Universidad
Carlos III de Madrid

Grupo SeTI · Dpto. Informática

T 2 CRIPTOGRAFÍA
T 2.3 CRIPTOSISTEMAS SIMÉTRICOS. CIFRADORES DE BLOQUE Y FLUJO (parte 2)

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2016-2017

Índice

- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - Esquema de Feistel
    - Modos de operación
    - Cifradores de bloque: Ventajas y desventajas
    - **Data Encryption Standard (DES)**
    - AES
  - Cifradores de flujo

Data Encryption Standard (DES)

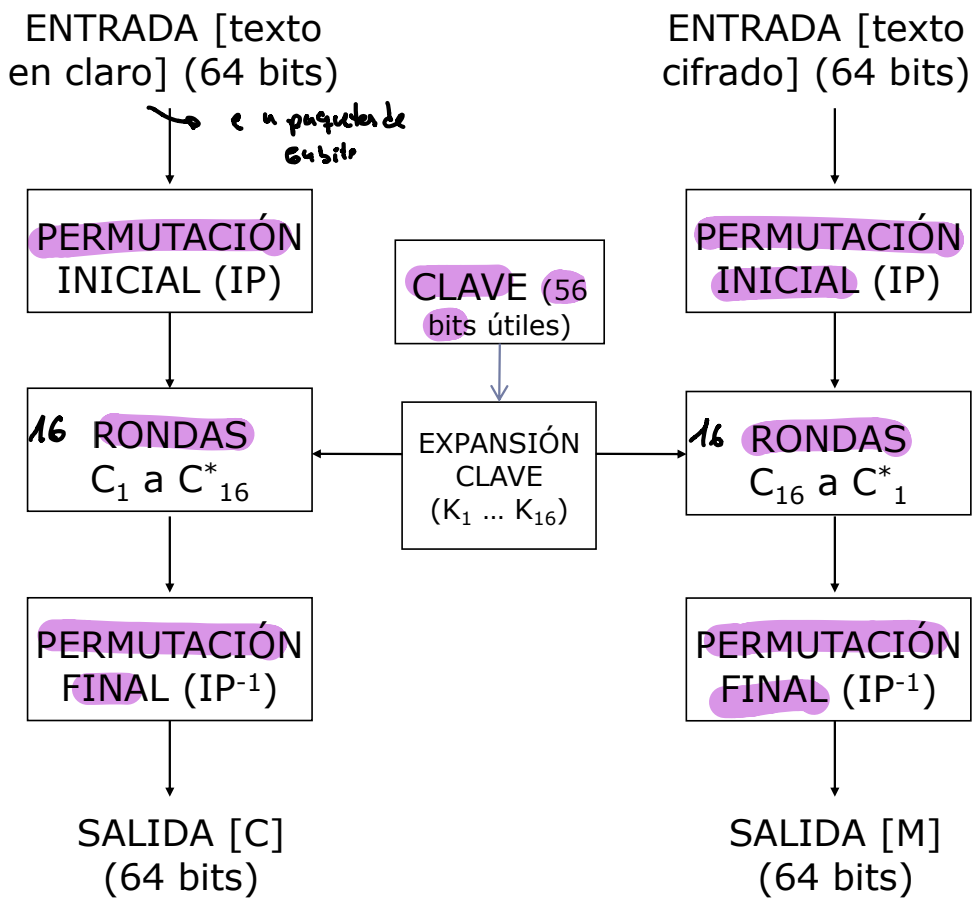
- 1973, 1974: NBS (actualmente NIST) publica sendos concursos para algoritmos de cifrado.
- 1976: IBM presenta un candidato LUCIFER, diseñado por Horst Feistel. La NSA lleva a cabo algunas modificaciones y finalmente:
- 1977: DES es publicado como estándar de cifrado (estadounidense) a nivel comercial, bancario y para comunicaciones no clasificadas a nivel gubernamental.
- 1983, 1988, 1993: Es repetidamente confirmado como estándar de cifrado.
  - Longitud de clave inadecuada de 56 bits ~ por la NSA
  - Falta de transparencia sobre diseño
    - Sospechas de la existencia de una puerta trasera para la National Security Agency (NSA)

Data Encryption Standard (DES)

- 1990: Criptoanálisis diferencial (Biham and Shamir)
  - Cifrar 2^{47} textos en claro escogidos
- 1993: Criptoanálisis lineal (Matsui)
  - Cifrar 2^{43} textos en claro conocidos
- 1998: DES Cracker de la Electronic Frontier Foundation (EFF)
  - Descifra un mensaje DES en 56 horas
  - Usando 1536 chips especializados
  - Menos de $250K, menos de 1 año para construirlo
- 1999: DES Cracker version 2
  - Descifra un mensaje DES en 22 horas
  - Combina 100K PCs
- 1999: Se establece el Triple DES como el estándar, dejando el DES para los sistemas heredados.
- **2001: El DES es sustituido por el AES (Advanced Encryption Standard)**

DES: Esquema de cifrado y descifrado

- Clave: 64 bits
  - (8 de paridad)
- Bloque: 64 bits
- Rondas: 16
  - La última requiere una permutación adicional (*)
- Claves internas:
  - 16 de 48 bits
- Bases matemáticas:
  - sustituciones
    - lineales
    - no lineales
  - permutaciones



Índice

- (…)
- Data Encryption Standard (DES)
  - **Cifrado**
  - Expansión de la clave
  - Descifrado
  - Triple DES
  - Seguridad
- AES
- (…)

DES: Descripción del algoritmo

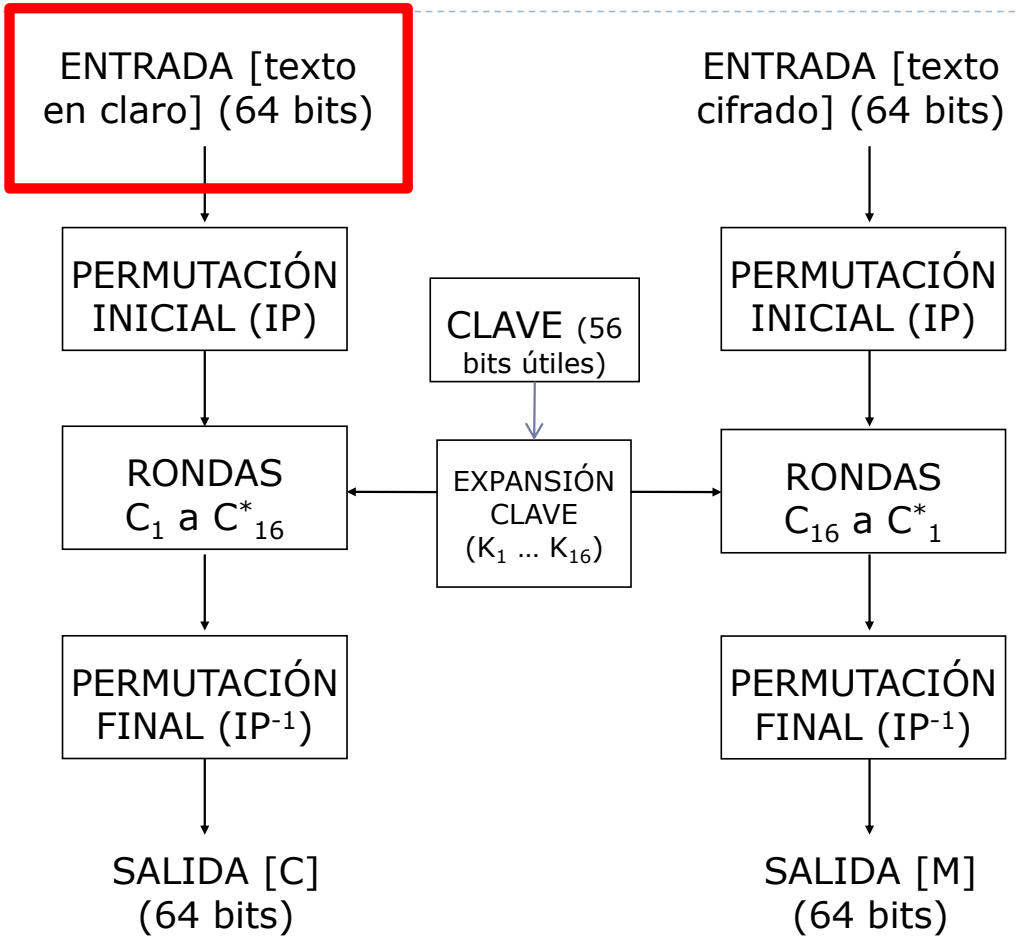
Texto en claro

1.- Selección del bloque M a cifrar

2.- Disposición de los 64 bits del bloque de Texto en claro

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

“Mapa de situación”



DES: Descripción del algoritmo

Del Texto en claro a la Permutación Inicial, IP

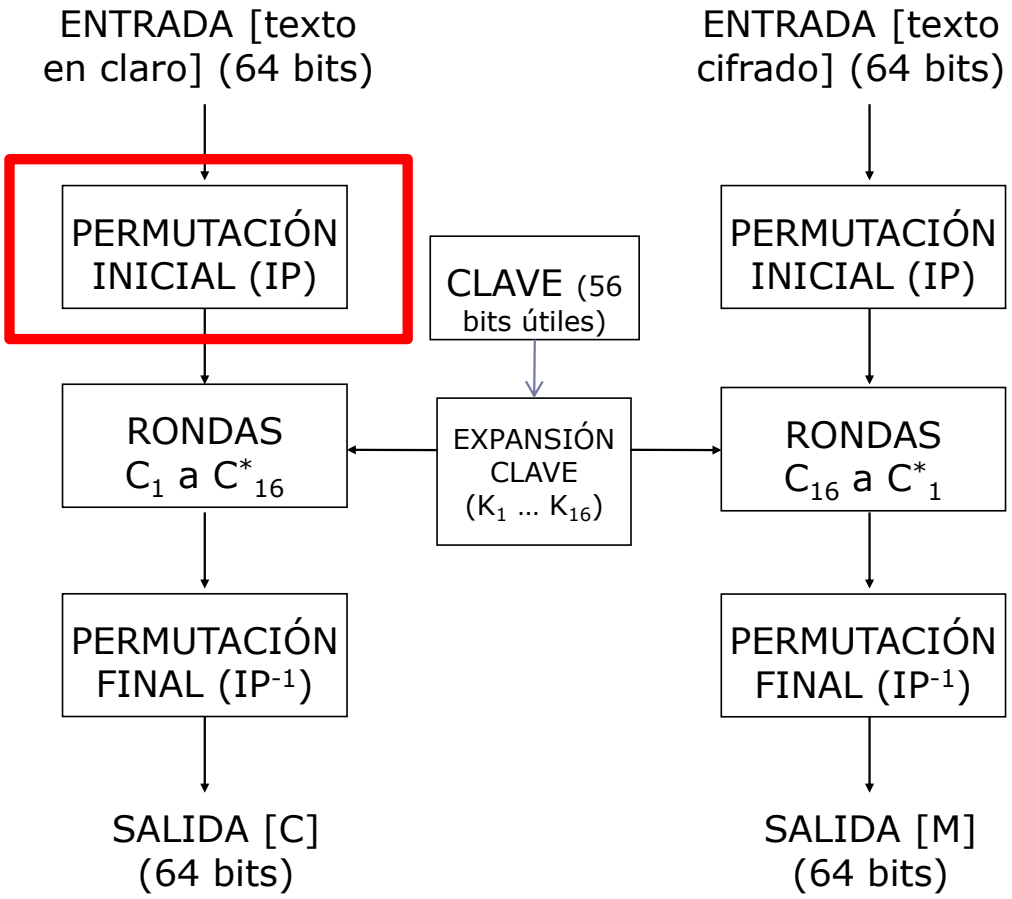
3.- Permutación inicial, IP

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

Paren

Impares

“Mapa de situación”



DES: Descripción del algoritmo

- **Operaciones previas a la entrada al primer ciclo**

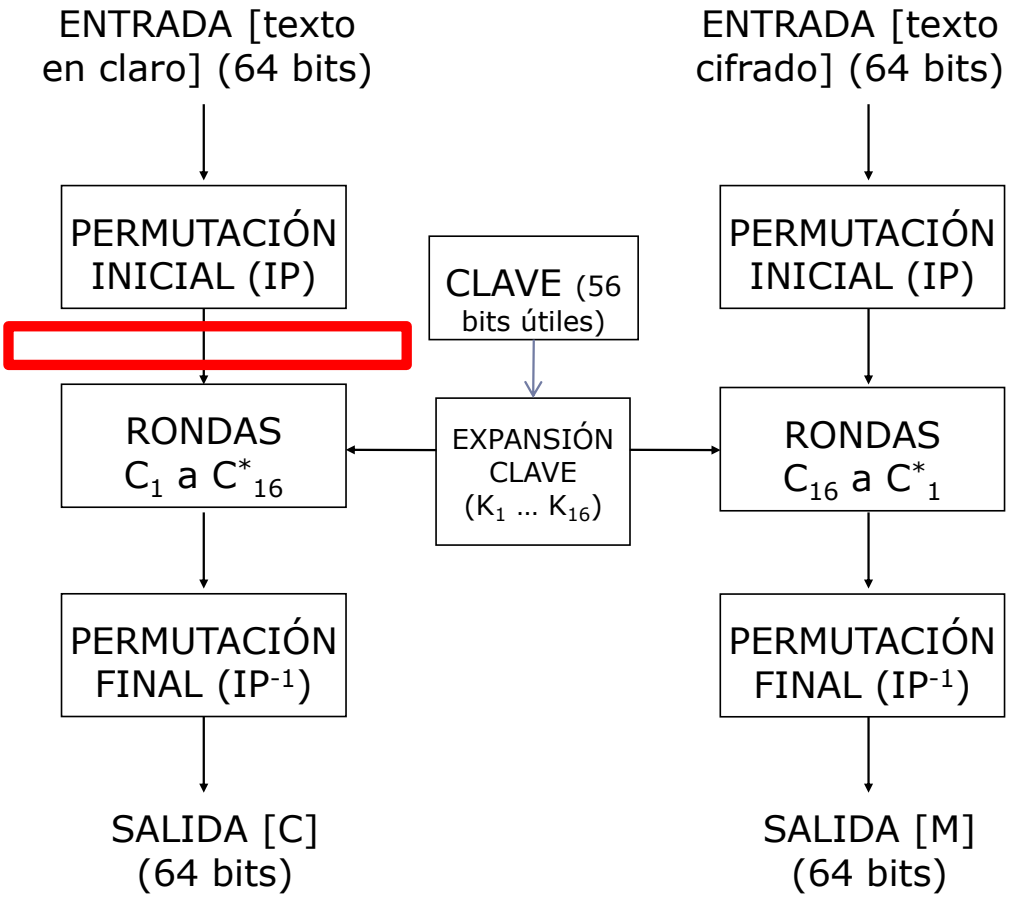
4.- Obtención de subbloques izquierdo, L_0, y derecho, R_0, de 32 bits

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

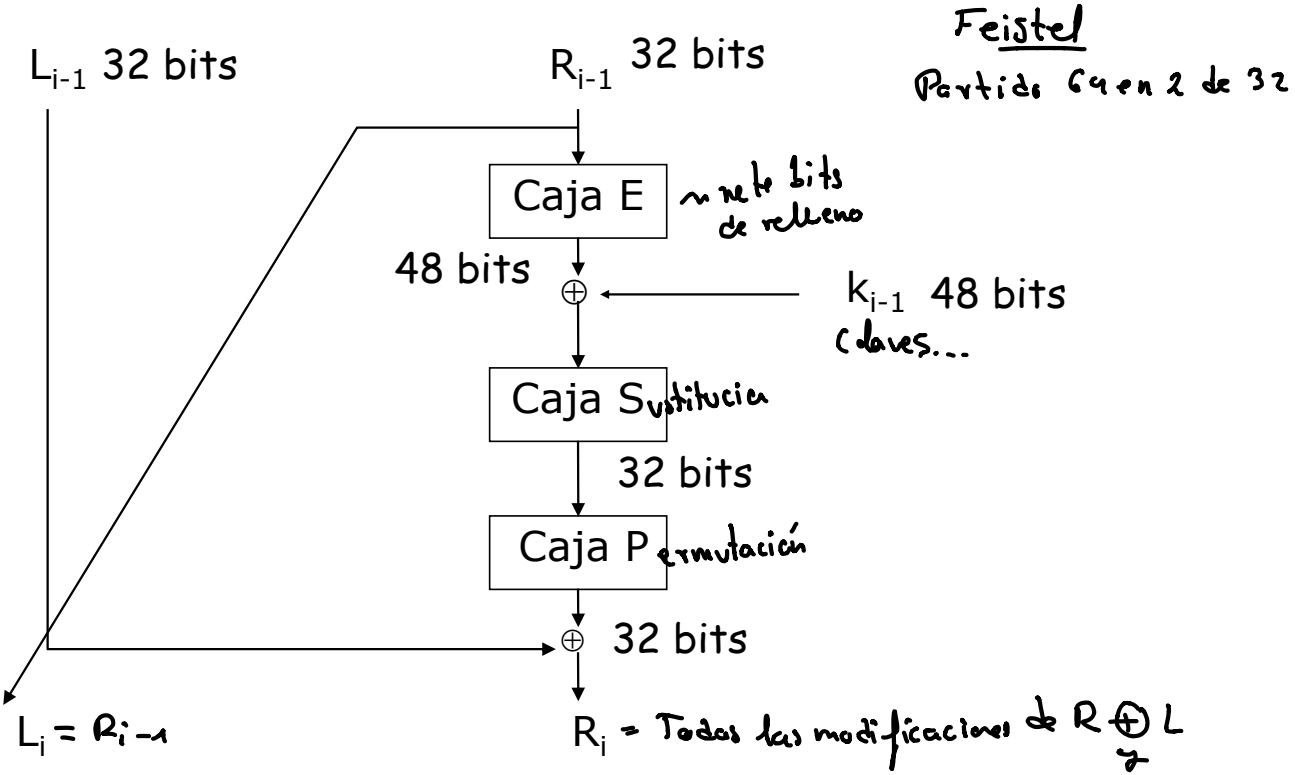
L_0 = 58 50 42 34 26 18 10 02 60 52 44
36 28 20 12 04 62 54 46 38 30 22 14
06 64 56 48 40 32 24 16 08

R_0 = 57 49 41 33 25 17 09 01 59 51
43 35 27 19 11 03 61 53 45 37 29 21
13 05 63 55 47 39 31 23 15 07

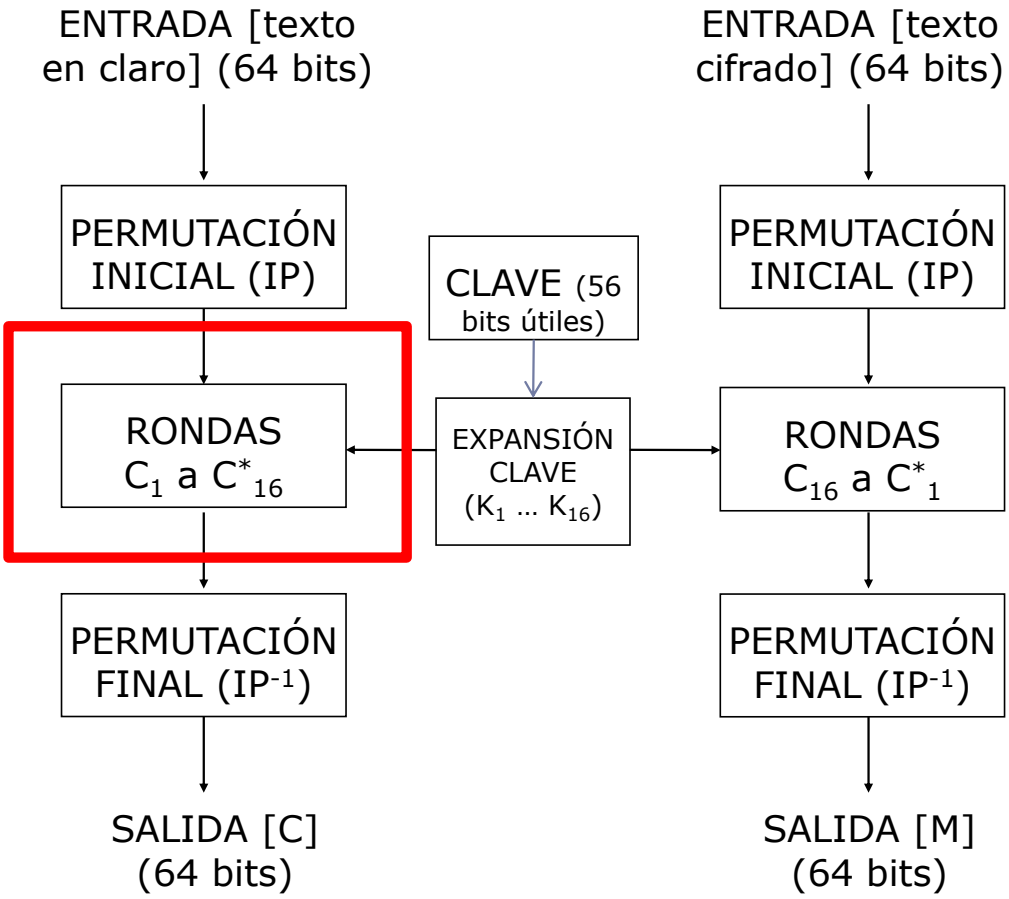
“Mapa de situación”



DES: Esquema de cada ronda

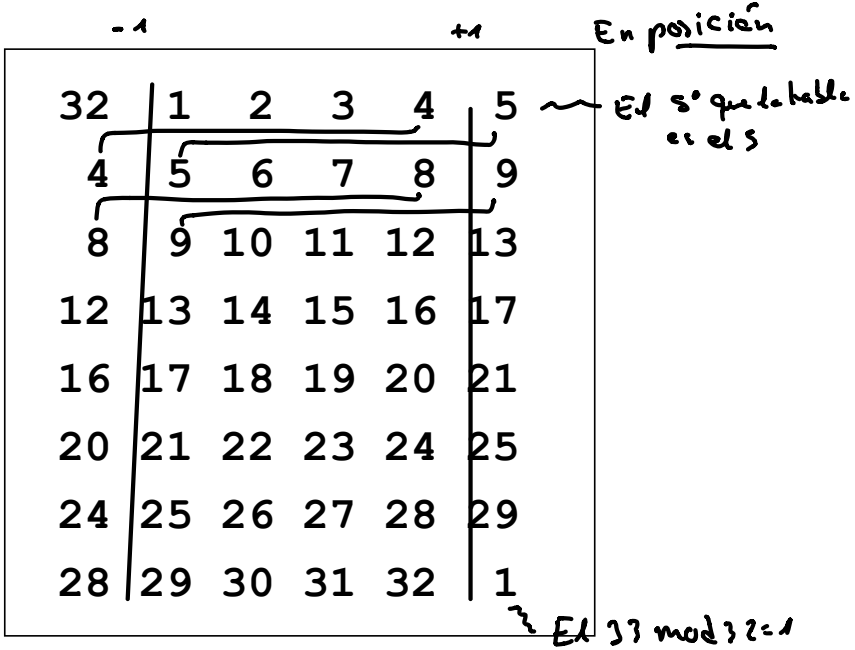


“Mapa de situación”

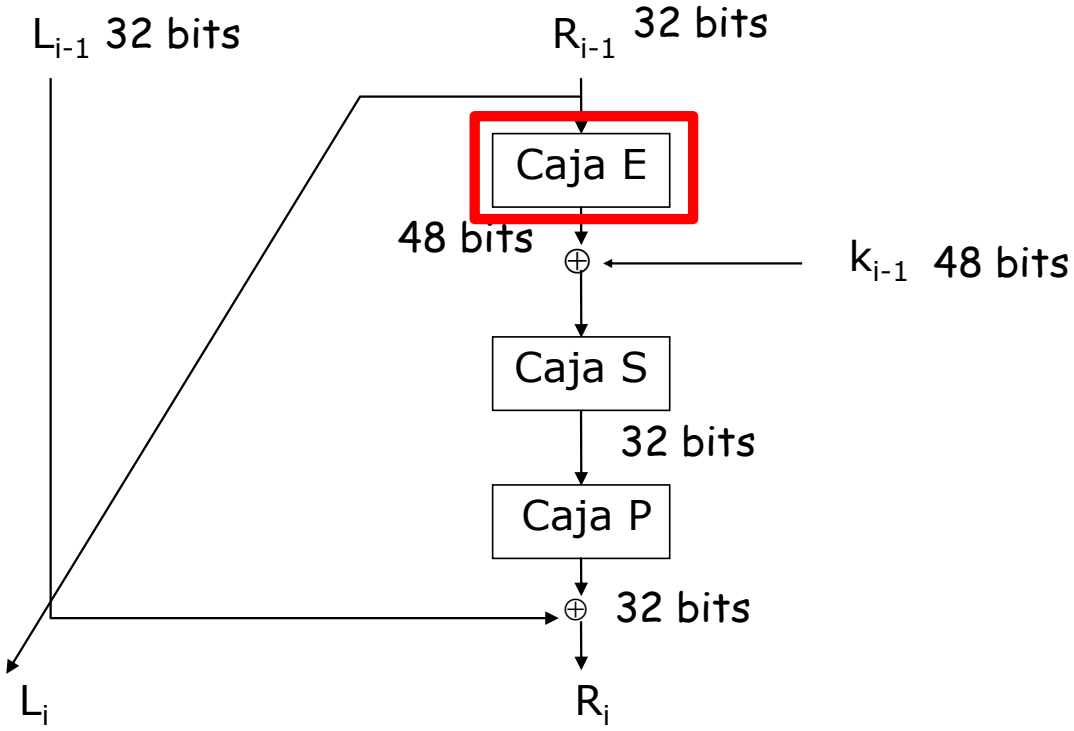


DES: Caja E

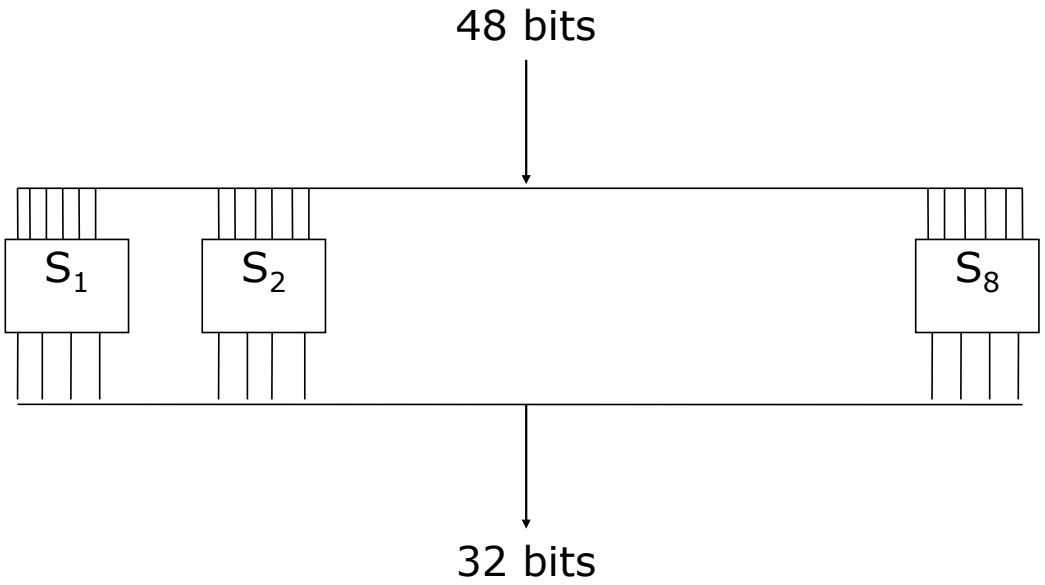
- De 32 bits a 48 bits (PERMUTACIÓN EXPANDIDA)



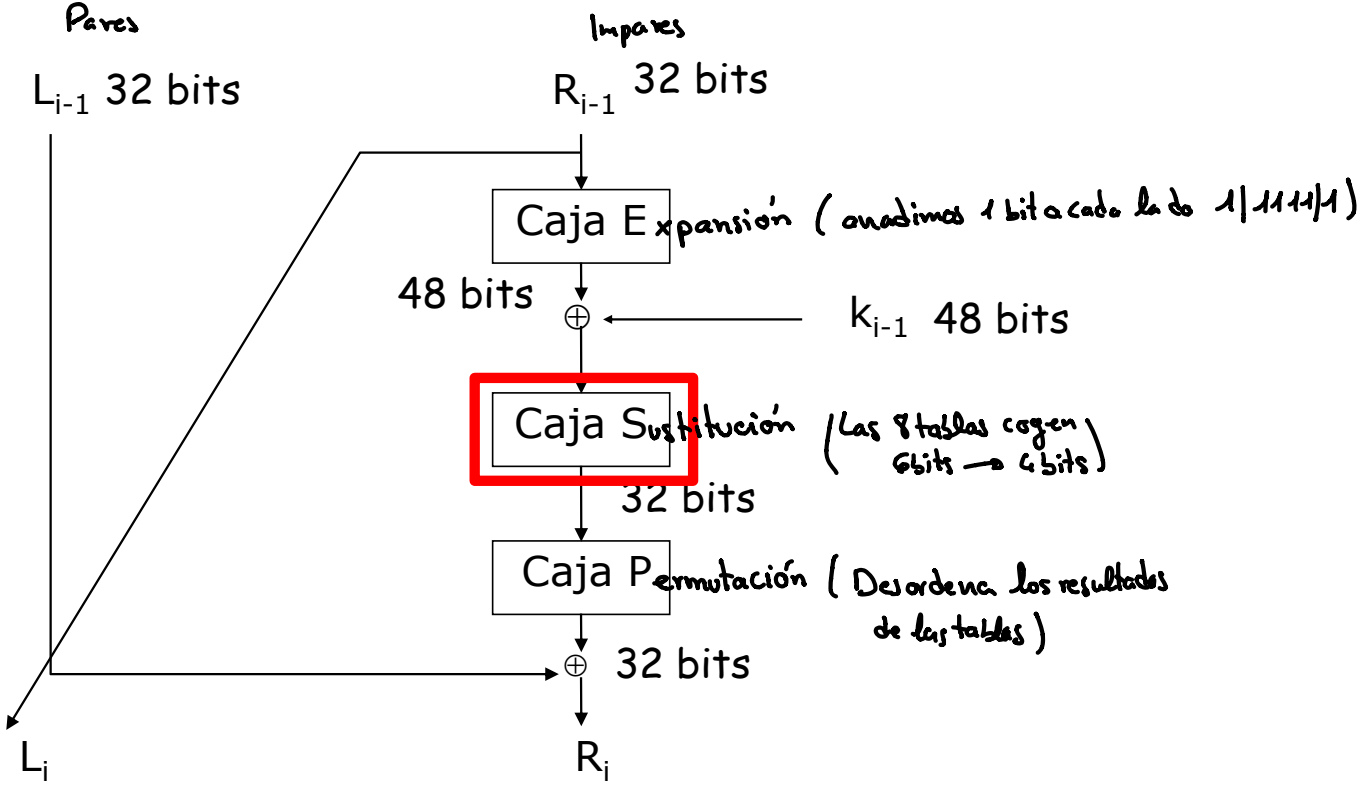
“Mapa de situación” -- RONDA



DES: Esquema de las cajas S



“Mapa de situación” -- RONDA



DES: Esquema de las cajas S

La caja S está compuesta por ocho matrices $S_1, S_2, ..., S_8$, donde cada S_i toma como entrada seis bits consecutivos $b_0, b_1, ..., b_5$

Nº	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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

Caja S_1

- Los dos bits b_0 b_5, en decimal, especifican la fila de la matriz S_i
- Los cuatro bits b_1 b_2 b_3 b_4, igualmente en decimal, expresan la columna de S_i
- La intersección de fila y columna en S_i, pasado ahora a binario, constituye la salida, que se trata de un número de cuatro bits

Ejemplo: usando S_1, si la entrada fuera 110011, se trataría de la fila 3 (11) y columna 9 (1001), cuya salida, 11, serían los bits 1011

DES: Esquema de las cajas S

S_1

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

S_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

S_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

S_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

DES: Esquema de las cajas S

S_5

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

S_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

S_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

S_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

DES: Caja P

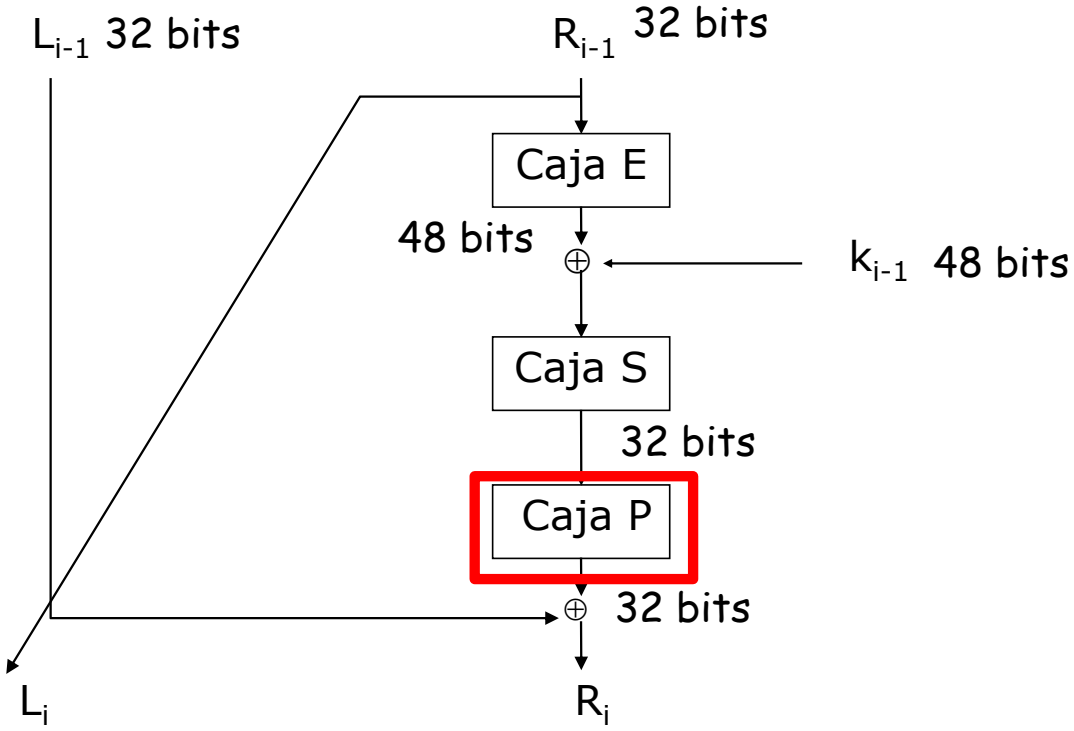
- De 32 bits a 32 bits

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

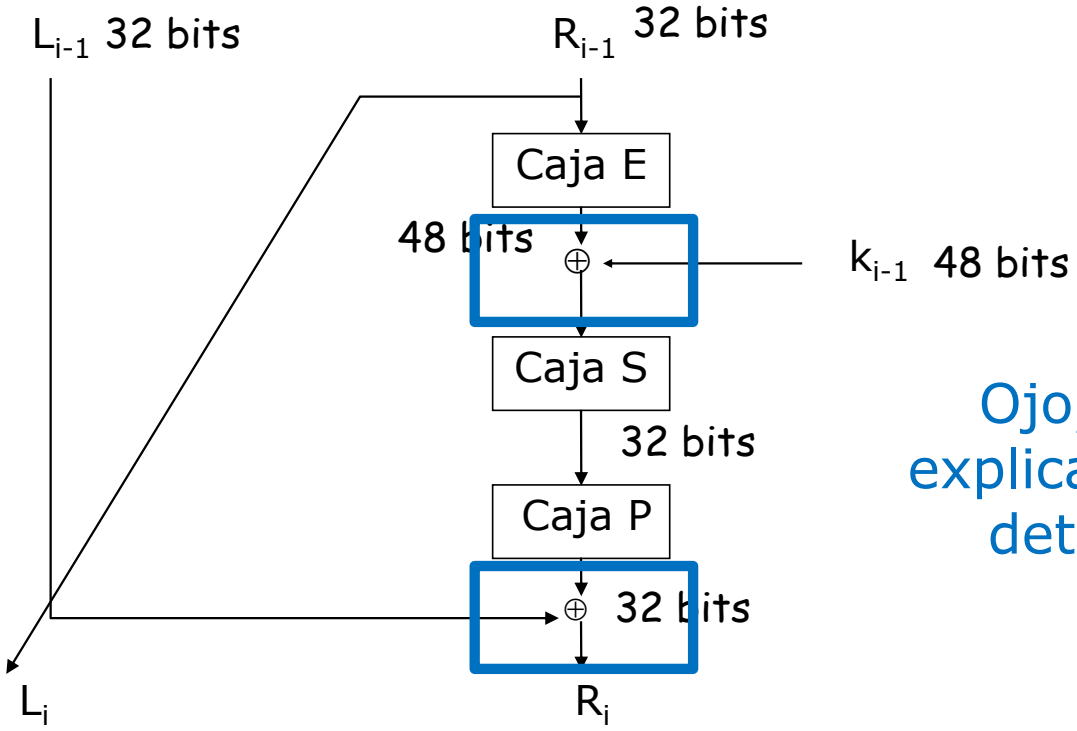
Desordenar los posiciones como indica la tabla

El 16 a la 1ª pos.

“Mapa de situación” -- RONDA



“Mapa de situación” -- RONDA

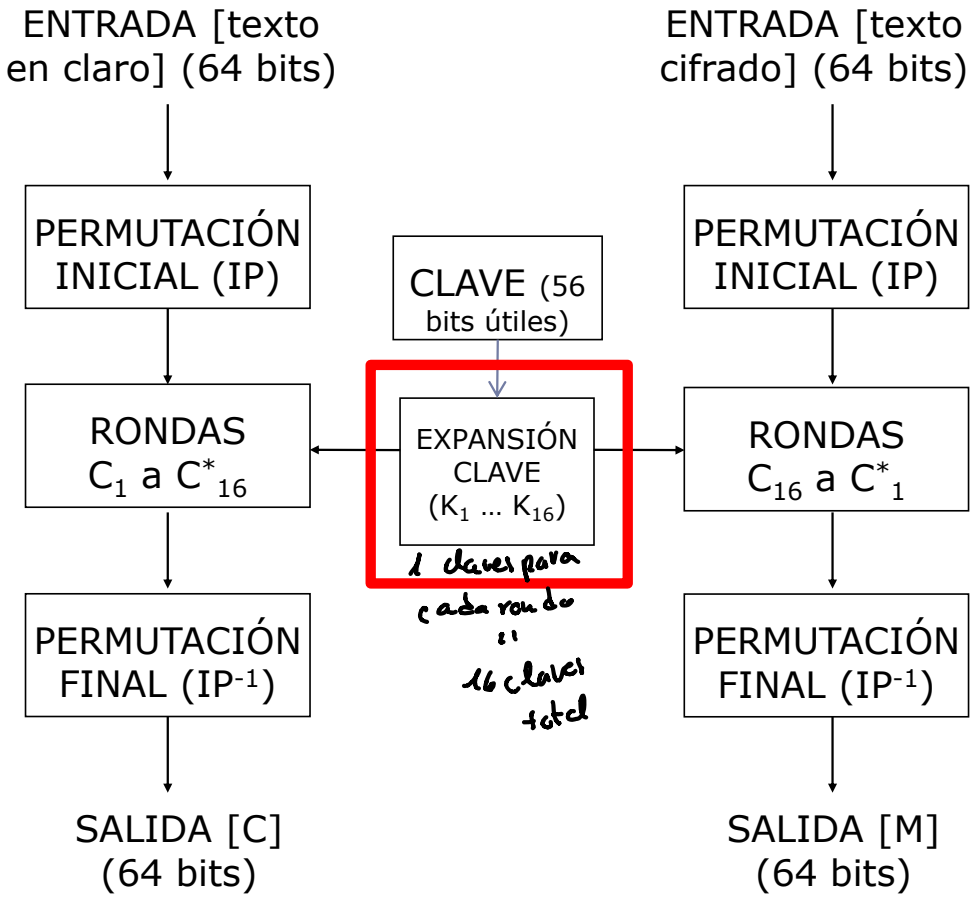


Ojo, no explicado en detalle

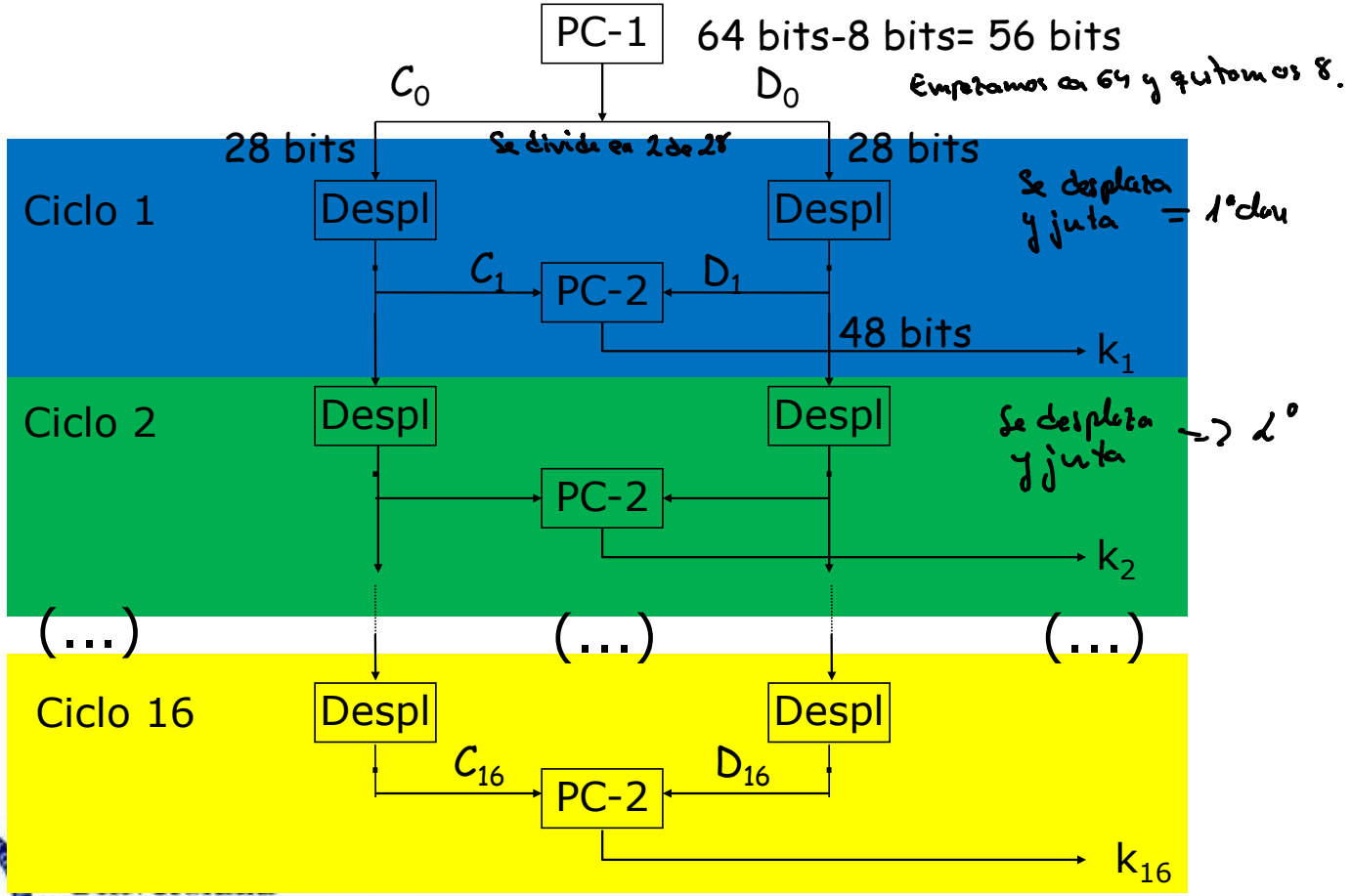
Índice

- (…)
- Data Encryption Standard (DES)
  - Cifrado
  - **Expansión de la clave**
  - Descifrado
  - Triple DES
  - Seguridad
- AES
- (…)

“Mapa de situación”



DES: Esquema de obtención de las claves internas



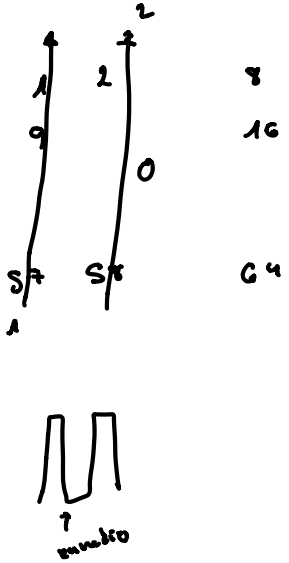
DES: Expansión de la clave

1. Permutación comprimida PC-1 de la clave: transponer orden y eliminar bits de paridad => 56 bit.
2. División en dos bloques de 28 bits.
3. i=1
4. Desplazamiento circular hacia izquierda de cada bloque (1 o 2 bits en función del ciclo [del valor de i])
5. Obtención clave interna k_i:
    1. Concatenación de los 2 bloques => 56 bit.
    2. Permutación comprimida PC-2 => 48 bit = clave interna k_i.
    3. i= i +1
    4. Vuelvo al paso 4 mientras i<=16

- Resultado: 16 claves internas de 48 bits
- En el cifrado se utilizan en el orden $k_1 – k_{16}$ (y en el descifrado en orden inverso $k_{16} – k_1$)

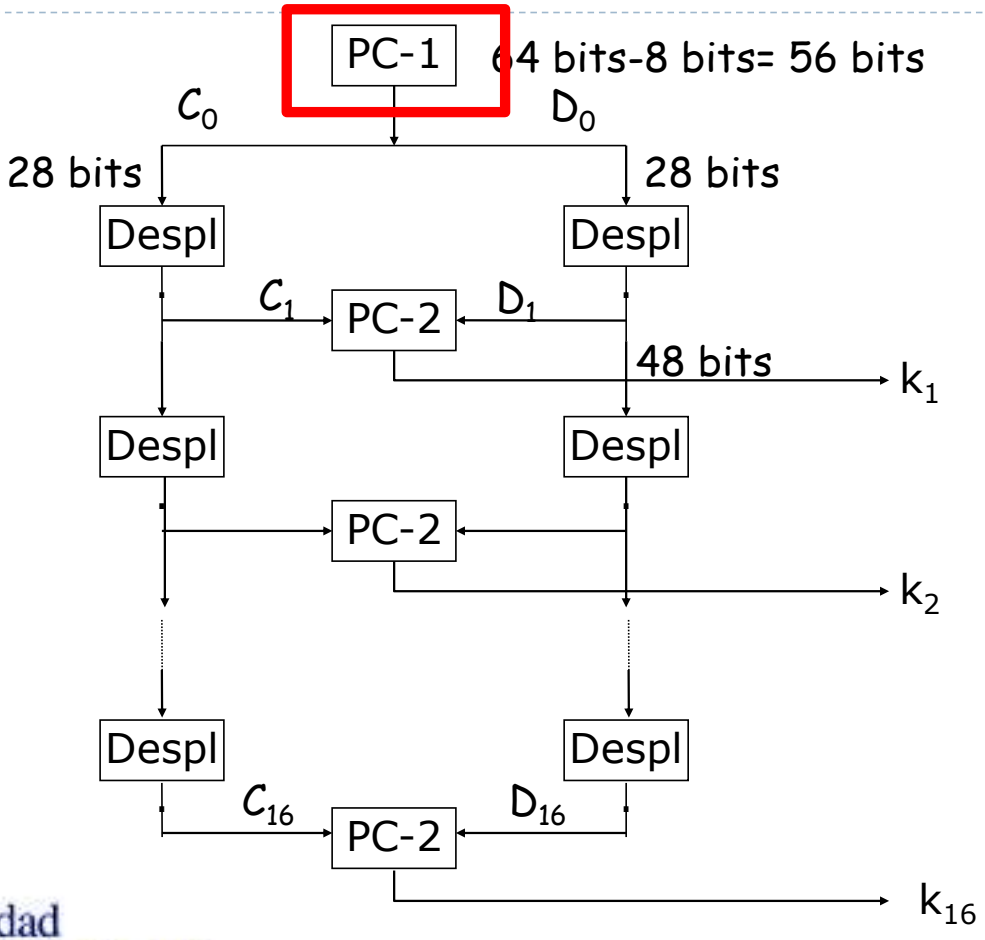
DES: Permutación PC-1

- De 64 a 56 bits



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

“Mapa de situación” – CLAVES INTERNAS



DES: Permutación PC-1

- En el primer proceso, PC-1 actúa como dos subbloques, C_0 y D_0

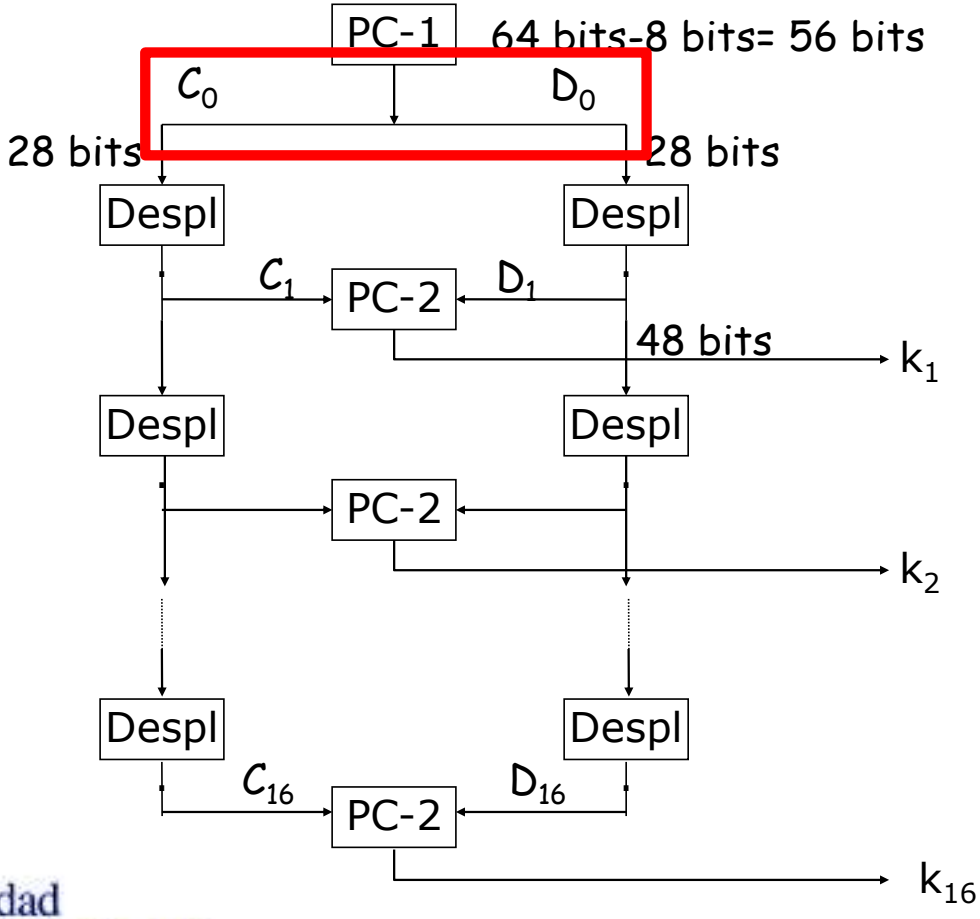
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

Bloque C_0

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

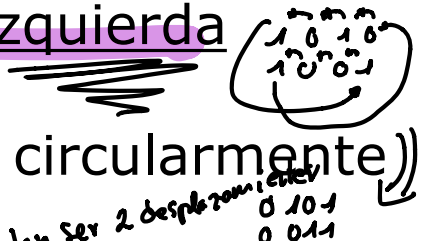
Bloque D_0

“Mapa de situación” – CLAVES INTERNAS



DES: Desplazamiento

- En cada uno de los siguientes ciclos se va obteniendo una nueva entrada a PC-2, desdoblada en los correspondientes bloques C_i y D_i , que se obtienen de los anteriores bloques C_{i-1} y D_{i-1} por un desplazamiento (rotación) circular a la izquierda

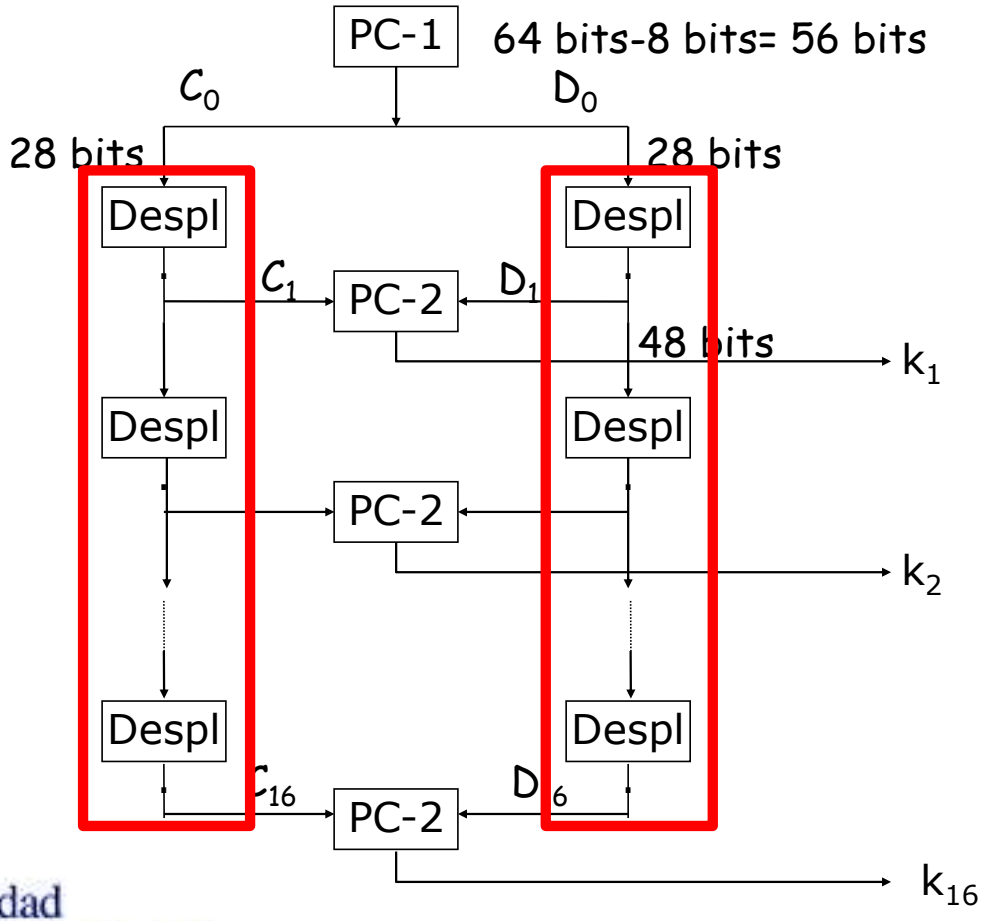


- El número de bits desplazados circularmente (rotados), en función del ciclo, es:

Pueden ser 2 desplazamientos: 1 0 1 0 1 0 1 1

Ciclo nº	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits a desplazar	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

“Mapa de situación” – CLAVES INTERNAS



DES: Permutación PC-2

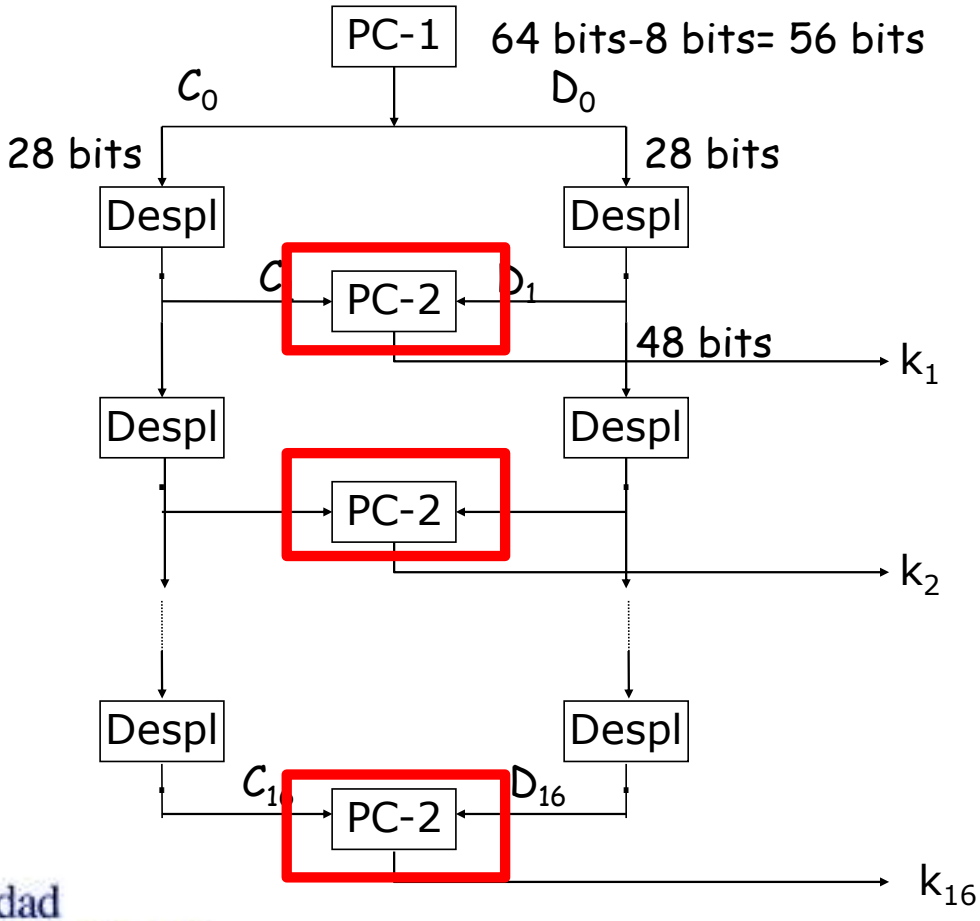
- Los dos bloques se concatenan para, a partir de los 56 bits, someterse a una nueva permutación comprimida PC-2, de la que desaparecen 8 bits y los restantes 48 cambian de posición

- De 56 a 48 bits

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

Indican posición

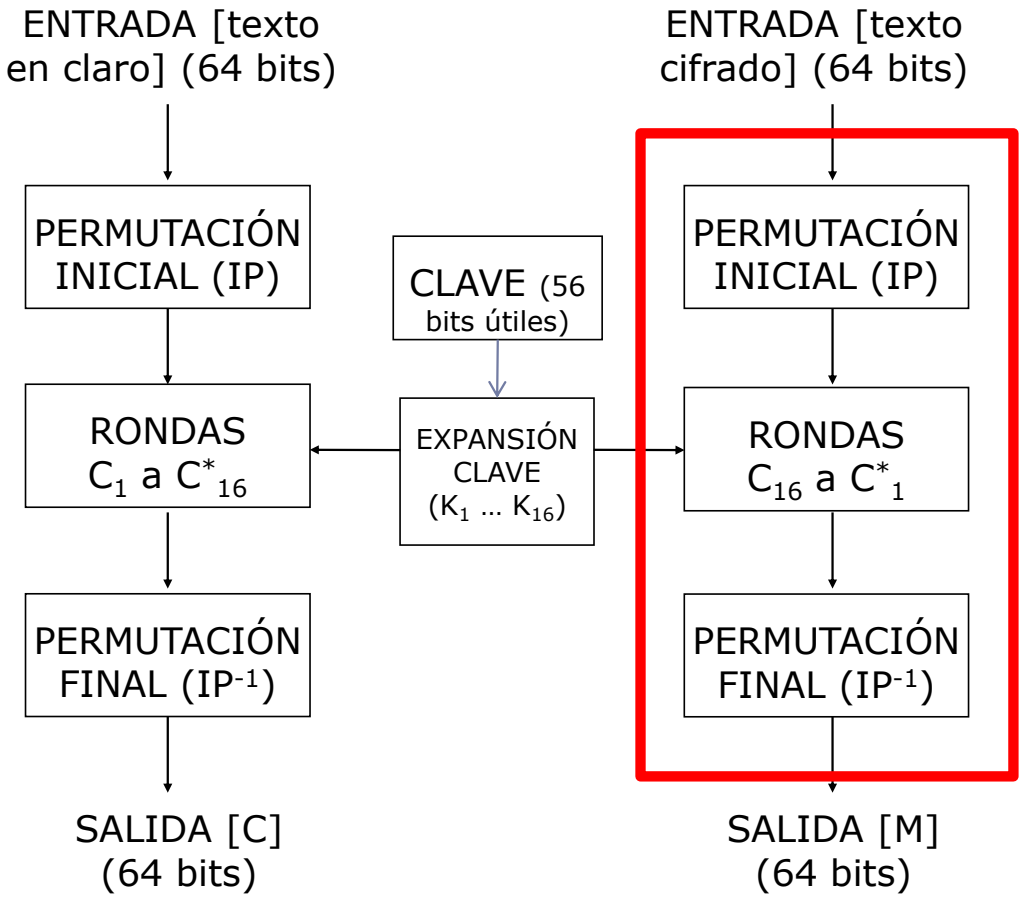
“Mapa de situación” – CLAVES INTERNAS



Índice

- (…)
- Data Encryption Standard (DES)
  - Cifrado
  - Expansión de la clave
  - **Descifrado**
  - Triple DES
  - Seguridad
- AES
- (…)

“Mapa de situación”



Descifrado DES

- Mismo algoritmo con 2 modificaciones:

1. Las claves internas se aplican en orden inverso
   1. De k_{16} a k_1

Desplazamiento a la derecha ahora

2. Si se desea generar las claves en ese orden a partir de k, se puede utilizar el mismo algoritmo de expansión de claves pero hay que recorrerlo "subiendo" (en lugar de "bajando") y considerar que:
   2. Tras realizar PC-1, $C_0=C_{16}$ y $D_0=D_{16}$
   3. Los desplazamientos que se aplican a los bloques C_i y D_i se deben realizar hacia la derecha (en lugar de hacia la izquierda)

Índice

- (…)
- Data Encryption Standard (DES)
  - Cifrado
  - Expansión de la clave
  - Descifrado
  - **Triple DES**
  - Seguridad
- AES
- (…)

Cifrado múltiple con DES

- Cuando un sistema de cifrado cumple que el cifrado de un mensaje con una clave K1 y el cifrado del resultado con otra clave K2 es equivalente a cifrar el mensaje original con una clave K3, decimos que el sistema es un grupo.
  - Ej.: Cifrado monoalfabeto por desplazamiento puro con claves B y C – equivale a cifrado con clave D
- En este caso, realizar cifrado múltiple no significa aumentar el tamaño efectivo de la clave, no teniendo sentido práctico el uso del cifrado múltiple.
- DES no es grupo, por lo tanto sí tiene sentido realizar cifrado múltiple usando este sistema como base.

Triple DES (TDES)

- 3 DES con 2 claves (2TDES) => clave de 112 bit
  - $C = E(k_1, D(k_2, E(k_1,M)))$
  - Compatibilidad con simple DES si $k_1 = k_2$
    Suficiente
- 3 DES con 3 claves (3TDES)
  - $C = E(k_3, D(k_2, E(k_1,M)))$
  - Apenas usado ya que triple DES con 2 claves suficiente

1º mensaje con 1ª clave
Mensaje cifrado con 2ª clave

Índice

- (…)
- Data Encryption Standard (DES)
  - Cifrado
  - Expansión de la clave
  - Descifrado
  - Triple DES
  - **Seguridad**
- AES
- (…)

Seguridad

- Ataques al DES
  - Fuerza bruta
    - Roto en menos de un día con HW especializado http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html
  - Criptoanálisis diferencial (necesita 2^{49} textos en claro elegidos y sus correspondientes cifrados)
  - Criptoanálisis lineal (necesita 2^{49} textos en claro conocidos y sus correspondientes cifrados)
- Ataques al Triple DES
  - El ataque "Meet-in-the-middle" y ataques de textos en claro conocidos o elegidos reducen el tamaño efectivo de la clave

meterse en el proceso y alterar las claves desde dentro

Índice

- Métodos de cifra moderna
- Criptosistemas simétricos
  - Cifradores de bloque
    - Introducción
    - Esquema de Feistel
    - Modos de operación
    - Cifradores de bloque: Ventajas y desventajas
    - Data Encryption Standard (DES)
    - **Advanced Encryption Standard (AES)**
  - Cifradores de flujo

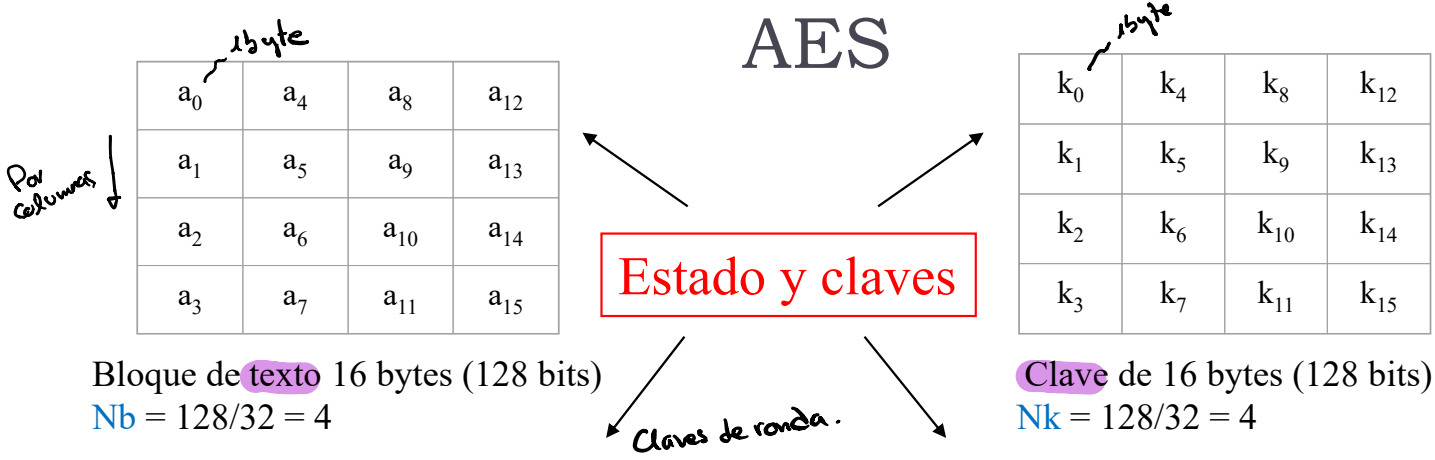
AES (Advanced Encryption Standard)

- 1976: Se adopta el DES como estándar
- 2001: NIST elige RIJNDAEL (Vincent Rijmen y Joan Daemen) como el *Avanced Encryption Standard (AES)* para:
  - Comunicaciones gubernamentales
  - Transferencia de fondos bancarios
  - Comunicaciones civiles por satélite
  - Software de libre distribución
  - Seleccionado y criptoanálizado analizado de manera pública. Toda la comunidad criptográfica mundial participó en su estudio

AES. Características

- Implementa criptografía simétrica
- Cifrador de bloque
  - Opera sobre bloques de 16 bytes (128 bits) Su unidad es el byte.
- Acepta tres longitudes de claves: 128, 192, 256 bits
  - Se generan subclaves o claves internas de 128 bits
- Es una red de sustitución-permutación, no una red Feistel (No divide y opera.)
- Es rápido tanto en software como en hardware, fácil de implementar y requiere poca memoria
- Se basa en cuatro funciones invertibles, aplicadas en un número determinado de rondas, a los bytes de una matriz llamada *Estado* (Para descifrar se siguen las funciones inversas.)
- La matriz *Estado* se carga inicialmente con los bytes del bloque de entrada ⊕ la primera de las subclaves generadas (128 bits)

AES. Estado de entrada y claves del AES



a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

Bloque de texto 16 bytes (128 bits)
Nb = 128/32 = 4

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

Clave de 16 bytes (128 bits)
Nk = 128/32 = 4

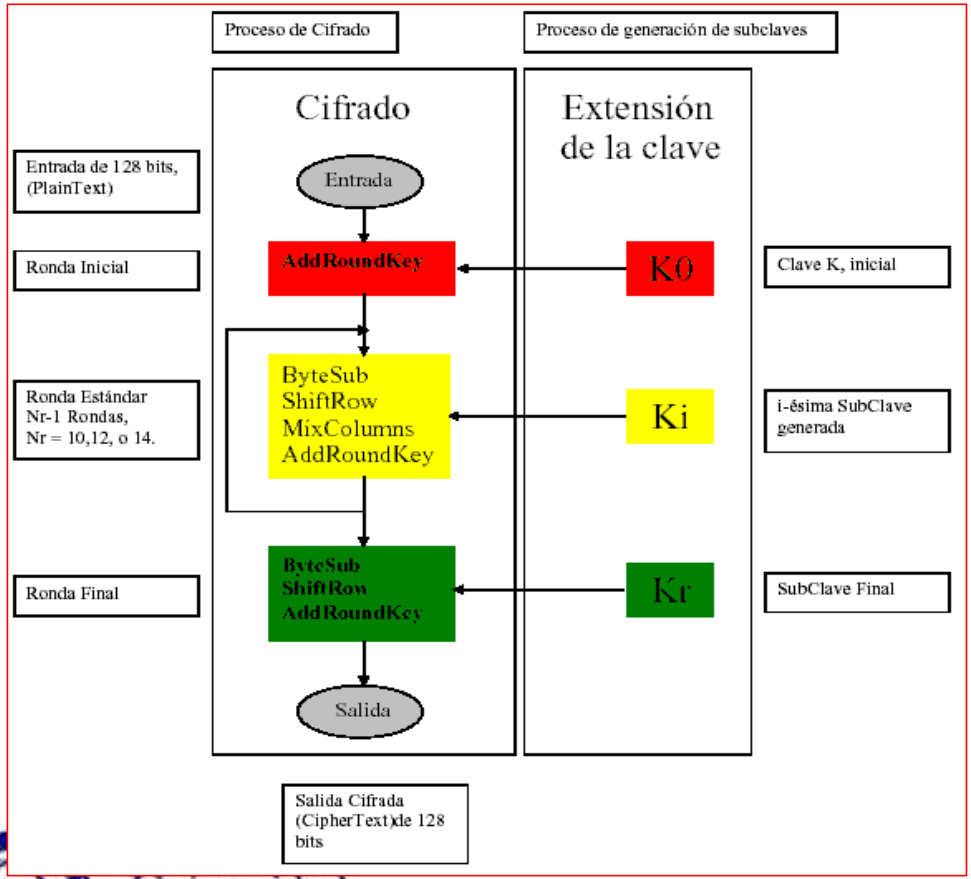
k_0	k_4	k_8	k_{12}	k_{16}	k_{20}
k_1	k_5	k_9	k_{13}	k_{17}	k_{21}
k_2	k_6	k_{10}	k_{14}	k_{18}	k_{22}
k_3	k_7	k_{11}	k_{15}	k_{19}	k_{23}

Clave de 24 bytes (192 bits)
Nk = 192/32 = 6

k_0	k_4	k_8	k_{12}	k_{16}	k_{20}	k_{24}	k_{28}
k_1	k_5	k_9	k_{13}	k_{17}	k_{21}	k_{25}	k_{29}
k_2	k_6	k_{10}	k_{14}	k_{18}	k_{22}	k_{26}	k_{30}
k_3	k_7	k_{11}	k_{15}	k_{19}	k_{23}	k_{27}	k_{31}

Clave de 32 bytes (256 bits)
Nk = 256/32 = 8

AES. Esquema



Funciones en cifrado (se recorre el esquema de arriba abajo):

- *AddRoundKey*
- *ByteSub*
- *ShiftRow*
- *MixColumns*

Funciones en descifrado (se recorre el esquema de abajo a arriba):

- *InvAddRoundKey*
- *InvByteSub*
- *InvShiftRow*
- *InvMixColumns*

Se realizará además una expansión de la clave K para generar desde K_0 hasta Kr.

Algoritmo RIJNDAEL

```
Rijndael(State, Key) {
    KeyExpansion( Key, ExpandedKey );
    AddRoundKey( State, ExpandedKey );
    for (i=1; i<10; i++)
            Round(State, ExpandedKey+4Xi);
    FinalRound(State,ExpandedKey+4X10);
}
```

```
Round(State, RoundKey) {
    ByteSub(State);
    ShiftRow(State);
    MixColumn(State);
    AddRoundKey(State, RoundKey);
}
```

State	-- array de 4 words (de 32 bits)
No. of Rounds	-- 10 rondas para la combinación de 128-128 bits
	-- XOR de las keywords (de 32 bits),
	S-box lookups, rotación de bytes intra-word
AddRoundKey	-- bitwise-XOR con las keywords
FinalRound	-- similar a Round pero sin MixColumn

AES. Operaciones con bytes

Unidad básica de tratamiento: el byte

- Suma y multiplicación. Son cálculos en Cuerpos de Galois GF(2^8) con 8 bits.
- Para la reducción de polinomios se usará el polinomio primitivo $p(x) = x^8 + x^4 + x^3 + x + 1$. no siempre es este polinomio.

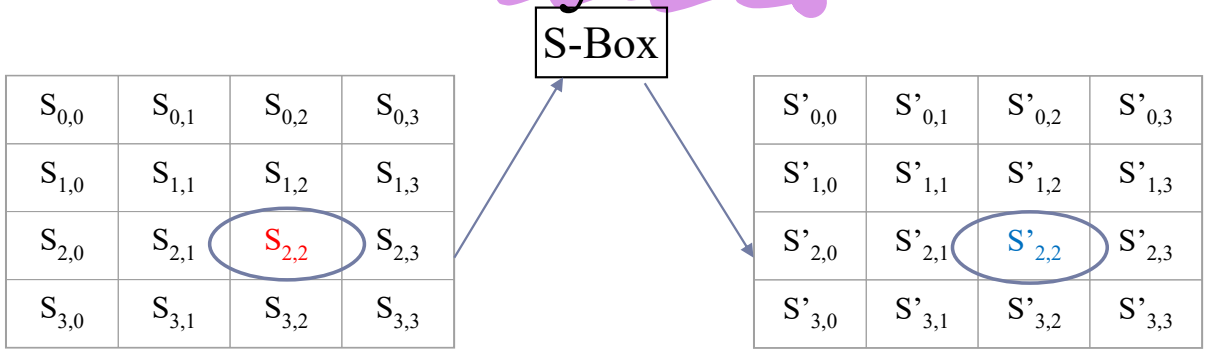
AES. Combinaciones de estados

Combinaciones posibles de estados en AES	Longitud del bloque (Nb palabras)	Longitud de la clave (Nk palabras)	Número de Rondas (Nr)
AES – 128	4	4	10
AES – 192	4	6	12
AES – 256	4	8	14

Para las funciones de cifrado y descifrado se usarán 4 transformaciones orientadas a bytes:

1. Sustitución de un byte mediante una tabla S-box (ByteSub).
2. Desplazamiento de filas de un estado (ShiftRow).
3. Mezcla de datos dentro de cada columna de estado (MixColumn).
4. Añade una clave de vuelta al estado. (AddRoundKey)

AES. Función ByteSub



Se trata de una función no lineal que se realiza a través de una S-box.

La S-box se construye:

a) calculando el inverso de la entrada en CG(2^8), y

b) calculando la siguiente transformación afín sobre CG(2):

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Representación matricial

Valor $\{63\}_{16}$ o $\{011000011\}_2$

Es el inverso del valor de entrada

Ej. $b'_0 = b_0 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7 \oplus c_0$ (Es fija, del standar)

AES. Tabla ByteSub

Usando la siguiente tabla, se llega a igual resultado que calculando el inverso y luego aplicando la transformación matricial mostrada en la diapositiva anterior.

En la siguiente diapositiva hay un ejemplo para el valor 5a mostrado.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES. Ejemplo de operación ByteSub

Se pide calcular el ByteSub de 5a

5a = 01011010 = $x^6 + x^4 + x^3 + x$

inv (5A) = 22 = 00100010

$$\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

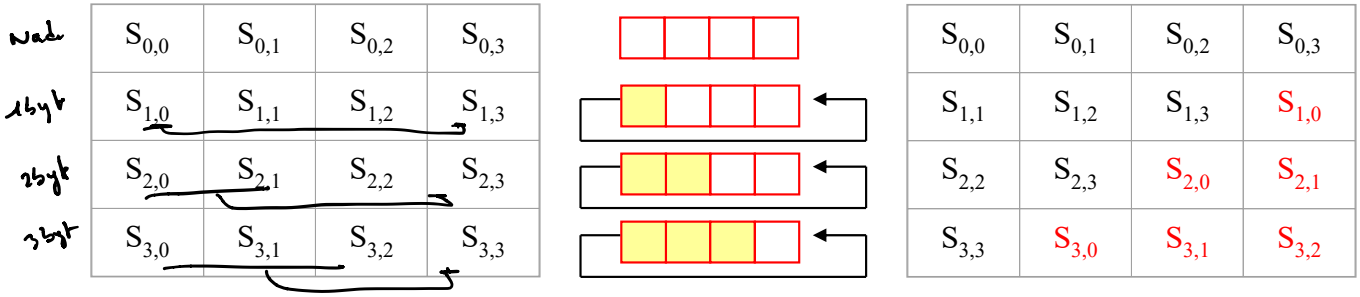
Al mismo valor se llega si en la tabla buscamos la intersección entre la fila 5 y la columna a: el resultado es el valor be.

Operando filas por columnas y sumando al resultado el valor $\{011000011\}_2$ se obtiene: 1011 1110 = be.

AES. Función ShiftRow

La función consiste en desplazar bloques de un byte hacia la izquierda módulo columna (en este caso 4) dentro de una fila.

Así la fila 0 no desplaza, la fila 1 desplaza un byte, la fila 2 desplaza dos bytes y la fila 3 desplaza tres bytes como se muestra.



Función MixColumns

Opera sobre columnas (que son consideradas como un polinomio) sobre GF(2^8) multiplicando cada columna por el polinomio fijo a(x) módulo $x^4 + 1$, en donde los valores {} están en hexadecimal. a(x) es primo relativo con $x^4 + 1$ y por tanto asegura el inverso.

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Recuerde que $\{03\} = x + 1$, $\{02\} = x$, $\{01\} = 1$.

Representación matricial de la función MixColumns

$$\begin{pmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{pmatrix}$$

Para $0 \le C < Nb$

Luego, las operaciones sobre columnas se expresan como:

$$S'_{0,C} = (\{02\} \bullet S_{0,C}) \oplus (\{03\} \bullet S_{1,C}) \oplus S_{2,C} \oplus S_{3,C}$$
$$S'_{1,C} = S_{0,C} \oplus (\{02\} \bullet S_{1,C}) \oplus (\{03\} \bullet S_{2,C}) \oplus S_{3,C}$$
$$S'_{2,C} = S_{0,C} \oplus S_{1,C} \oplus (\{02\} \bullet S_{2,C}) \oplus (\{03\} \bullet S_{3,C})$$
$$S'_{3,C} = (\{03\} \bullet S_{0,C}) \oplus S_{1,C} \oplus S_{2,C} \oplus (\{02\} \bullet S_{3,C})$$

AES.Ejemplo de operación MixColumns

Si suponemos que el estado intermedio es el indicado:

e1	a8	63	0d
fb	18	f4	c8
96	5b	73	11
7c	a0	e6	fd

El primer byte de estado $S'_{0,0}$ quedará:

$S'_{0,0} = \{02\}S_{0,0} \oplus \{03\}S_{1,0} \oplus S_{2,0} \oplus S_{3,0}$; $S'_{0,0} = \{02\}e1 \oplus \{03\}fb \oplus 96 \oplus 7c$

$\{02\}e1 = x(x^7 + x^6 + x^5 + 1) = x^8 + x^7 + x^6 + x$;

$\{02\}e1 = (x^8 + x^7 + x^6 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = d9$

$\{03\}fb = (x + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + x + 1)$

$\{03\}fb = x^8 + x^3 + x^2 + 1$

$\{03\}fb = (x^8 + x^3 + x^2 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = 16$

XOR
nº pares 1's ⇒ 0
nº impar 0's ⇒ 1

$S'_{0,0} = d9 \oplus 16 \oplus 96 \oplus 7c$

Luego: $\mathbf{S'_{0,0} = 25}$

Los bytes hasta $S'_{4,4}$ se calculan de forma similar.

e1	a8	63	0d
fb	18	f4	c8
96	5b	73	11
7c	a0	e6	fd

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

$p(x) = x^8 + x^4 + x^3 + x + 1 = 100011011$

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} e1 \\ fb \\ 96 \\ 7c \end{pmatrix} = \begin{pmatrix} 10 \cdot 1110\,0001 \oplus 11 \cdot 1111\,1011 \oplus 01 \cdot 1001\,0110 \oplus 01 \cdot 0111\,1100 \\ 01 \cdot 1110\,0001 \oplus 10 \cdot 1111\,1011 \oplus 11 \cdot 1001\,0110 \oplus 01 \cdot 0111\,1100 \end{pmatrix}$$

$$= \begin{pmatrix} 11100010 \oplus 100001101 \oplus 10010110 \oplus 01111100 \\ \end{pmatrix} = \begin{pmatrix} 25 \\ \end{pmatrix}$$

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a8 \\ 18 \\ 5b \\ a0 \end{pmatrix}$$

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} 63 \\ f4 \\ 76 \\ e6 \end{pmatrix}$$

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} 0d \\ c8 \\ 11 \\ fd \end{pmatrix}$$

AES.Ejemplo de operación MixColumns

El primer byte de estado $S'_{0,0}$ quedará:

$S'_{0,0} = \{02\}S_{0,0} \oplus \{03\}S_{1,0} \oplus S_{2,0} \oplus S_{3,0}$; $S'_{0,0} = \{02\}e1 \oplus \{03\}fb \oplus 96 \oplus 7c$

$\{02\}e1 = (0000\ 0010)(1110\ 0001) = (1\ 1100\ 0010)$;

$\{02\}e1 = (1\ 1100\ 0010) \oplus (1\ 0001\ 1011) = (1101\ 1000) = d9$

$\{03\}fb = (0000\ 0011)\ (1111\ 1011) = (0000\ 0010)\ (1111\ 1011) \oplus (1111\ 1011)$

$\{02\}fb = (0000\ 0010)\ (1111\ 1011) = (1\ 1111\ 0110)$

$\{02\}fb = (1\ 1111\ 0110) \oplus (1\ 0001\ 1011) = (1110\ 1101)$

$\{03\}fb = (1110\ 1101) \oplus (1111\ 1011) = (0001\ 0110) = 16$

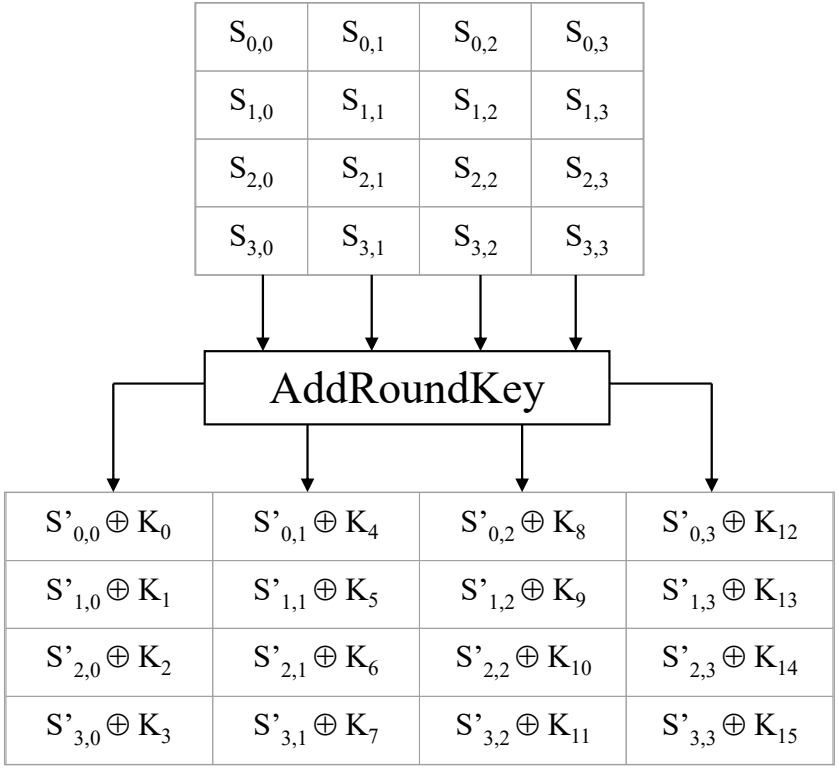
$S'_{0,0} = d9 \oplus 16 \oplus 96 \oplus 7c$

Luego: $\mathbf{S'_{0,0} = 25}$

AES. Función AddRoundKey

Se sumarán or exclusivo el estado intermedio con la clave de cada ronda.

En la ronda 0 será el or exclusivo entre el texto de entrada y la clave inicial; en las rondas siguientes (p.e. 1 a 9) será el or exclusivo de las subclave de cada ronda con la salida de la función MixColumns y en la última ronda (10) el or exclusivo de la subclave de estado 10 y la salida de ShiftRows.



AES. Expansión de la clave

Número de bits de las subclaves para valores estándar de Nb y Nk.

Bloque / Clave	Nk = 4 (128 bits)	Nk = 6 (192 bits)	Nk = 8 (256 bits)
Nb = 4 128 bits	Nr = 10 1.408 bits	Nr = 12 1.664 bits	Nr = 14 1.920 bits
Nb = 6 192 bits	Nr = 12 2.304 bits	Nr = 12 2.496 bits	Nr = 14 2.880 bits
Nb = 8 256 bits	Nr = 14 3.840 bits	Nr = 14 3.328 bits	Nr = 14 3.840 bits

- ✓ La expansión generará los bytes de las subclaves a partir de la clave K principal.
- ✓ Será un array lineal W de palabras de 4 bytes y con longitud Nb∗(Nr+1).

Cada una es una palabra

- EJEMPLO
  - Si K es de 128 bits, Nk = 4. Bloque de texto de 128 bits (Nb = 4).
  - ¿! La longitud del array W será (4*[10+1]) = 44 palabras de 4 bytes.
  - En las cuatro primeras posiciones (0 a 3) se copia la clave principal K.
  - Las restantes 40 palabras de las posiciones 4 a 43 ($4 \leq i \leq 43$) se calcularán mediante un algoritmo (NO ENTRAMOS A VERLO)