Criptología simétrica
(moderna)

Criptografía simétrica

- Términos equivalentes: Cifrado
  - simétrico
  - convencional
  - de clave secreta
  - de una clave
- Requisitos:
  - Emisor y receptor comparten clave (secreta)
  - Algoritmo de cifrado bueno
- Supone que algoritmo es conocido
- Implica un canal seguro para distribuir clave
- Algoritmos:
  DES, 3-DES, Bowfish, RC4, RC5, IDEA, AES, CAST-128, ...

Cifrado de Feinsel

Trabaja con bloques

- Divide bloque en 2
- Procesa en varias etapas
  - Sustitución de parte izquierda basada en parte derecha y subclave
  - Permutación intercambiando mitades

Parámetros:

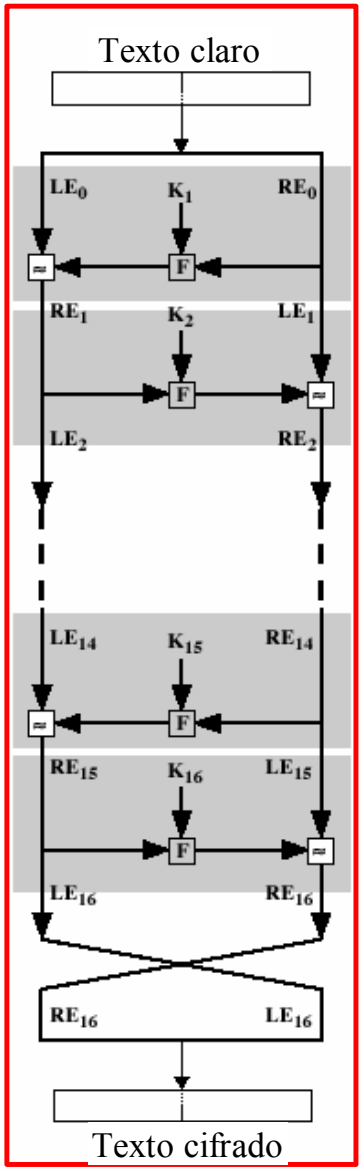
- Tamaño del bloque:
  + grande → + seguridad, -rápido
- Tamaño de clave:
  + grande → + seguridad, -rápido
- Número de etapas:
  + grande → + seguridad, -rápido
- Algoritmo de subclave:
  + complejo → + seguridad, -rápido
- Función:
  +compleja → + seguridad, -rápido

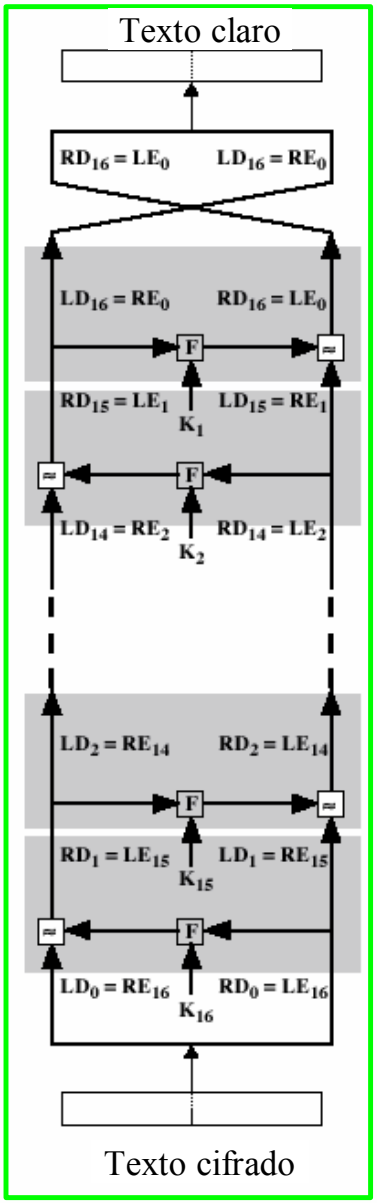
Facilidad de análisis

Rapidez de proceso

Proceso inverso para descifrado

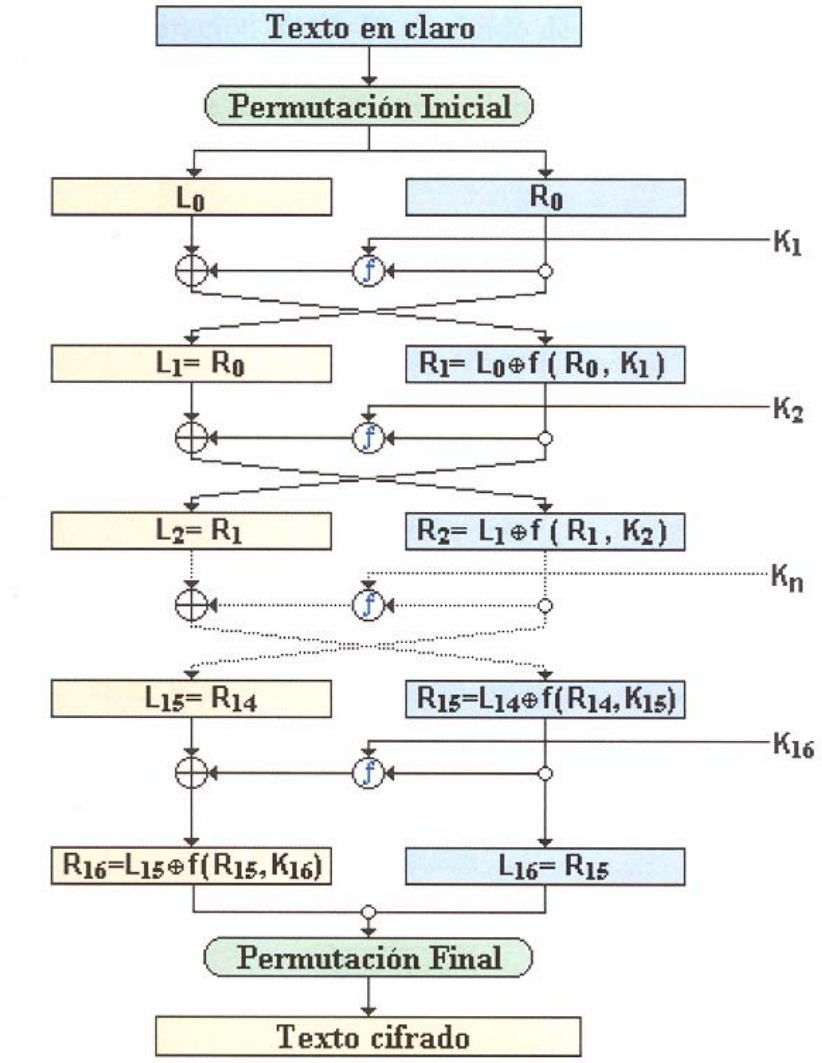
Base de muchos otros





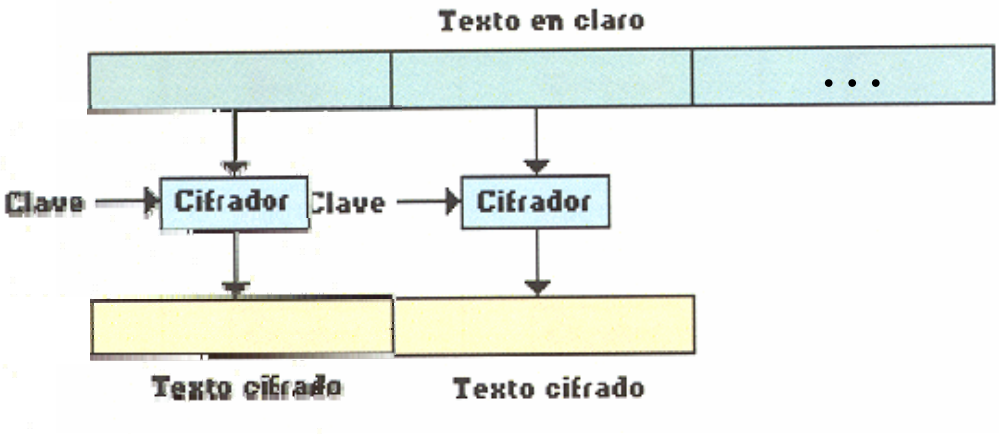
DES (*Data Encriptation Standard*)

- Sigue diseño de Feinsel
- De IBM (origen en Lucifer)
- Adoptado por NIST como estándar federal (FIPS PUB 46) en 1977
- Sustituido por AES como estándar NIST en 2000
- Trabaja con bloques de 64 bits y clave de 56 bits:
  - Permutación inicial (tabla)
  - 16 etapas con la misma función, con subclave distinta
  - Permutación final (tabla)
- Preocupación por longitud de clave y algoritmo



DES. Modos de operación

- ECB (*Electronic Code Book*)
  - Cifrado de cada bloque es independiente
  - Necesario rellenar bloque final
  - Para texto corto



Ventajas:

- Descifrado de cada bloque es independiente
- Procesamiento en paralelo

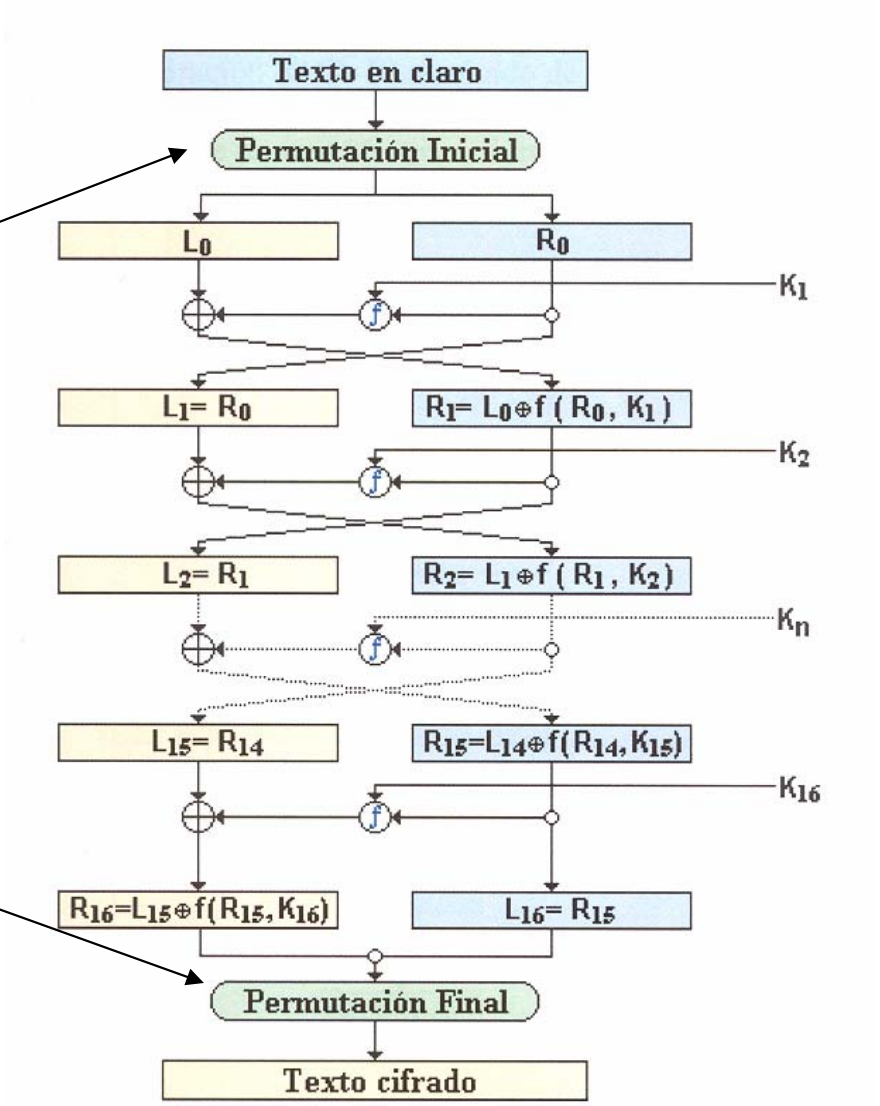
Desventajas:

- Ataques de texto conocido fáciles
- Se pueden ver repeticiones de texto
  (Bloques iguales en texto claro dan lugar a bloques iguales de texto cifrado)
- Fácil sustituir, reordenar, borrar o insertar bloques antiguos

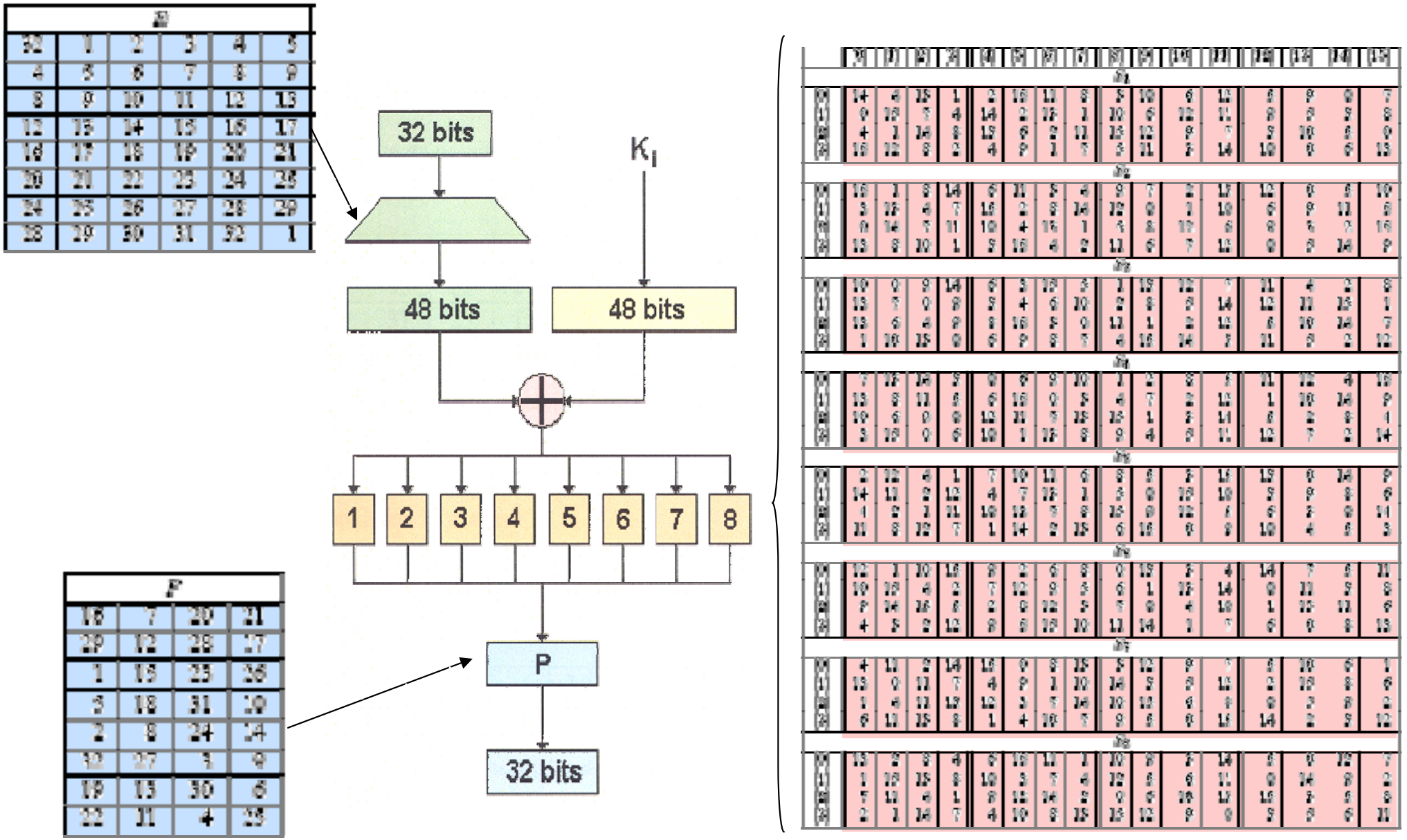
DES. Permutación inicial y final

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	55	45	37	29	21	13	5
63	63	47	39	31	23	15	7

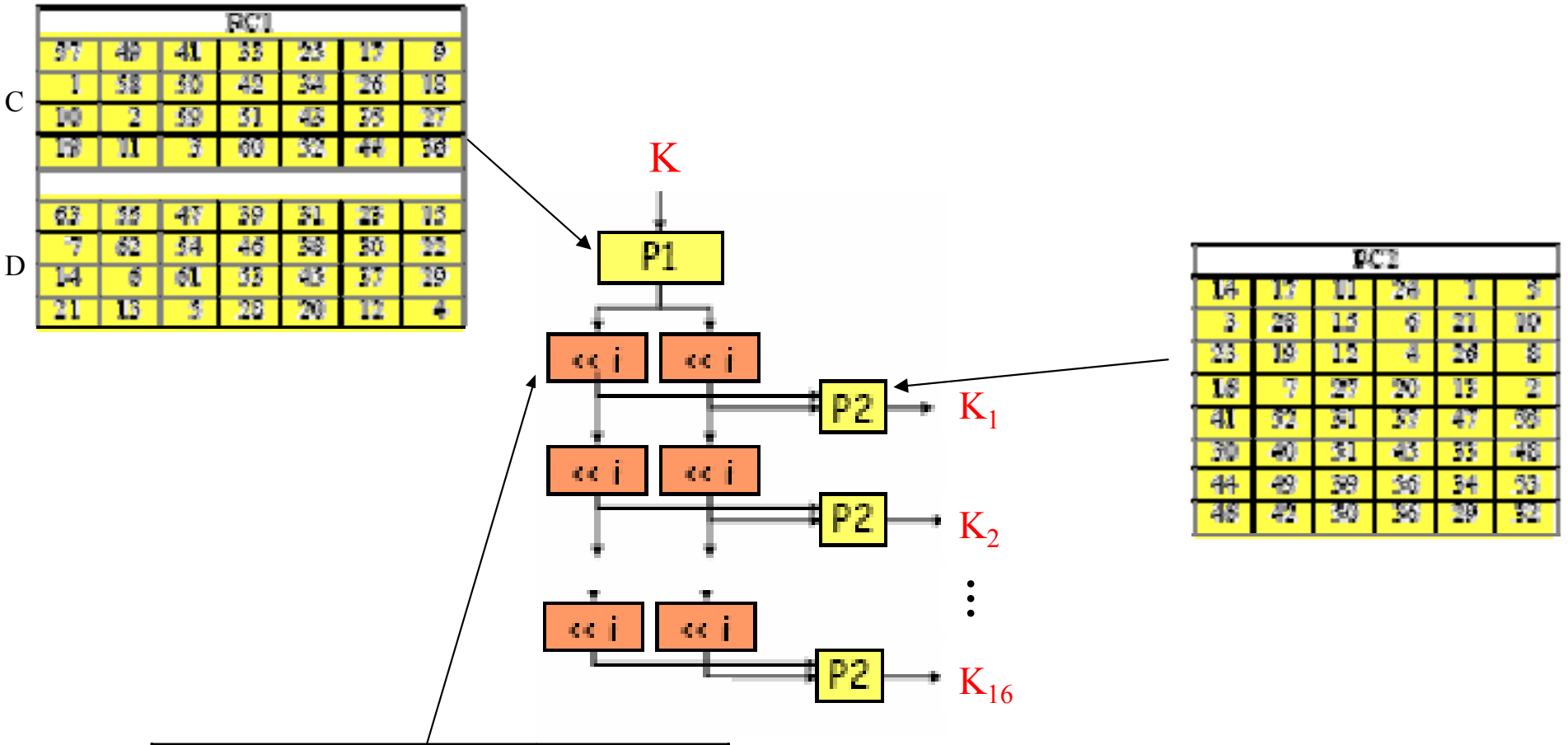
IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



DES. Función principal de etapa



DES. Generación de subclaves



Nº ITERACIÓN	Nº DESP. IZDA
1,2,9,16	1
3,4,5,6,7,8,10,11,12,13,14,15	2

DES. Criterios de diseño de cajas S

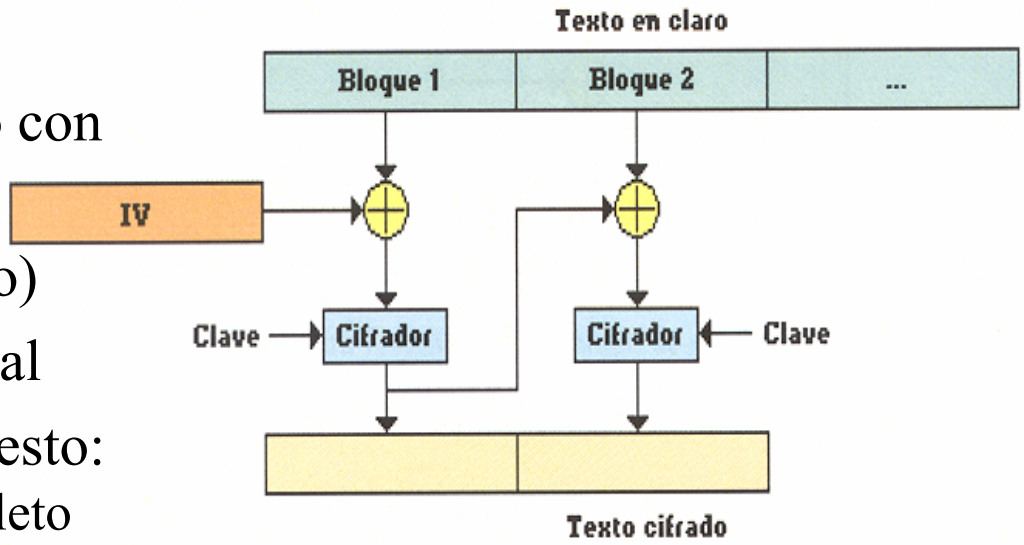
- Ninguna salida de caja S demasiado cerca de una función lineal de bit de entrada
- Cada fila de caja S debe incluir todos los 16 posibles valores de salida
- Si dos entradas de una caja S difieren en un bit, sus salidas deben diferir en, al menos, dos bits (difusión y amplificación de las diferencias)
- Si dos entradas de una caja S difieren en los dos bits centrales centrales, sus salidas deben diferir en, al menos, dos bits
- Si dos entradas de una caja S difieren en sus dos primeros bits y son iguales en los dos últimos, las salidas no deben ser iguales
- Para cualquier diferencia de 6 bits no nula, no mas de 8 de los 32 pares de entradas con esa diferencia pueden dar la misma diferencia de salida (para evitar criptoanálisis diferencial)

DES. Criterios de diseño de P

1. Las cuatro salidas de cada caja S en vuelta i-ésima deben ser distribuidas de forma que dos de ellas afecten a los bits centrales de siguiente vuelta
   - Los bits centrales no son compartidos entre cajas S
   - Los bits extremos son los que se comparten
2. Los cuatro bits de salida de cada caja S deben afectar a 6 cajas S en la siguiente vuelta y no a ella misma (difusión)
3. Para dos cajas S_j y S_k, si un bit de S_j afecta un bit central de S_k en siguiente vuelta, entonces, un bit de salida de S_k no puede afectar a un bit central de S_j (evitar ciclos)
   - Para j=k, un bit de salida de S_j no debe afectar a un bit central de esa misma caja, en la siguiente ronda

DES. Modos de operación (cont.)

- CBC (*Cipher Block Chaining*)
  - Cada nuevo bloque relacionado con anterior mediante XOR
  - Necesario vector inicial (secreto)
  - Necesario completar bloque final
  - Cambio en un bloque afecta a resto: Cifrado depende de mensaje completo



Ventajas:

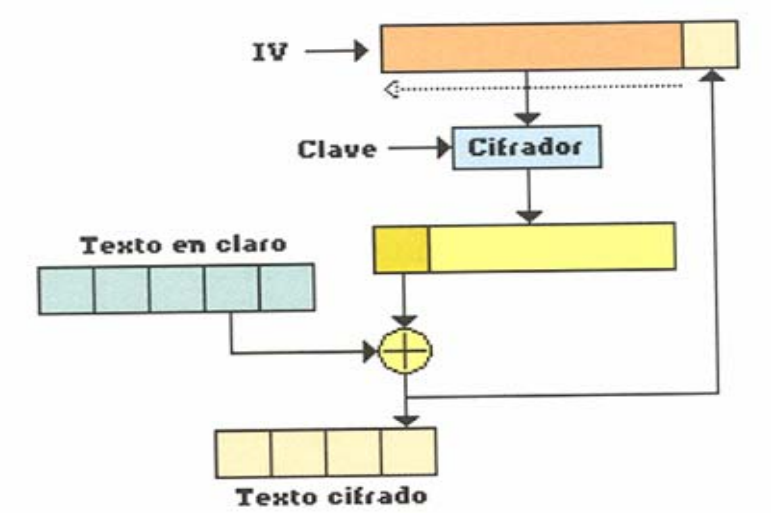
- Descifrado de cada bloque análogo
- Bloques iguales en texto claro dan lugar a bloques distintos de texto cifrado

Desventajas:

- Propagación de errores
- Repetición de vector inicial con misma clave añade vulnerabilidad

DES. Modos de operación (cont.)

- CFB (*Cipher Feedback*)
  - Cifra bit (carácter) a bit (carácter)
  - Texto cifrado realimentado
  - Necesario vector inicial
  - No necesario completar final



Ventajas:

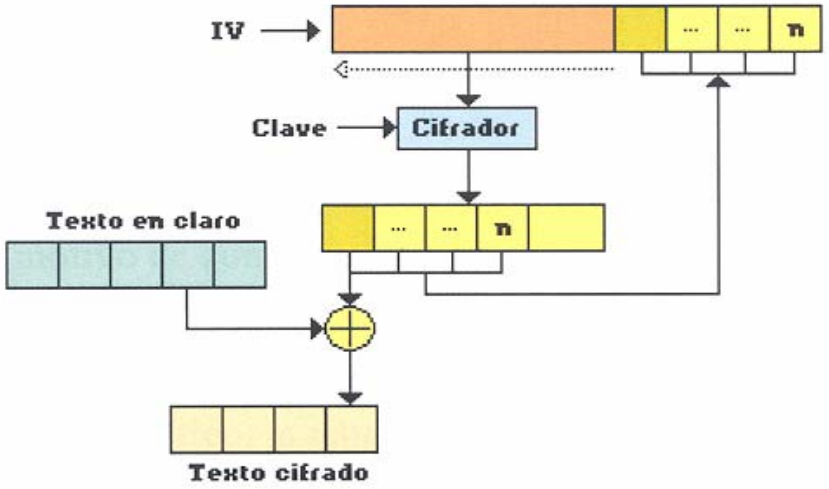
- Simula cifrador de flujo

Desventajas:

- Propagación de errores

DES. Modos de operación (cont.)

- OFB (*OutputFeedback*)
  - Cifra bit (carácter) a bit (carácter)
  - Salida de 'cifrador' añadida a mensaje y realimentada
  - Necesario vector inicial
  - No necesario completar final
  - Realimentación es independiente de texto



Ventajas:

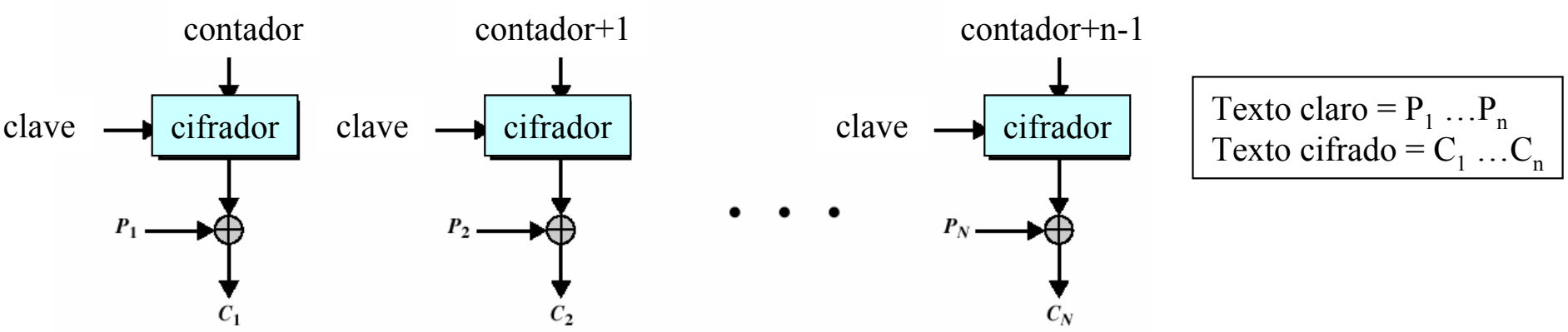
- Simula cifrador de flujo
- Permite cálculos por adelantado
- No propagación de errores

Desventajas:

- Repetición de vector inicial con misma clave añade vulnerabilidad

DES. Modos de operación (cont.)

- CTR (*CounTeR*)
  - Posterior a anteriores
  - Similar a OFB, pero cifra valor de contador en lugar de realimentado
  - Comienza con contador aleatorio



Ventajas:

- Simula cifrador de flujo

Desventajas:

- Reutilización de valores clave/contador añade vulnerabilidad

- Modos de operación generalizables a otros cifradores por bloques

DES. Ataques

- Análisis diferencial:
  - Murphy, Biham y Shamir en 1990
  - Compara pares de textos cifrados relacionados cuyos textos originales tienen diferencias conocidas y concretas
  - Analiza evolución de diferencias de textos claros a medida que se propagan por etapas de cifrador de bloques
  - DES requiere 2^{47} textos en claro elegidos (y su criptograma)
- Análisis lineal:
  - Matsui en 1993
  - Busca aproximaciones lineales para describir acción de un cifrador de bloques
  - DES requiere 2^{47} textos en claro conocidos (y su criptograma)

DES. Ataques (cont.)

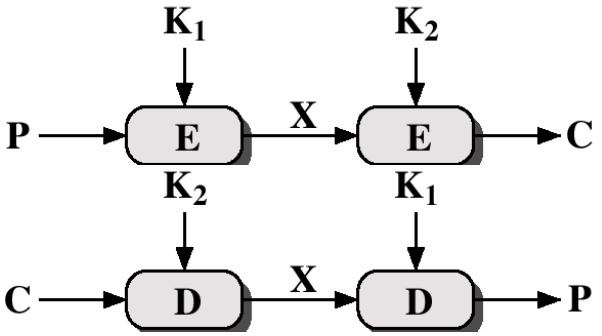
- Fuerza bruta:
  - 1997: por Internet tras unos meses
  - 1998: con hardware especial (Deep Crack) tras unos días
  - 1999: con combinación de hardware y red tras 22 horas

¿Clave más larga?

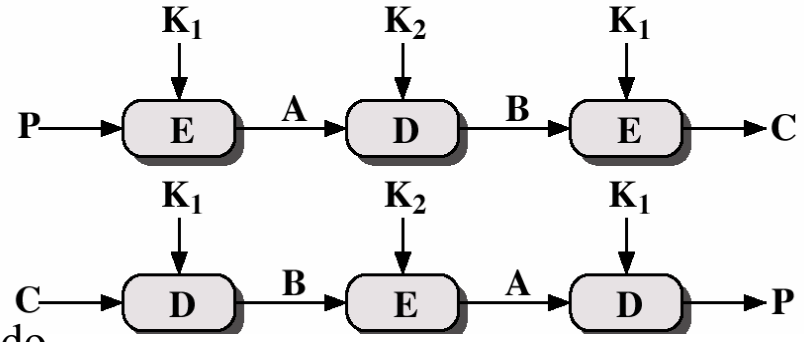
¿Reemplazar DES?

DES múltiple

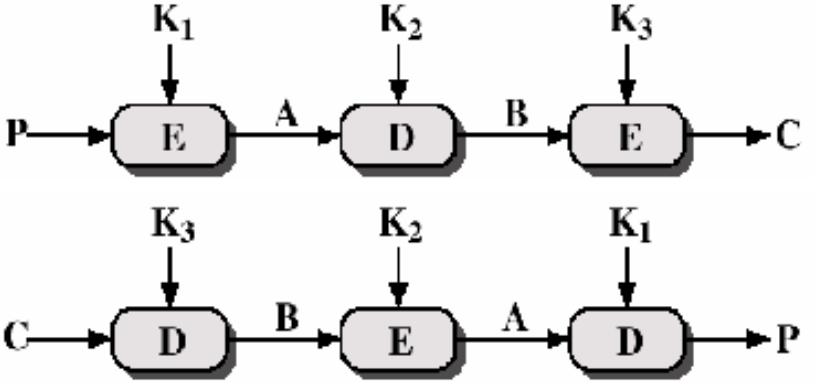
- Doble DES:
  - Complejidad de ataque similar a fuerza bruta sobre DES



- Triple DES:
  - Dos claves (112 bits)
    - Ataques posibles, pero no prácticos
      - Merkle y Hellman, 1981: 2^{56} pares texto claro elegido/texto cifrado



  - Tres claves (168 bits)
    - Complejidad de ataque aumenta, pero no hay diferencia sustancial con anterior
    - Muy lento en software

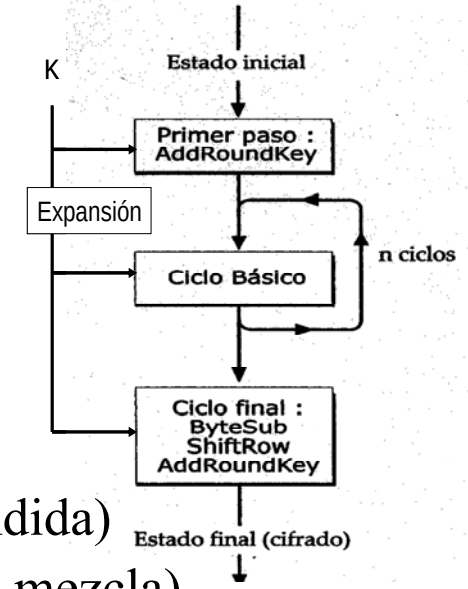


Imágenes de [Stallings, 2004]

AES (*Advanced Encryption Standard*)

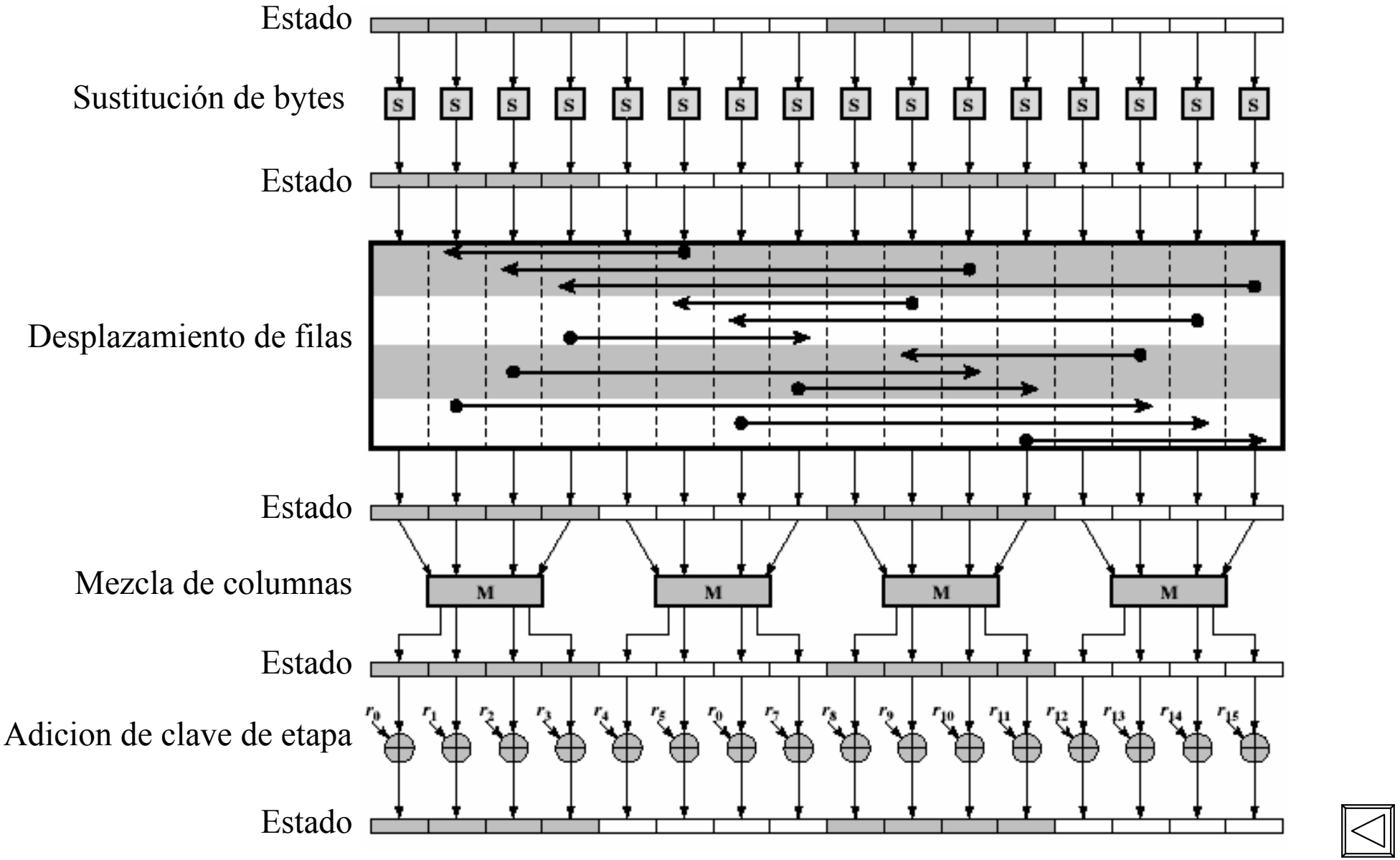
- Rijndael de Vincent Rijmen y Joan Daemen en 1997
- Estándar de NIST (FIPS PUB 197) en 2001 tras concurso
- Varios tamaños:
  - Claves de 128/192/256 bits con 9/11/13 etapas y bloques de datos de 128 bits

PROCEDIMIENTO:



  - Datos en 4 grupos de 4 bytes
  - Operaciones con bloque entero en cada etapa:
    - Sustitución de byte (1 caja-S sobre cada byte)
    - Desplazamiento de filas (permuta bytes entre columnas)
    - Mezcla de columnas (sustitución usando matrices de multiplicación de grupos)
    - Adición de clave de etapa (XOR con parte de clave expandida)
  - XOR inicial con parte de clave y última etapa incompleta (sin mezcla)
- Implementación muy eficiente
- Criptoanálisis: Ataque sobre estructura algebraica. Seguro por ahora
- Descifrado: Similar a cifrado, con operaciones inversas para sustitución, mezcla y desplazamiento

AES. Etapa



Tomado de [Stallings, 2004]

AES. Tablas de sustitución

x \ y	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	0c	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	0a	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	80	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	0e	55	28	df
f	8c	a1	89	0d	bf	E6	42	68	41	99	2d	0f	b0	54	bb	16

Cifrado

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

Descifrado

AES. Desplazamiento y mezcla

Tablas de desplazamiento

- Bloque de 128 y 192
  - fila 0: inamovible, fila 1: 1 lugar, fila 2: 2 lugares, fila 3: 3 lugares
- Bloque de 256
  - fila 0: inamovible, fila 1: 1 lugar, fila 2: 3 lugares, fila 3: 4 lugares

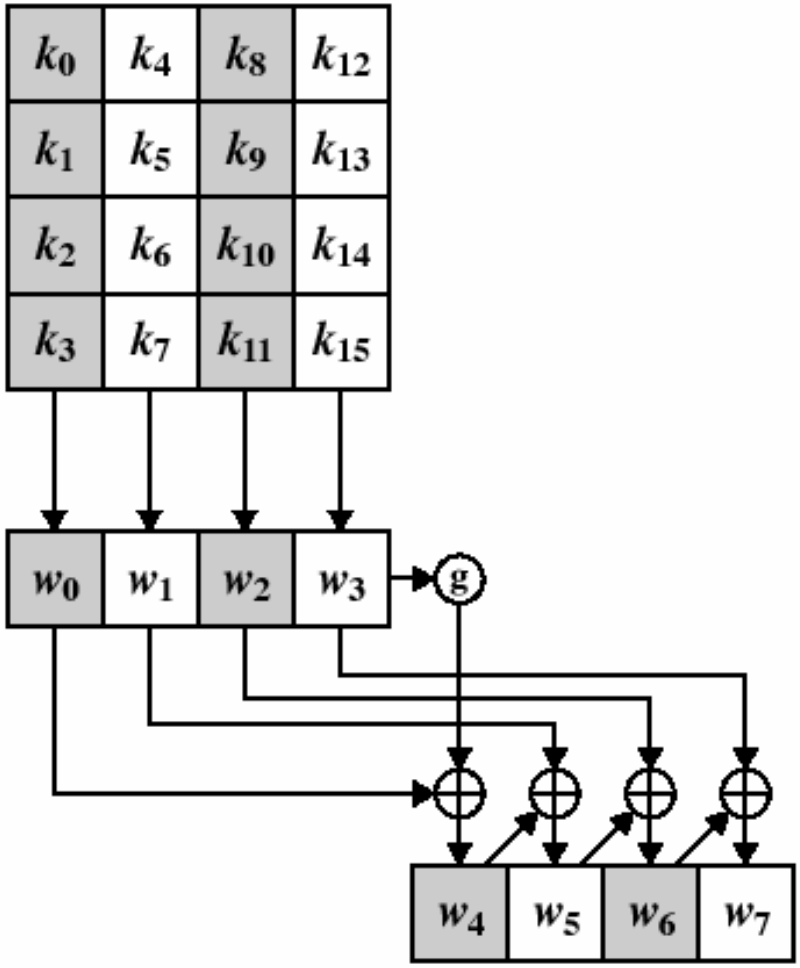
Matrices de mezcla

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

- Nuevo valor de elemento depende de todos los de su columna

AES. Expansión de clave

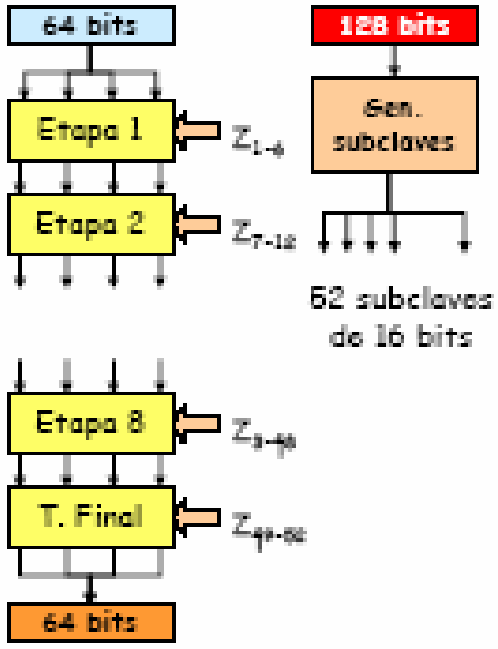
- Clave de 128/192/256 bits pasa a vector de 44/52/60 palabras de 32 bits
- Copia clave en 4 1as palabras de clave expandida
- Bucle para crear resto
  - Palabra nueva con XOR de anterior y 4 posiciones anteriores
    - Cada 4ª iteración usa caja S, desplazamiento y XOR con anterior antes de XOR
- Clave sólo usada en operación de adición (4 palabras)



Imágenes de [Jovall, 2003]

IDEA (*International Data Encription Algorithm*)

- Lai y Massey en 1990/1992, alternativa europea
- Trabaja con bloques de 64 bits y clave de 128 bits
- Consta de 8 etapas iguales y una transformación final
  - Se desvía de modelo de Feistel, usa:
    - XOR
    - Suma de enteros modulo 2^{16}
    - Multiplicación de enteros modulo 2^{16}-1 ($0=2^{16}$)

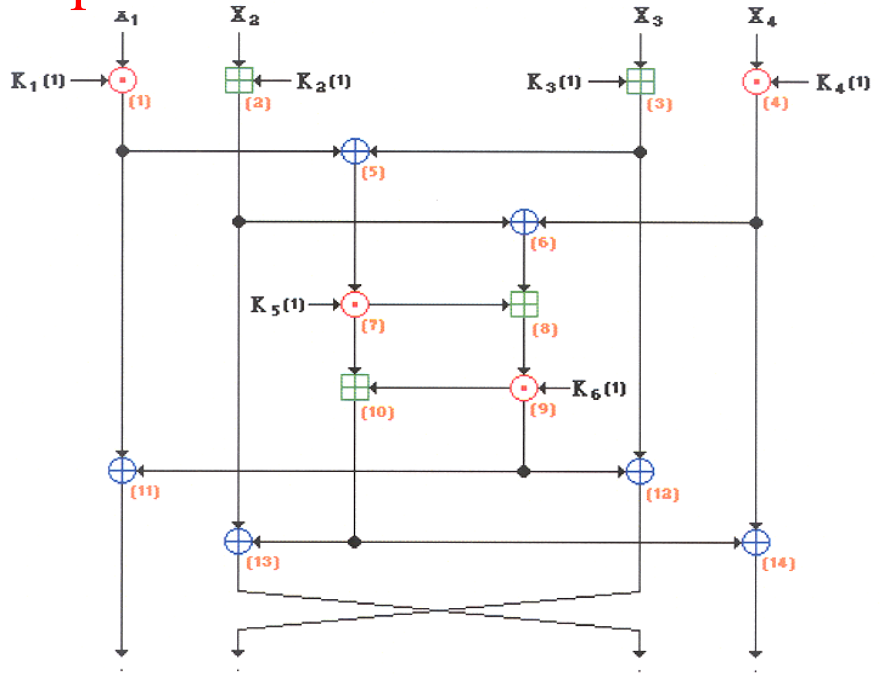


- Implementación eficiente en hardware y software
- Patentado, pero gratuito para uso no comercial
- Incluido en muchas aplicaciones de dominio público: PGP, ...
- Criptoanálisis: Muy seguro por ahora
- Descifrado: mismo algoritmo que cifrado con diferente uso y valor de claves de etapa

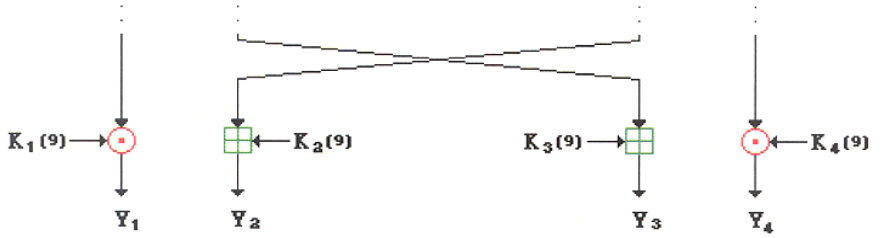
Imágenes de [Dávila, 2005]

IDEA. Procedimiento

Etapa



Transformación final



- 8 etapas iguales con bloques de 64 bits y subclaves de 96 bits
  - Bloque en argumentos de 16 bits
  - Operaciones: XOR, multiplicaciones y sumas modulares
  - Dos etapas de mezcla con claves intermedias
  - Función central: cada bit de salida depende de cada bit de argumentos
  - Intercambio final de bloques centrales

- Por último
  - Intercambio de bloques centrales
  - Combinación con claves
  - Depende de cuatro claves de 16 bits.

IDEA. Subclaves de cifrado y descifrado

- Clave original de 128 bits genera 832 bits de claves intermedias (necesarias 52 subclaves de 96 bits)
  - Subclaves en cada etapa utilizan un conjunto diferente de bits de clave inicial
  - Los 96 bits utilizados no son contiguos
- Claves de descifrado se deducen de claves de cifrado:
  - Cuatro primeras claves de i-ésima etapa se deducen de cuatro primeras claves de la etapa (10-i)-ésima de cifrado
  - 1ª y 4ª subclaves de descifrado son inversa multiplicativa (módulo 2^{16}-1) de 1ª y 4ª subclaves de cifrado
  - Para etapas 2 a 8, 2ª y 3ª subclaves de descifrado son inversa a suma módulo 2^{16} de 3ª y 2ª subclaves de cifrado