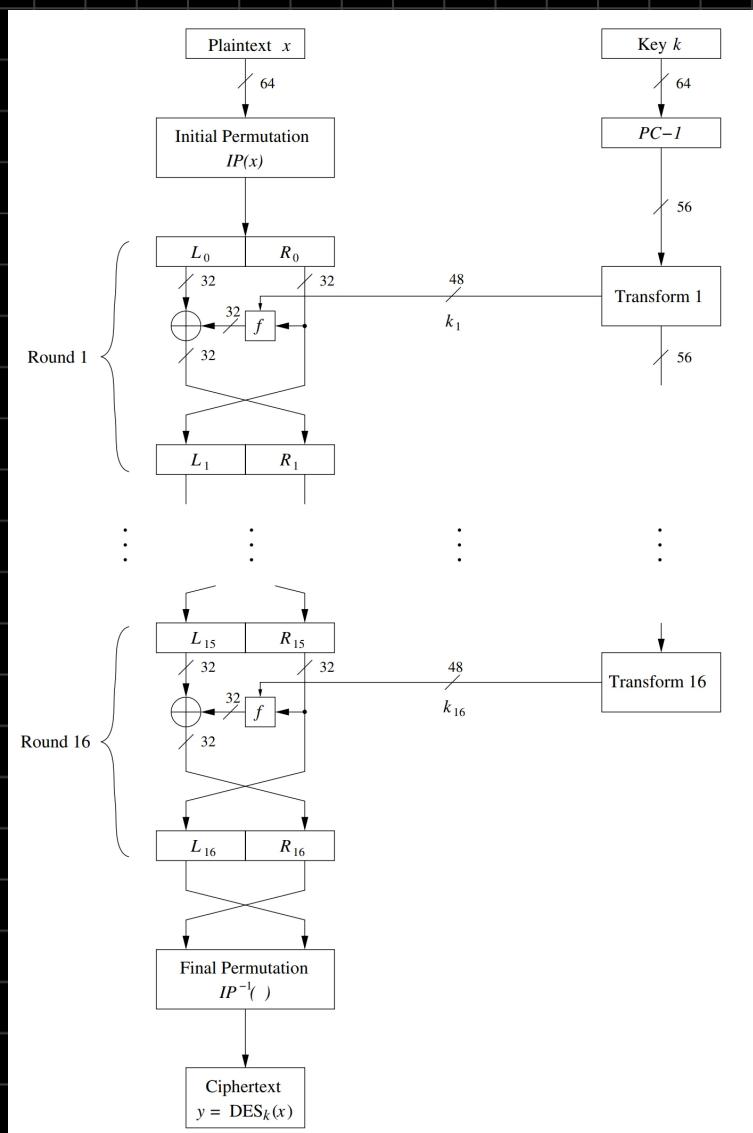


3.3. Estructura interna de DES

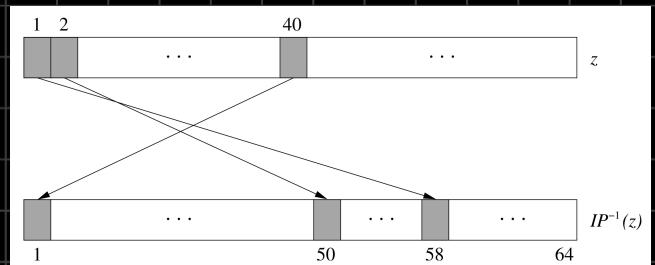
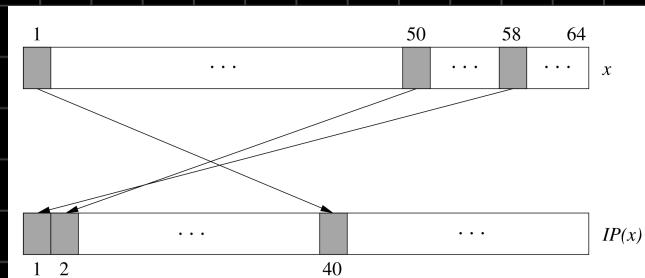
Propósito: "desmenuzar" el siguiente diagrama:



Bloques de construcción:

- Permutación inicial y final
- Rondas
- Función f
- Esquema de llaves

→ Permutación inicial y final



Estos son ejemplos de permutaciones bit a bit.



- Ambas permutaciones NO incrementan la seguridad de DES

- La razón exacta de su existencia se desconoce

↳ Parece probable que sirvieran para organizar el texto plano, el texto cifrado y los bits en forma de bytes para facilitar la búsqueda de datos para buses de 8 bits.

Table 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}

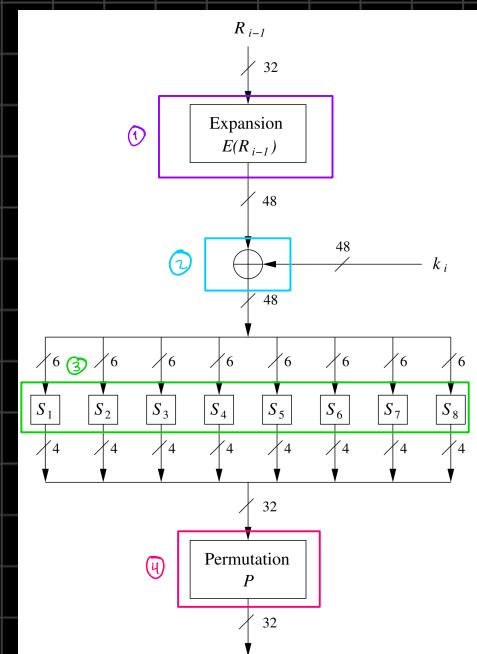
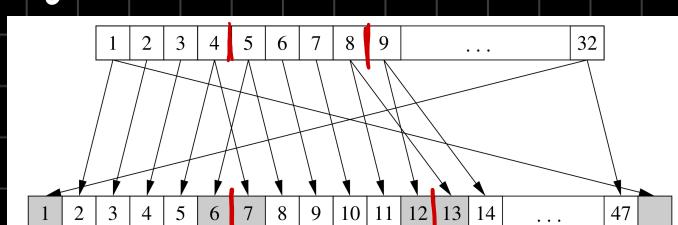
IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

→ Función f

Juega un rol fundamental en la seguridad de DES.

Paso ①: la entrada de 32 bits se expande a una de 48 bits partiendo la entrada en 8 bloques de 4 bits y éstos se expanden a 6 bits cada uno.

↳ Caja o expansión E



16 de las 32 entradas se repiten en la salida, pero ningún bit de entrada aparece dos veces en un mismo bloque de salida.

• La expansión incrementa la difusión

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1



Paso ②: el resultado de 48 bits se XORea con la llave de la ronda i , k_i .

Paso ③: los 8 bloques de 6-bits resultantes alimentan a 8 diferentes cajas de sustitución, o S-cajas

Cada S-caja es una tabla de búsqueda que manda una entrada de 6 bits en una salida de 4 bits

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
3	02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

→ Cómo leer las tablas?

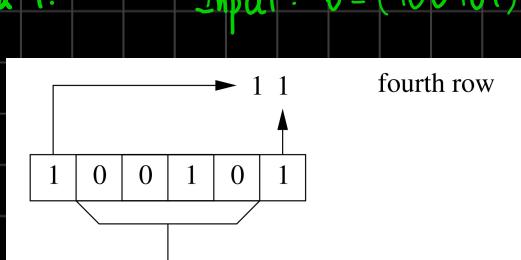
El bit más significativo (MSB) y el menos significativo (LSB) seleccionan la fila de la tabla

Los cuatro bits internos señalan la columna

Los enteros $00, \dots, 15$ de cada entrada de la tabla representan la notación decimal de un valor de 4 bits.

Ej: Usaremos la S-caja 1.

Input: $b = (100101)_2$



$$11_2 = 3 \rightarrow \text{fila } 4 \quad (\text{empezamos en } 0)$$

$$0010_2 = 2 \rightarrow \text{columna } 3 \quad (" " " ")$$

$$S_1(b) = 08 = 1000_2$$

→ Las S-cajas son el centro de la fuerza criptográfica de DES.

→ Crean confusión

→ Son el único elemento no lineal del algoritmo

→ Motivación de S-boxes (1977).  Created with Notewise

Las S-cajas fueron diseñadas por los siguientes motivos:

- ① Cada S-caja tiene entradas de 6 bits y salidas de 4 bits.
- ② Ningún bit de salida debería estar demasiado cerca de una combinación lineal de los bits de entrada.
- ③ Si los bits más bajo y más alto de la entrada se fijan y los cuatro bits de en medio varían, cada uno de los posibles valores de salida de 4 bits deben ocurrir exactamente una vez.
- ④ Si dos entradas de una S-caja difieren en exactamente un bit, sus salidas deben diferir en al menos dos bits.
- ⑤ Si dos entradas de una S-caja difieren en los dos bits del medio, sus salidas deben diferir en al menos dos bits.
- ⑥ Si dos entradas de una S-caja difieren en sus primeros dos bits y son idénticas en sus últimos dos bits, las dos salidas deben ser diferentes.
- ⑦ Para cualquier diferencia no cero entre dos entradas, no más de 8 de los 32 pares de entradas que exhiban tal diferencia puede resultar en la misma diferencia en salidas.
- ⑧ Una colisión en la salida de 32 bits de las 8 S-cajas es solamente posible para 3 S-cajas adyacentes.

Algunos de estos criterios no fueron revelados sino hasta los 90's.

→ Son los elementos más cruciales de DES pues introducen una no-linealidad al cifrado, en el sentido de que

$$S(a) \oplus S(b) \neq S(a \oplus b)$$

Además, frustran criptoanálisis diferenciales.

Paso ④: la salida de 32 bits se permuta bit a bit de acuerdo a la permutación P

→ A diferencia de las permutaciones inicial y final, P introduce difusión

↳ Los cuatro bits de salida de cada S-caja se permutan de tal forma que afectan S-cajas diferentes en la siguiente ronda.

Expansión E

S-cajas

Permutación P

}

diffusión

}

→ garantiza que cada bit al final de la ronda 5 sea función de cada bit del texto plano y cada bit de la clave.

Efecto avalancha



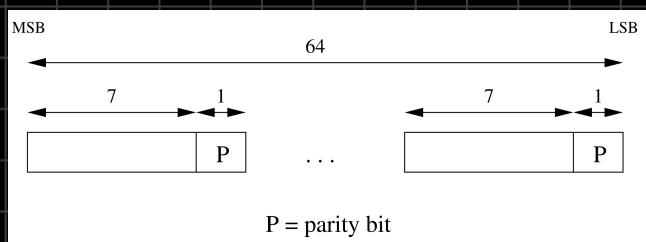
<i>P</i>
16
7
20
21
29
12
28
17
1
15
23
26
5
18
31
10
2
8
24
14
32
27
3
9
19
13
30
6
22
11
4
25

→ Esquema de Olas

Da 16 llaves k_i , una por ronda, de 48 bits cada una, todas derivadas de la original de 56 bits.

Obs. DES a menudo se afirma que es de 64 bits, donde cada octavo bit se usa como de chequeo de paridad sobre los 7 anteriores. En todo caso, dichos bits de paridad no son bits de la clave y no incrementan la seguridad.

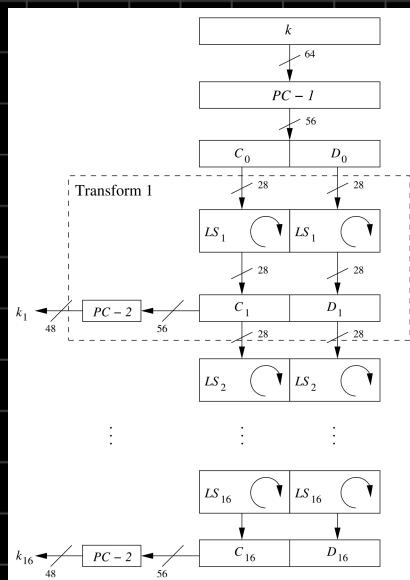
La llave de 64 bits se reduce a una de 56 bits al ignorar cada octavo bit



Los bits de paridad se quitan en la
permutación inicial PC-1
permitted choice 1

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

La llave resultante de 56 bits se divide en dos mitades, C_0 y D_0 , y el esquema de llaves empieza:



Las dos mitades de 28 bits se rotan hacia la izquierda una o dos posiciones (en bits) dependiendo de la ronda i:

- * Si $i = 1, 2, 9, 16$, las dos mitades se rotan una posición
- * Si $i \neq 1, 2, 9, 16$, las dos mitades se rotan dos posiciones

Las rotaciones sólo se hacen ya sea en la mitad de la izquierda o en la de la derecha.

El total de posiciones rotadas es $4 \cdot 1 + 12 \cdot 2 = 28$, lo que lleva a la propiedad curiosa de que
 $C_0 = C_{16}$ y $D_0 = D_{16}$
↳ útil para el descifrado

Para dar las subllaves k_i , las dos mitades se permutan bit a bit otra vez con PC - 2, que
permuta los 56 bits de entrada de C_i y D_i e ignora 8 bits.

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

El esquema de llaves es nuevamente un método para realizar sistemáticamente las 16 permutaciones

En hardware → fácil de implementar

- * Diseñado para que cada uno de los 56 bits se use en diferentes subllaves
↳ cada bit se usa aproximadamente en 14 de las 16 rondas