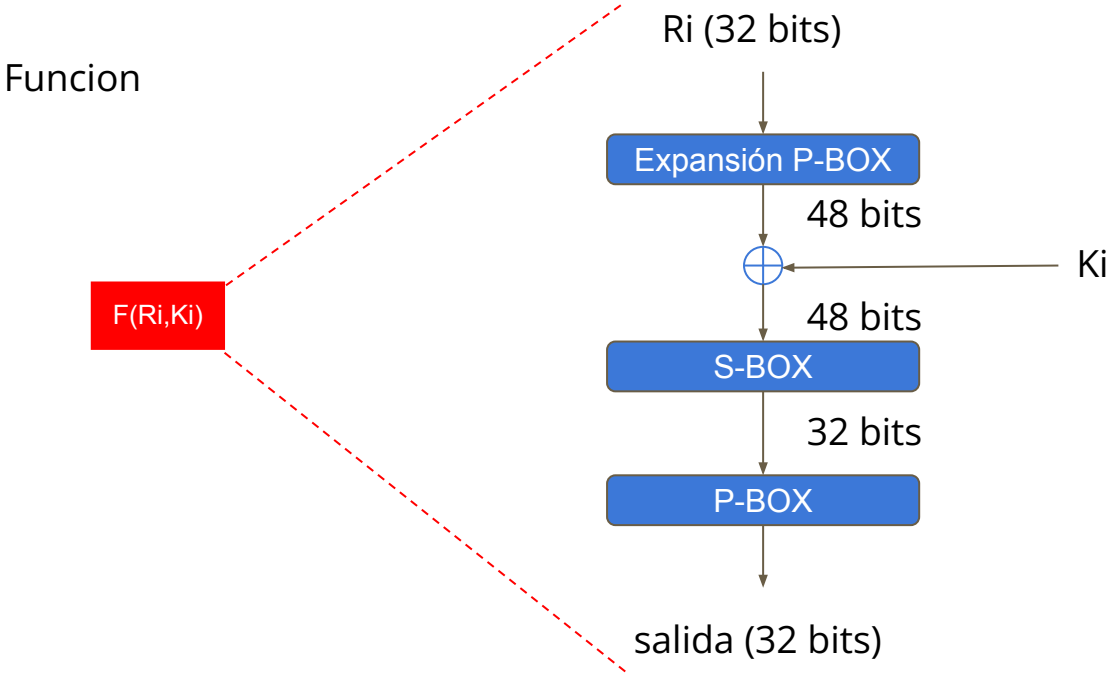
Proceso DES

Iniciar las 16 rodas

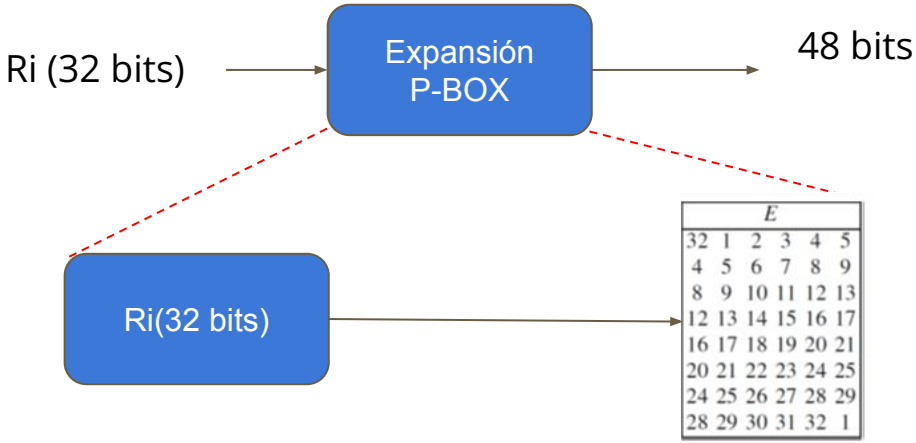


F(Ri,Ki)

Proceso DES

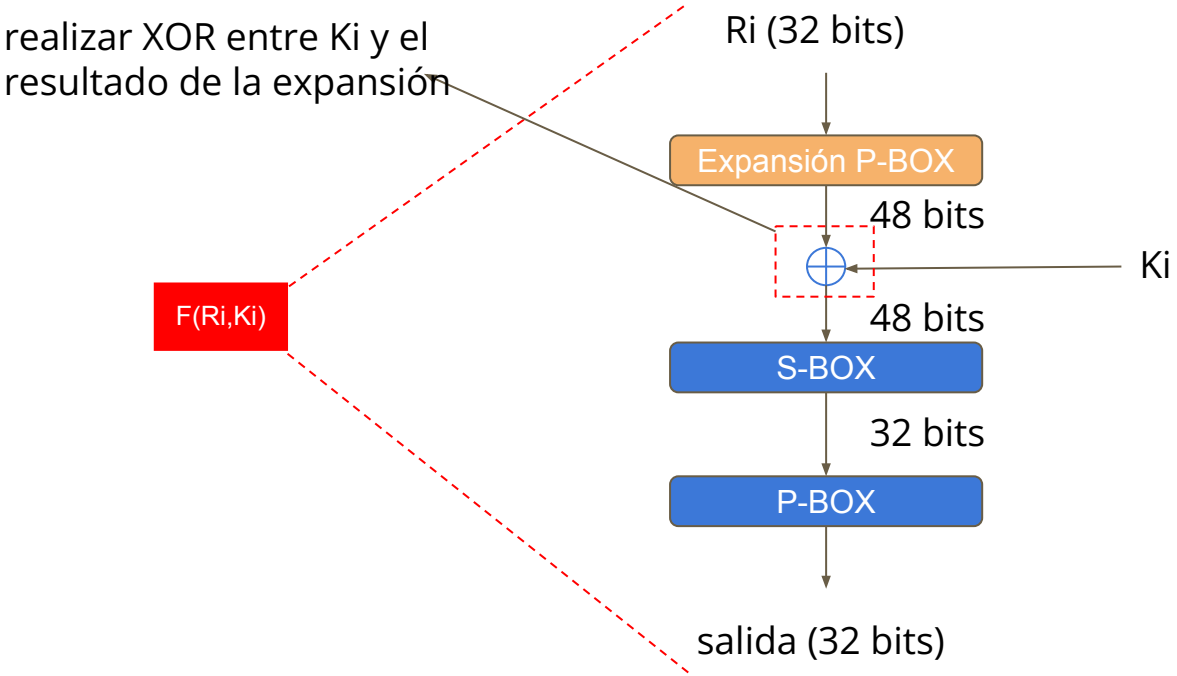

Funcion
F(Ri,Ki)
Ri (32 bits)
Expansión P-BOX
48 bits
Ki
48 bits
S-BOX
32 bits
P-BOX
salida (32 bits)

Proceso DES



IMPORTANTE
los 48 bits resultantes nos generarán 8 grupos de 6 bits cada uno

Proceso DES


realizar XOR entre Ki y el resultado de la expansión
Ri (32 bits)
Expansión P-BOX
48 bits
Ki
48 bits
S-BOX
32 bits
P-BOX
F(Ri,Ki)
salida (32 bits)

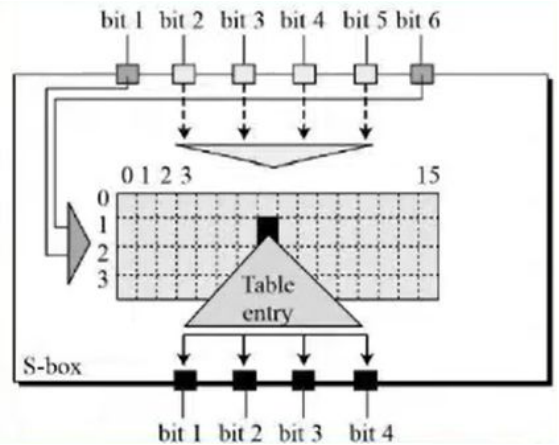
Proceso DES

Utilización de S-BOX

Consideremos el primer

grupo de 6 bits del paso anterior:

101010



Proceso DES

Utilización de S-BOX

Entrada: 101010

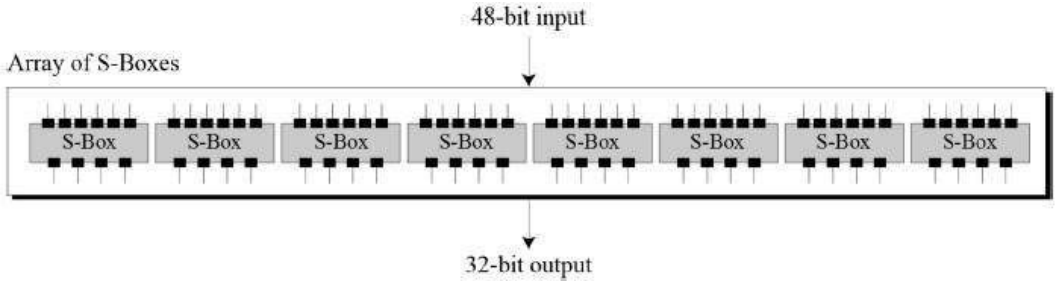
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

10=2

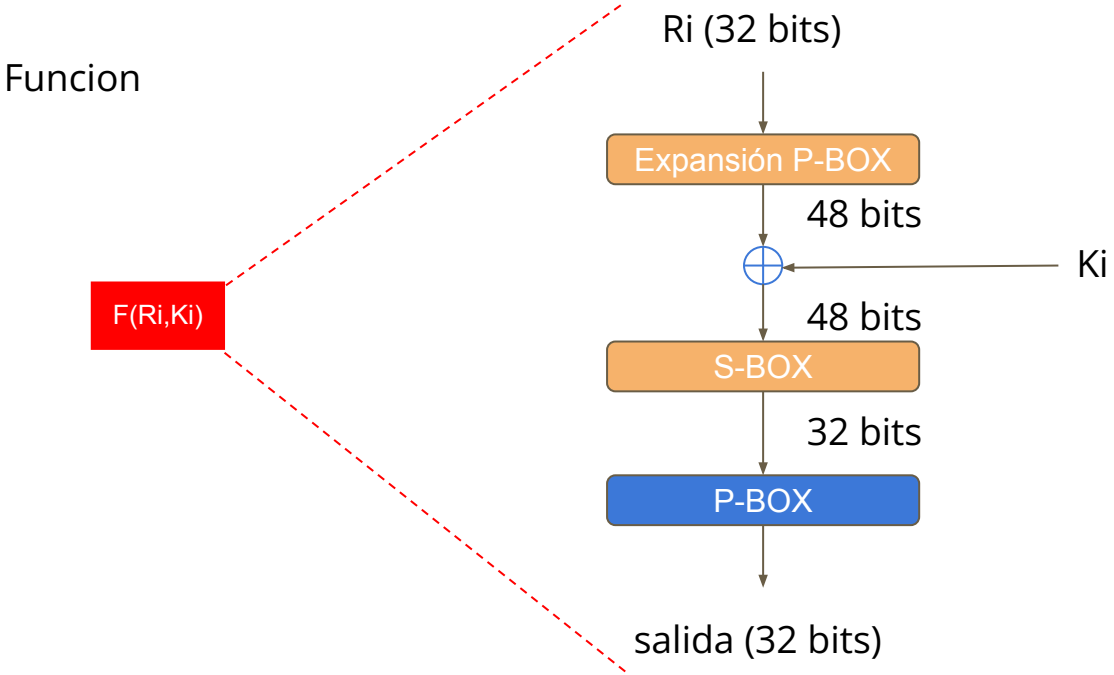
0101=5

6=0110

salida = 0110



Proceso DES


Funcion
F(Ri,Ki)
Ri (32 bits)
Expansión P-BOX
48 bits
Ki
48 bits
S-BOX
32 bits
P-BOX
salida (32 bits)

Proceso DES

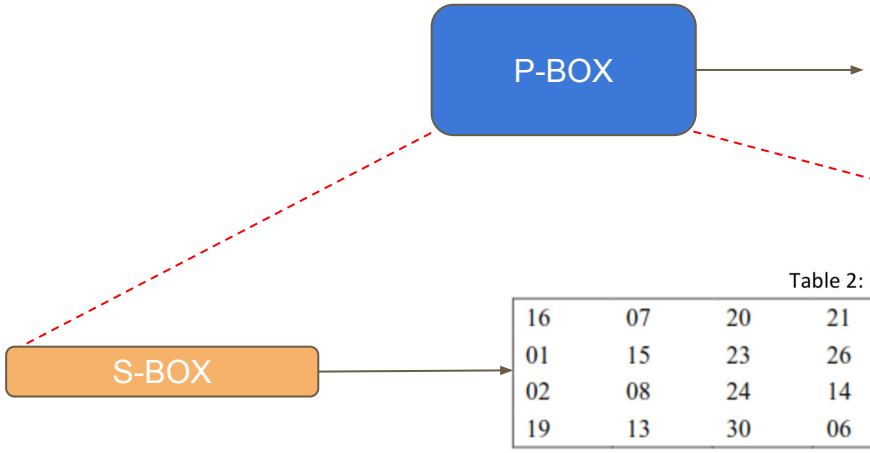


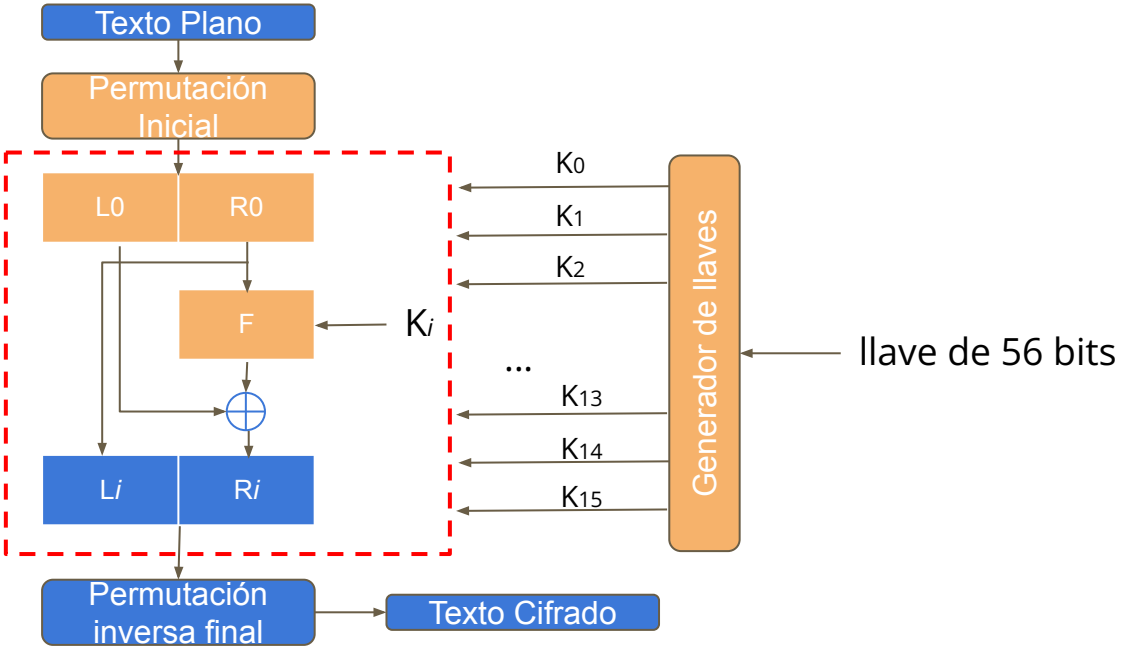
Table 2: Permutation P-Box

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

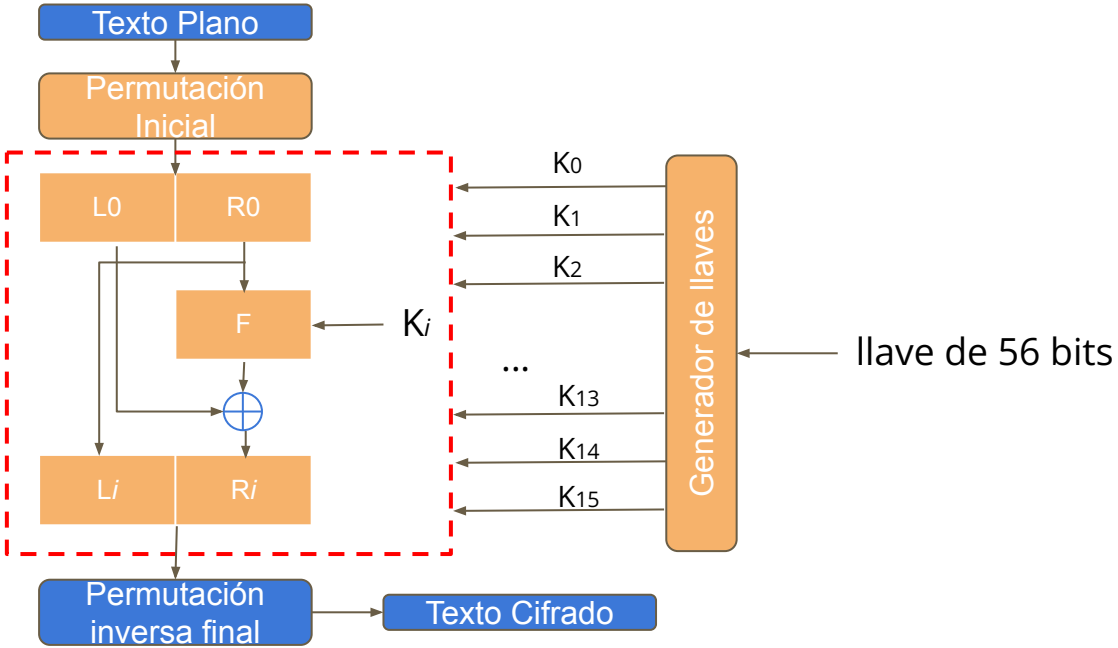
Proceso DES

Realizamos XOR entre Li y el resultado de F(Ri,Ki)

Repetimos el proceso durante 16 rondas.

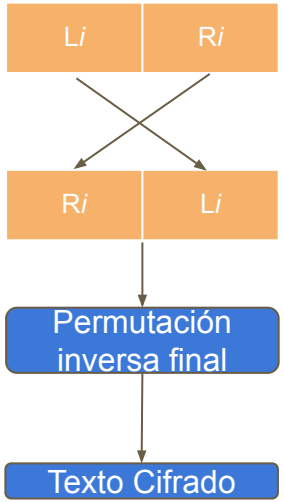


Proceso DES

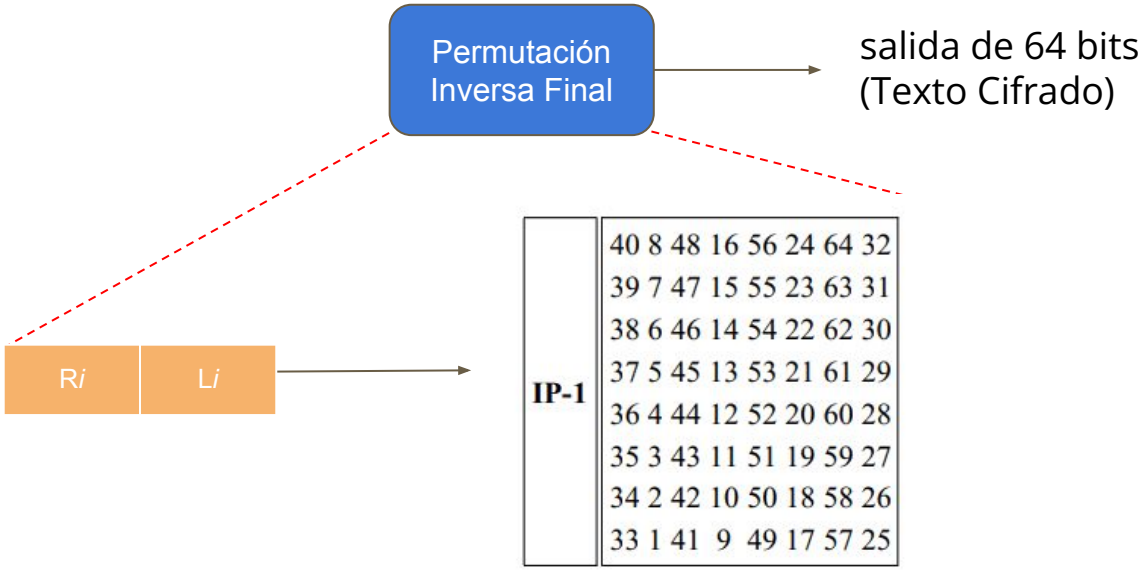

Texto Plano
Permutación Inicial
L0
R0
F
Ki
Li
Ri
K0
K1
K2
...
K13
K14
K15
Generador de llaves
llave de 56 bits
Permutación inversa final
Texto Cifrado

Proceso DES

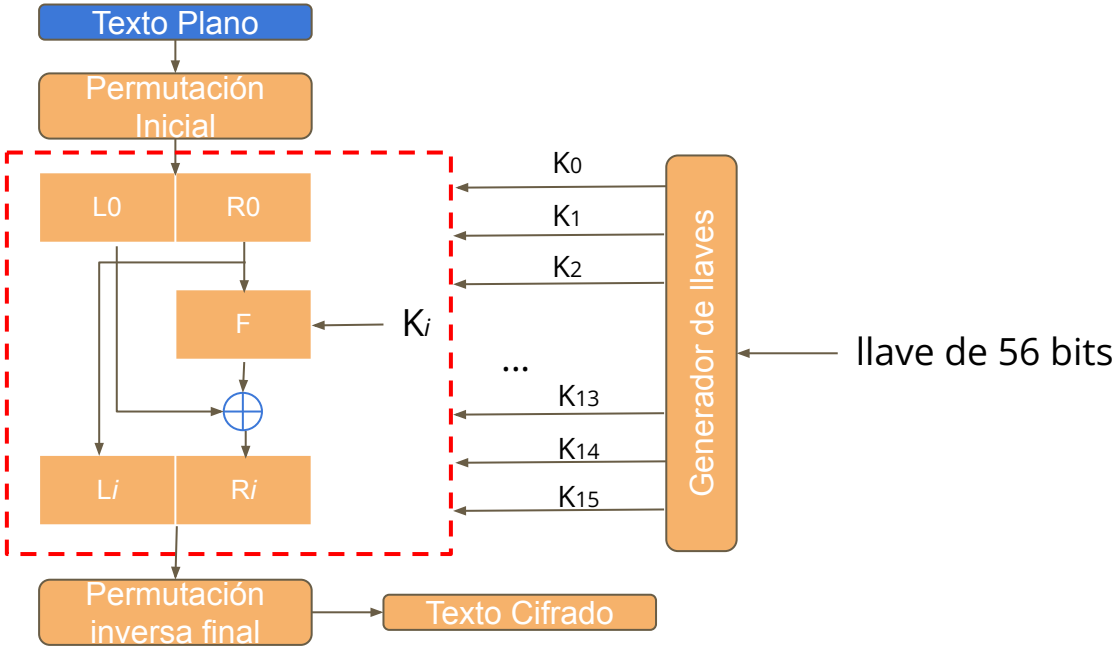
Antes de hacer la permutación inversa final se intercambia izquierda con derecha.



Proceso DES


Permutación
Inversa Final
salida de 64 bits
(Texto Cifrado)
Ri
Li
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

Proceso DES


Texto Plano
Permutación Inicial
L0
R0
F
Ki
Li
Ri
K0
K1
K2
...
K13
K14
K15
Generador de llaves
llave de 56 bits
Permutación inversa final
Texto Cifrado

Proceso DES

Descifrado