Criptografía Simétrica - Parte 2

Miguel Angel Astor Romero

24 de mayo de 2019

Agenda

Conceptos Fundamentales

Criptología

Ciencia que estudia la criptografía y el criptoanálisis.

Criptografía

Ciencia que estudia las propiedades y el diseño de criptosistemas.

Criptosistema

Algoritmo, técnica y/o herramienta para cifrar mensajes.

Criptoanálisis

Ciencia que estudia el descifrado de un mensaje encriptado sin necesidad de la clave, basándose en propiedades del algoritmo o del texto cifrado.

Tipos de cifrado

Cifrado simétrico

Conjunto de algoritmos y técnicas de cifrado que utilizan una única clave de cifrado secreta, compartida entre los participantes de la comunicación cifrada.

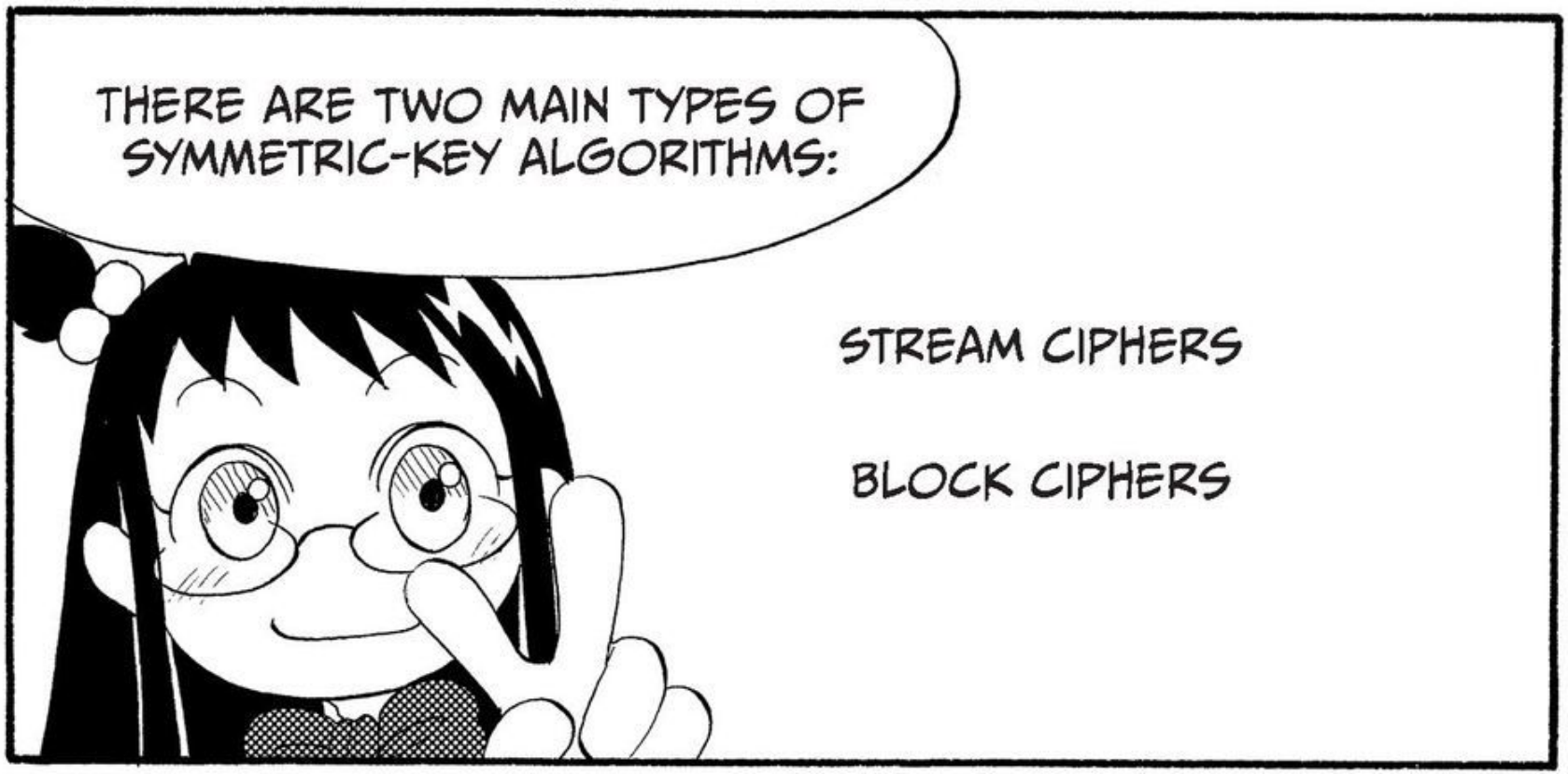
Cifrado asimétrico

Conjunto de algoritmos y técnicas de cifrado que utiliza dos claves de cifrado: una secreta o privada conocida solo a su dueño, y otra publica conocida por todo el mundo.

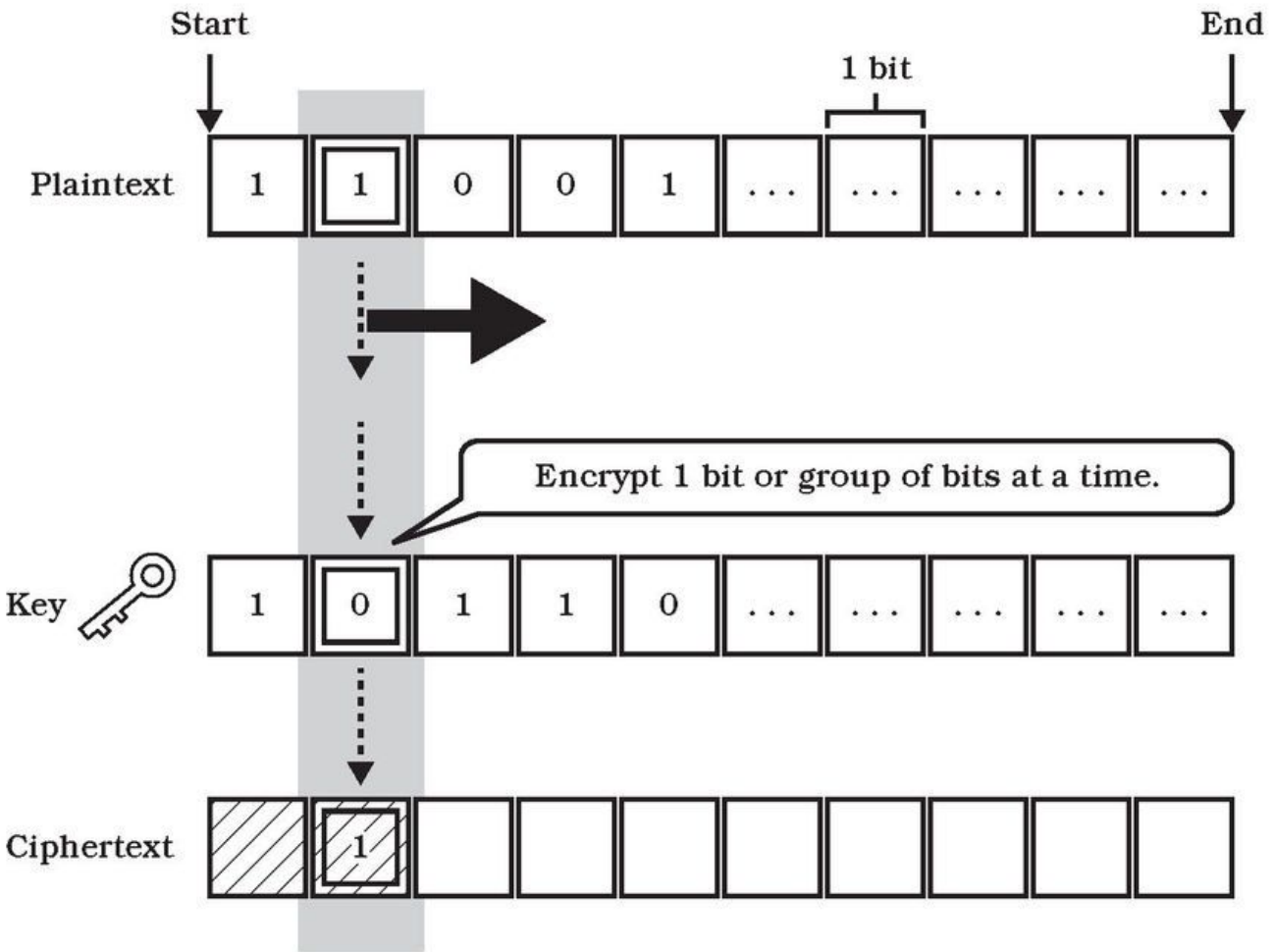
Modelo Básico de Criptografía Simétrica

Símbolos y Bits

Clases de Cifrado Simétrico



Cifrado de Flujos



Ejemplo 1 - Cifrado XOR

Ejemplo 1

texto plano	0b01001101 (0x4D -> 'M')
clave	0b10010001 (0x91)
texto cifrado	0b11011100 (0xDC)

Ejemplo 2

texto plano	0b01000001 (0x41 -> 'A')
clave	0b10010001 (0x91)
texto cifrado	0b11010000 (0xDC)

Ejemplo 2 - RC4

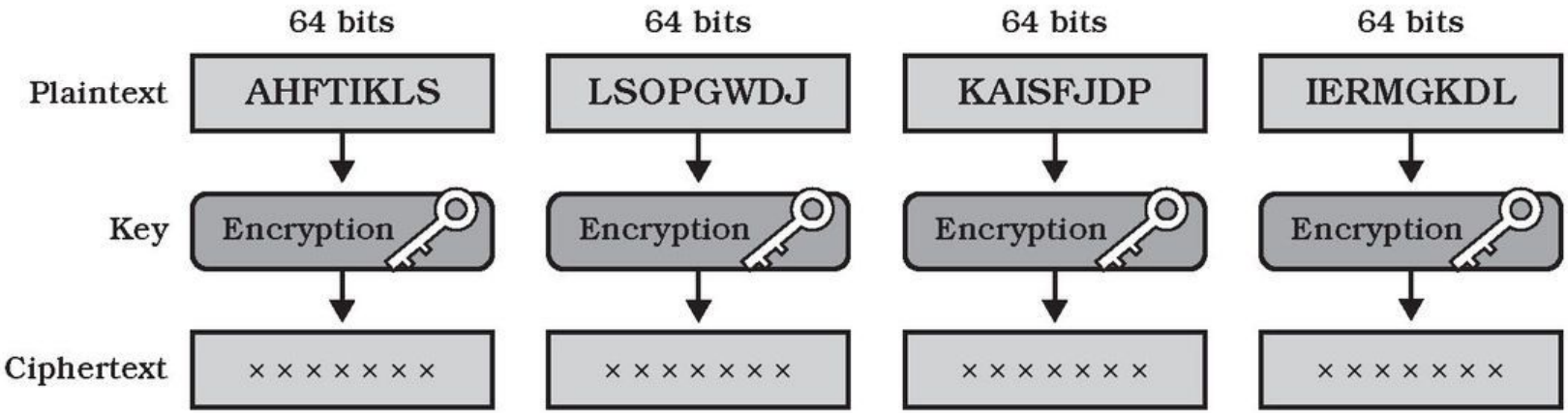
Generación de Claves

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := j + S[i]
    j := j + key[i % keylength]
    j := j % 256
    swap(S[i], S[j])
endfor
```

Generación Pseudo-Aleatoria

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) % 256
    j := (j + S[i]) % 256
    swap(S[i], S[j])
    K := S[(S[i] + S[j]) % 256]
    B := read()
    print(B ⊕ K)
endwhile
```

Cifrado de Bloques



Modos de Operación

Electric Code Book (ECB)

Cada bloque se cifra de manera individual.

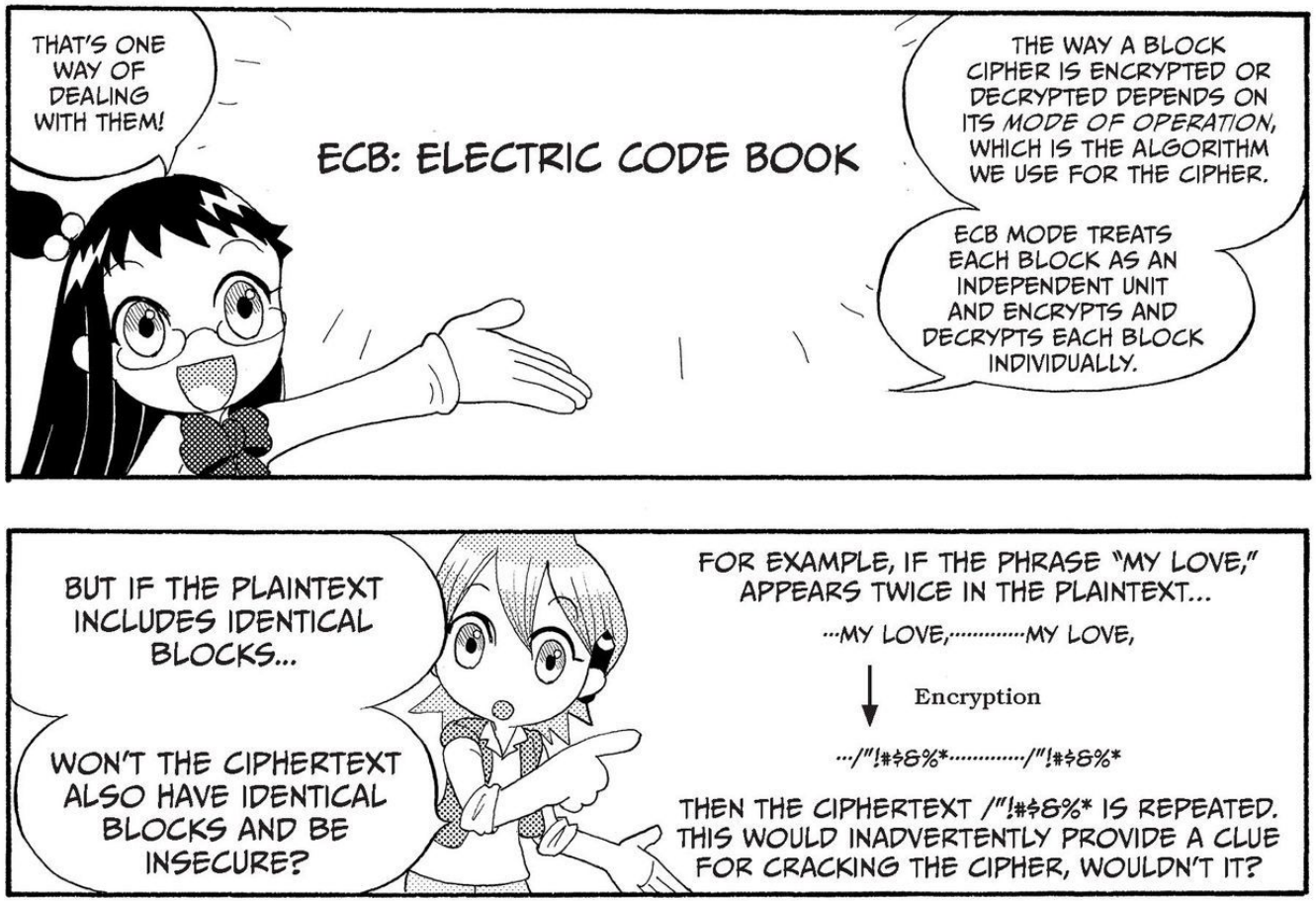
Cipher Block Chaining (CBC)

El cifrado de un bloque depende del bloque anterior.

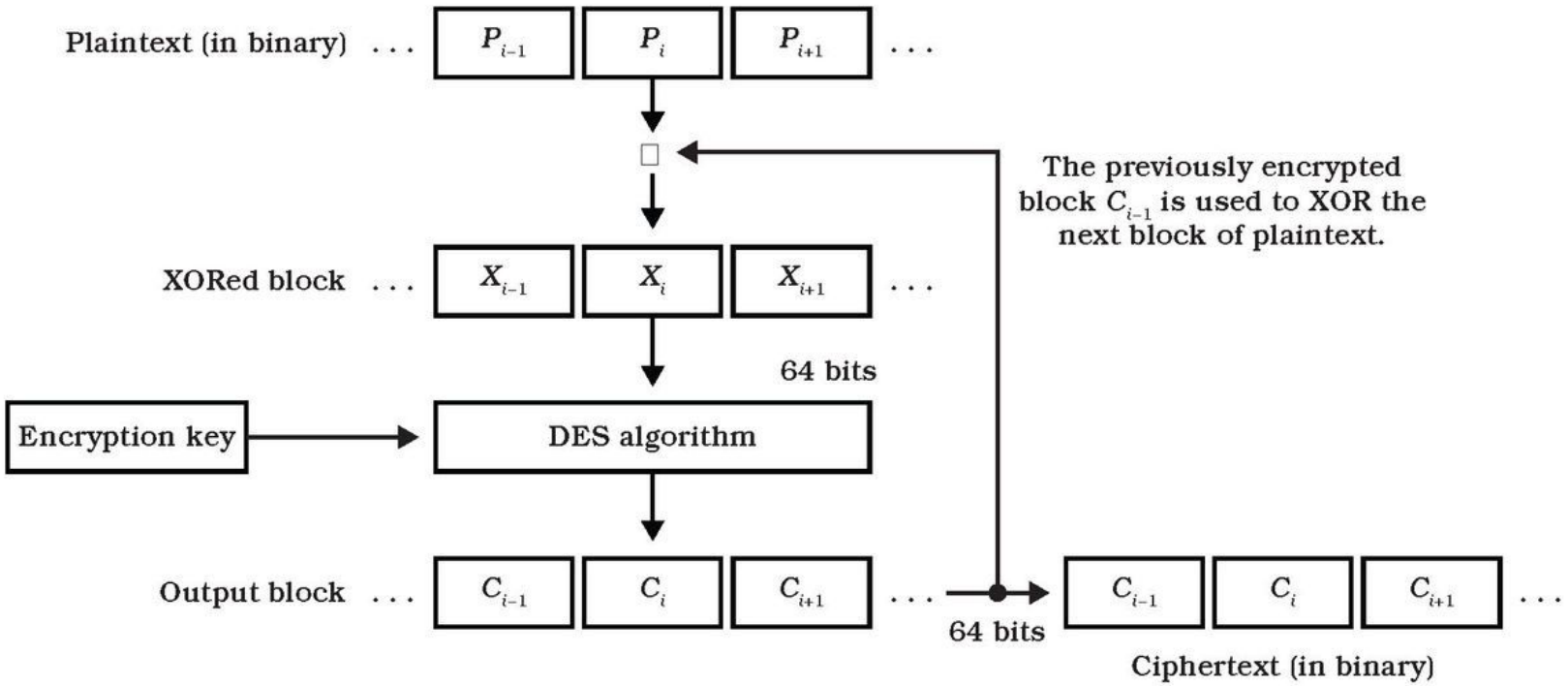
Otros modos de operación

- Output Feedback (OFB)
- Cipher Feedback (CFB)

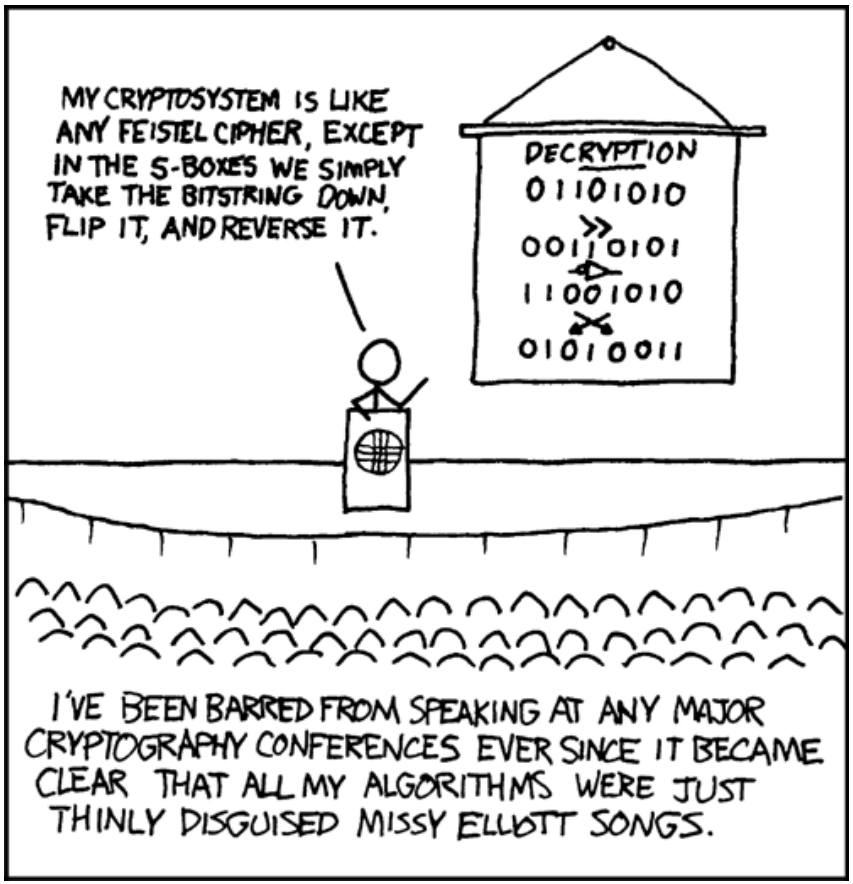
Electric Code Book



Cipher Block Chaining



Redes de Feistel



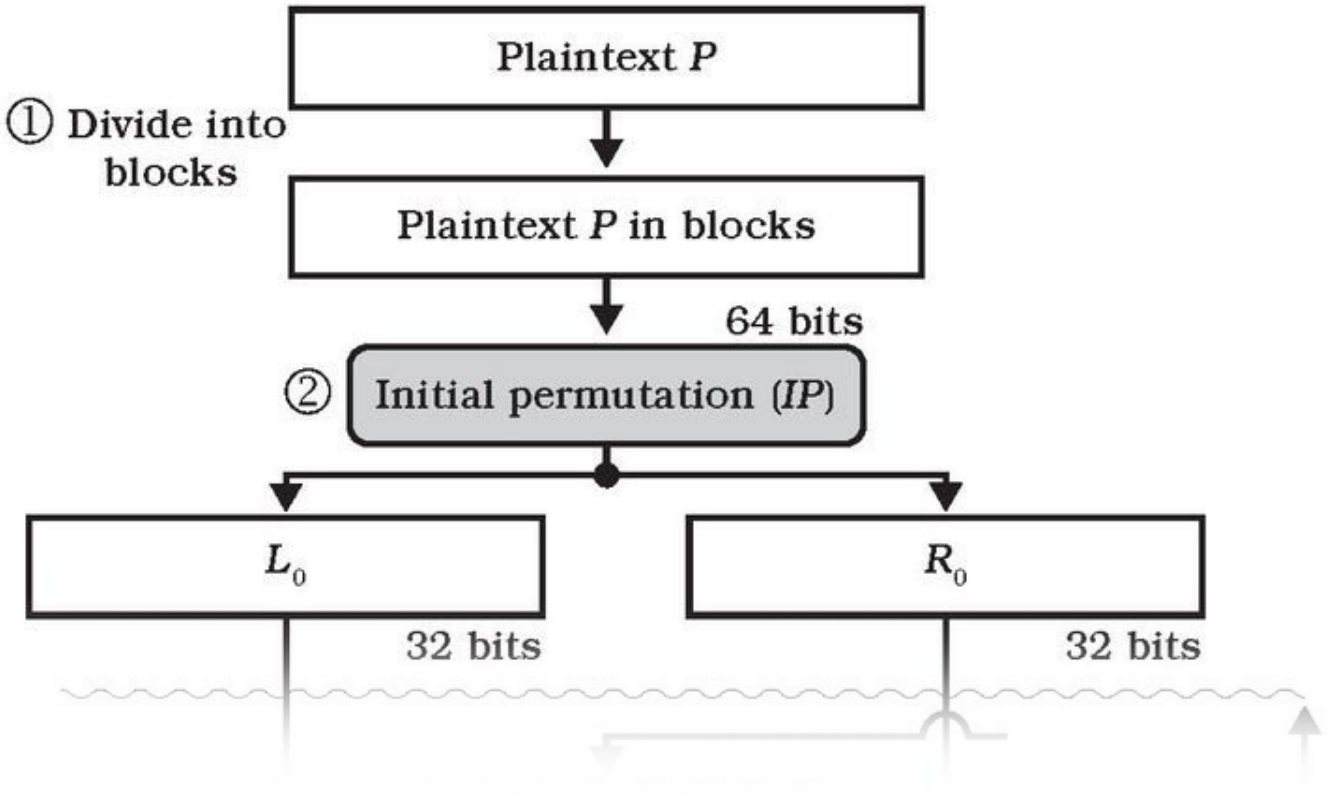
- Algoritmo de cifrado de bloques tipo CBC.
- Diseñado por Horst Feistel en 1970.
- Primera implementación: Cifrado Lucifer de IBM.
- Es una involución.

Funcionamiento de una Red de Feistel

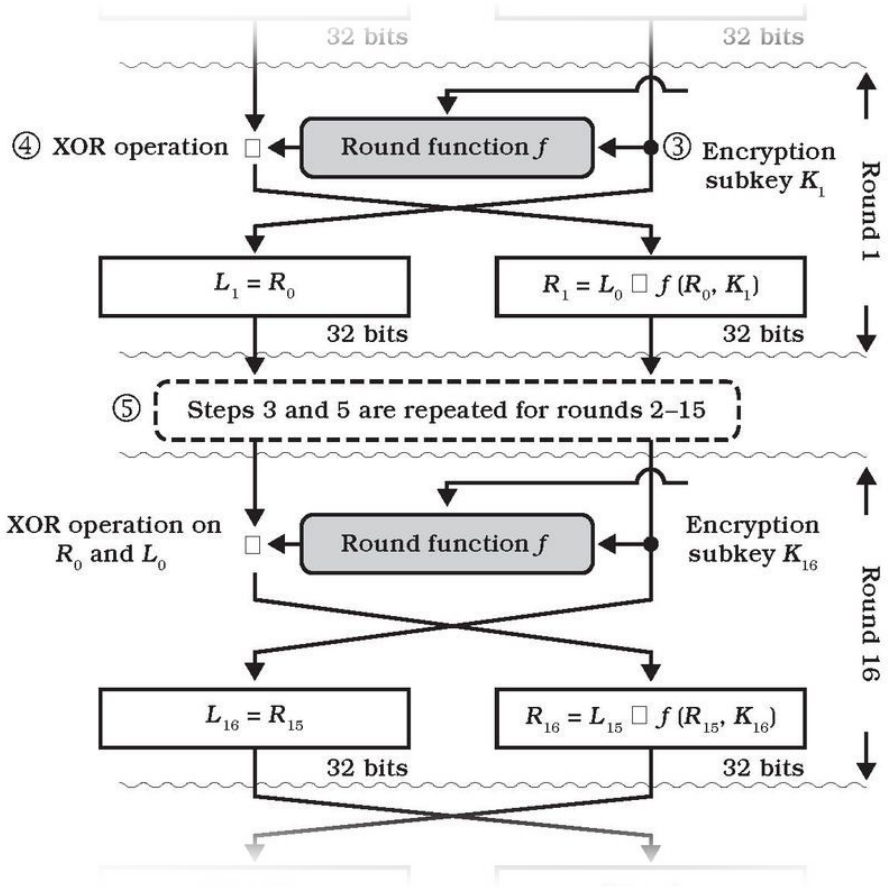
Algoritmo

1. Dividir el texto plano en bloques de 64 bits.
2. Separar bits en pares (L_0) e impares (R_0).
3. Aplicar función de ronda f con clave K_i a L_0.
4. Calcular XOR de $f(L_0, K_1)$ y R_0.
5. Repetir pasos 3 y 4 para las rondas 2 a 16.
6. Reconstruir bloque de 64 bits con resultado de la ronda 16.
7. Invertir permutación inicial.

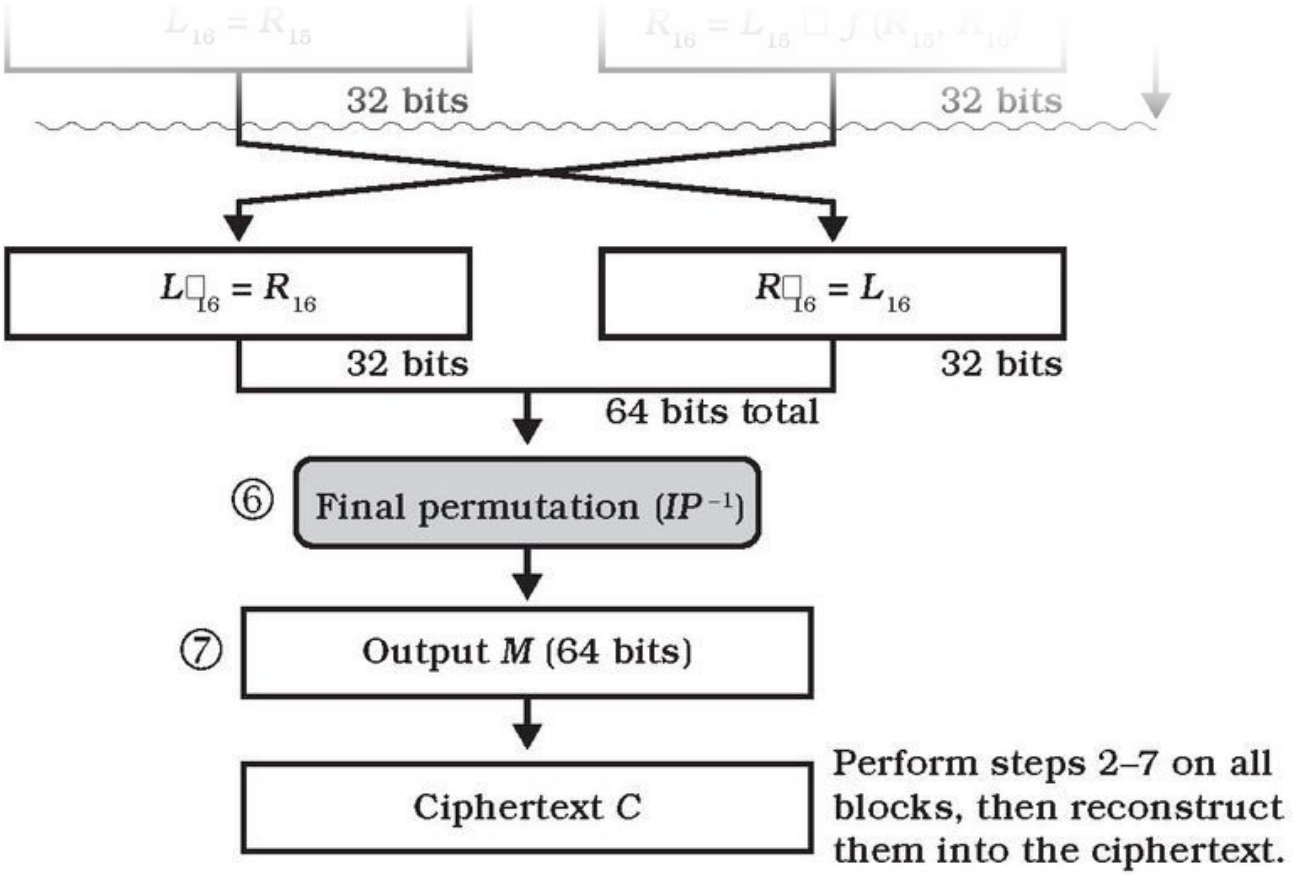
Pasos 1 y 2


Plaintext P
① Divide into blocks
Plaintext P in blocks
64 bits
② Initial permutation (IP)
L_0
R_0
32 bits
32 bits

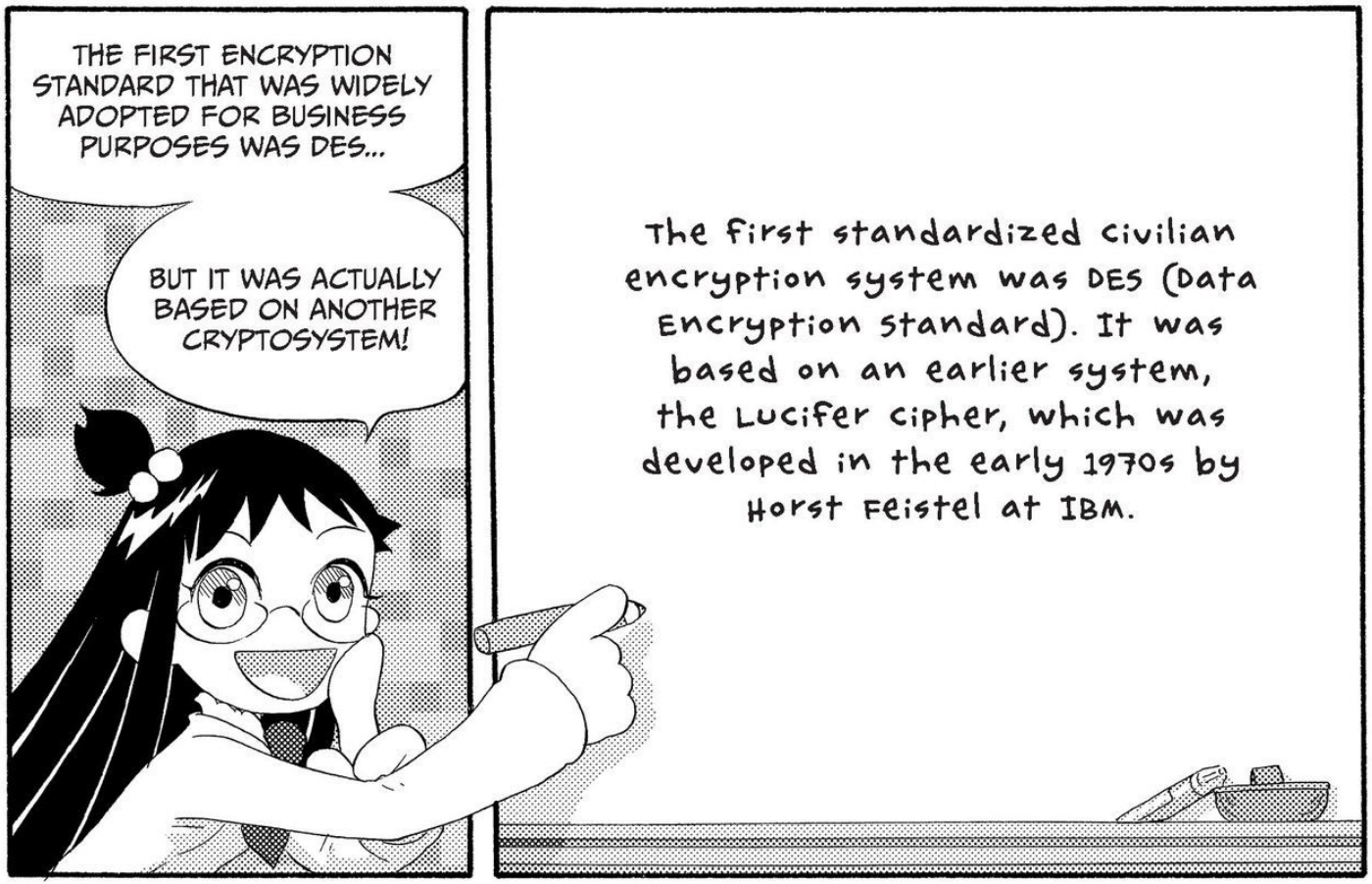
Pasos 3, 4 y 5


32 bits
32 bits
④ XOR operation
Round function f
③ Encryption subkey K_1
Round 1
$L_1 = R_0$
$R_1 = L_0 \square f(R_0, K_1)$
32 bits
32 bits
⑤ Steps 3 and 5 are repeated for rounds 2–15
XOR operation on R_0 and L_0
Round function f
Encryption subkey K_{16}
Round 16
$L_{16} = R_{15}$
$R_{16} = L_{15} \square f(R_{15}, K_{16})$
32 bits
32 bits

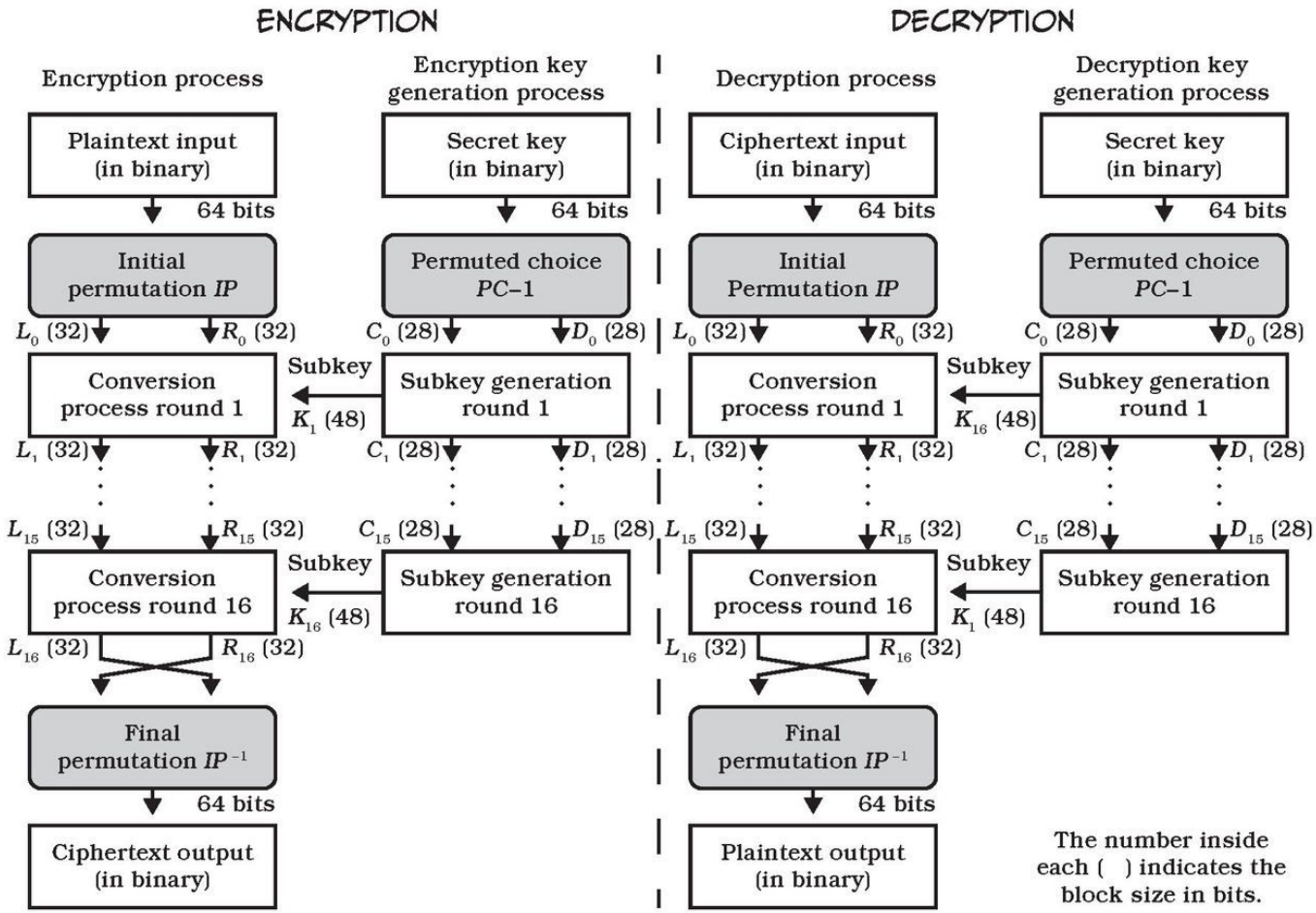
Pasos 6 y 7


32 bits
32 bits
$L_{16} = R_{15}$
$R_{16} = L_{15} \square f(R_{15}, K_{16})$
$L_{16} = R_{16}$
$R_{16} = L_{16}$
32 bits
32 bits
64 bits total
⑥ Final permutation (IP^{-1})
⑦ Output M (64 bits)
Ciphertext C
Perform steps 2–7 on all blocks, then reconstruct them into the ciphertext.

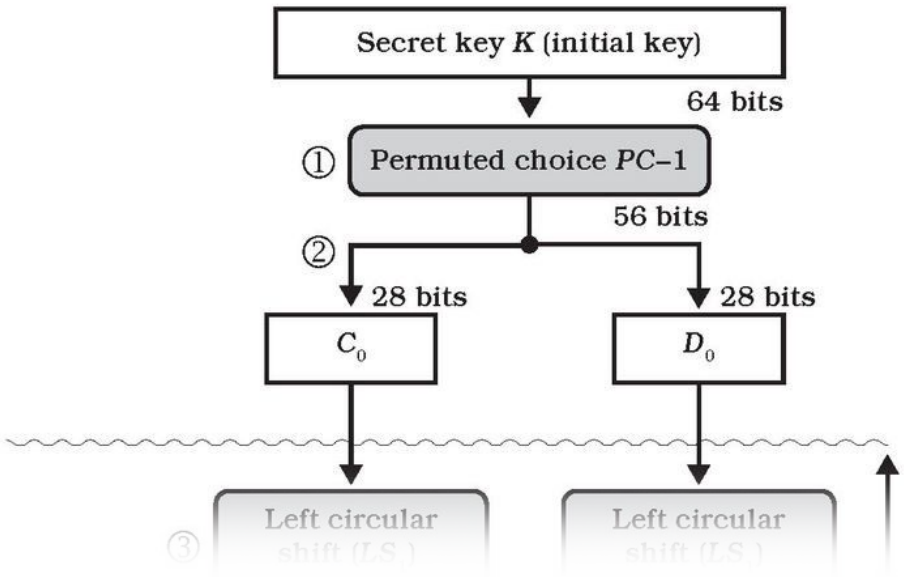
Data Encryption Standard - DES



Funcionamiento Completo de DES



Generación de Sub-Claves - 1

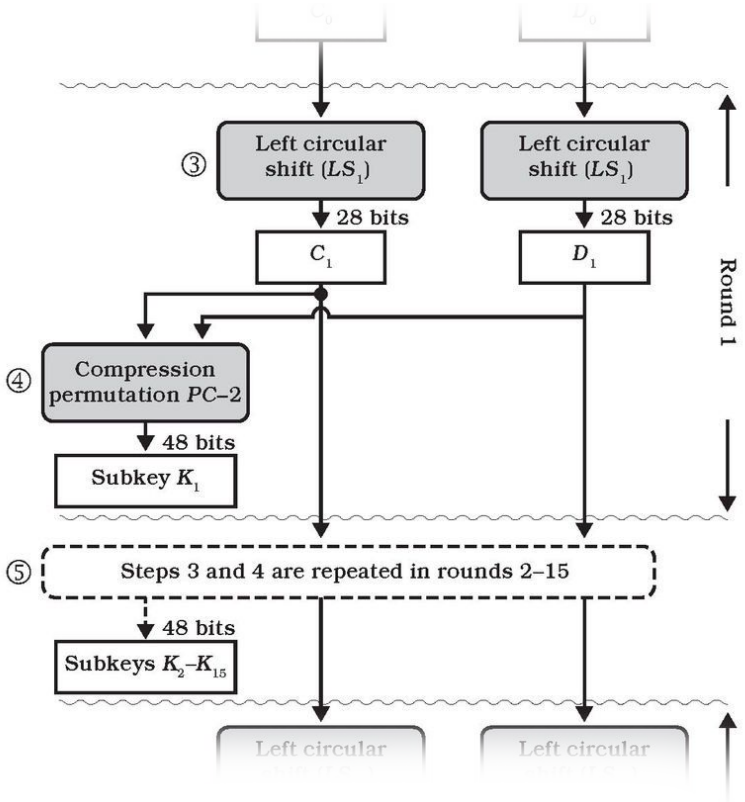


① A permutation called permuted choice 1 (*PC*–1) is performed on the 56 nonparity bits of the initial key. Permuted choice 1 is a special permutation method that transposes each of the 56 bits into specific positions. We won't cover the details of it here.

② The 56 bits are divided into a 28-bit left block (C_0) and a 28-bit right block (D_0).

③ The bits in C_0 and D_0 are left-circular

Generación de Sub-Claves - 2

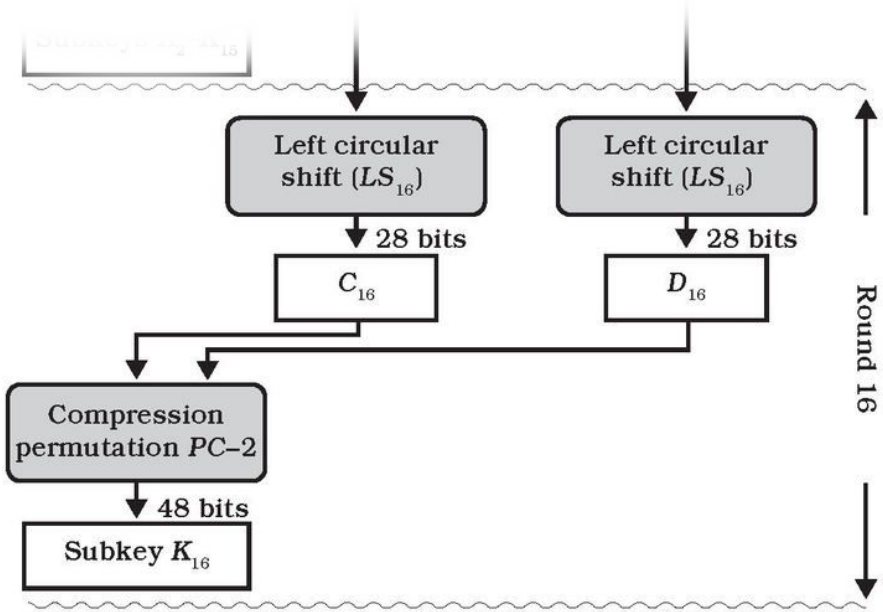


③
The bits in C_0 and D_0 are left-circular shifted to create C_1 and D_1. A left-circular shift moves every bit a certain number of places to the left, and the bits at the beginning of the block are shifted to the very end, as though the block's beginning and end were connected as in a circle.

④
C_1 and D_1 are joined. Then subkey K_1 is made through another permutation, permuted choice 2 (*PC*–2). *PC*–2 is applied to all 56 bits of C_1 and D_1 except for the 8 parity bits, resulting in a compressed 48-bit subkey.

⑤
Steps 3 and 4 are repeated for each round to generate each subkey K_n. Each of these subkeys will then be used for each round in DES.

Generación de Sub-Claves - 3



To generate the decryption subkeys, the bits are right-circular shifted instead. When the initial key is used for decryption, the subkeys are obtained in reverse order from K_{16} to K_1.

Función de Ronda

① The DES function only works on 48-bit blocks, so the rightmost block of data, which is only 32 bits, needs to be expanded using a 48-bit expansion permutation E. This results in the output ER_{n-1}, which is a 48-bit block.

② Perform an XOR operation on the data and the subkey.

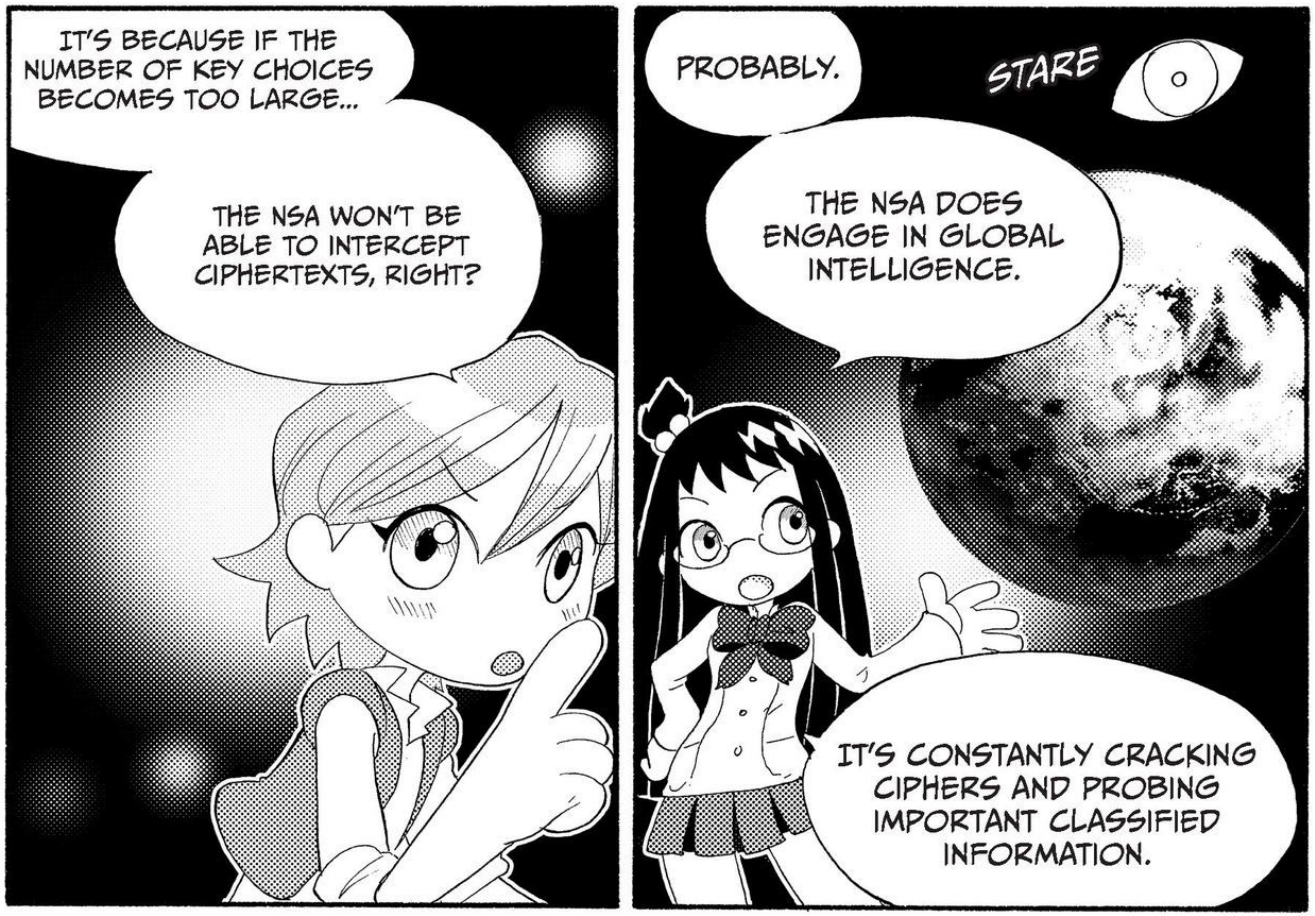
③ Separate the result of the operation into eight sets of 6-bit blocks each.

④ Substitute each 6-bit set of data with 4 bits using S-boxes 1 through 8.

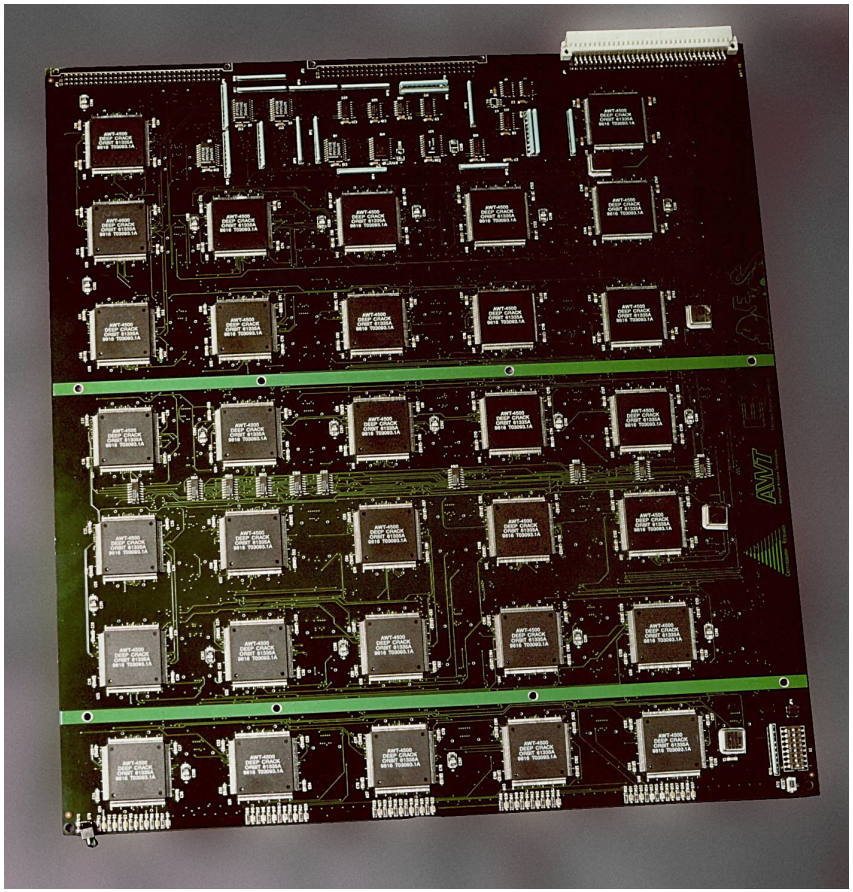
⑤ Combine the S-box output data sequentially to produce a 32-bit block.

⑥ Finally, apply permutation P to the data to yield the output of function f.

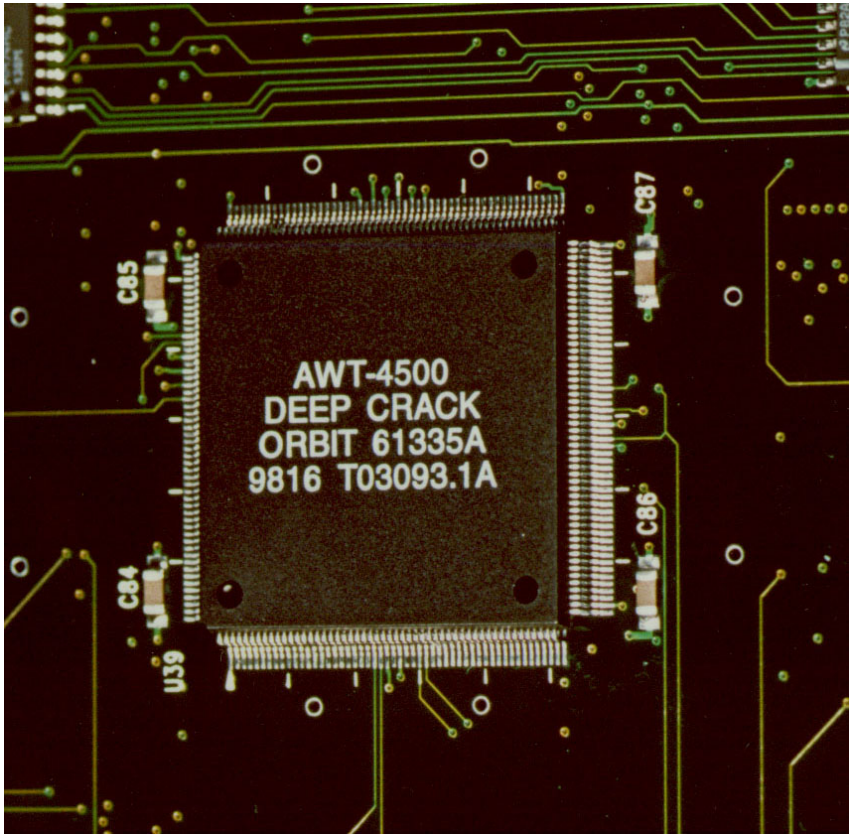
DES es Inseguro



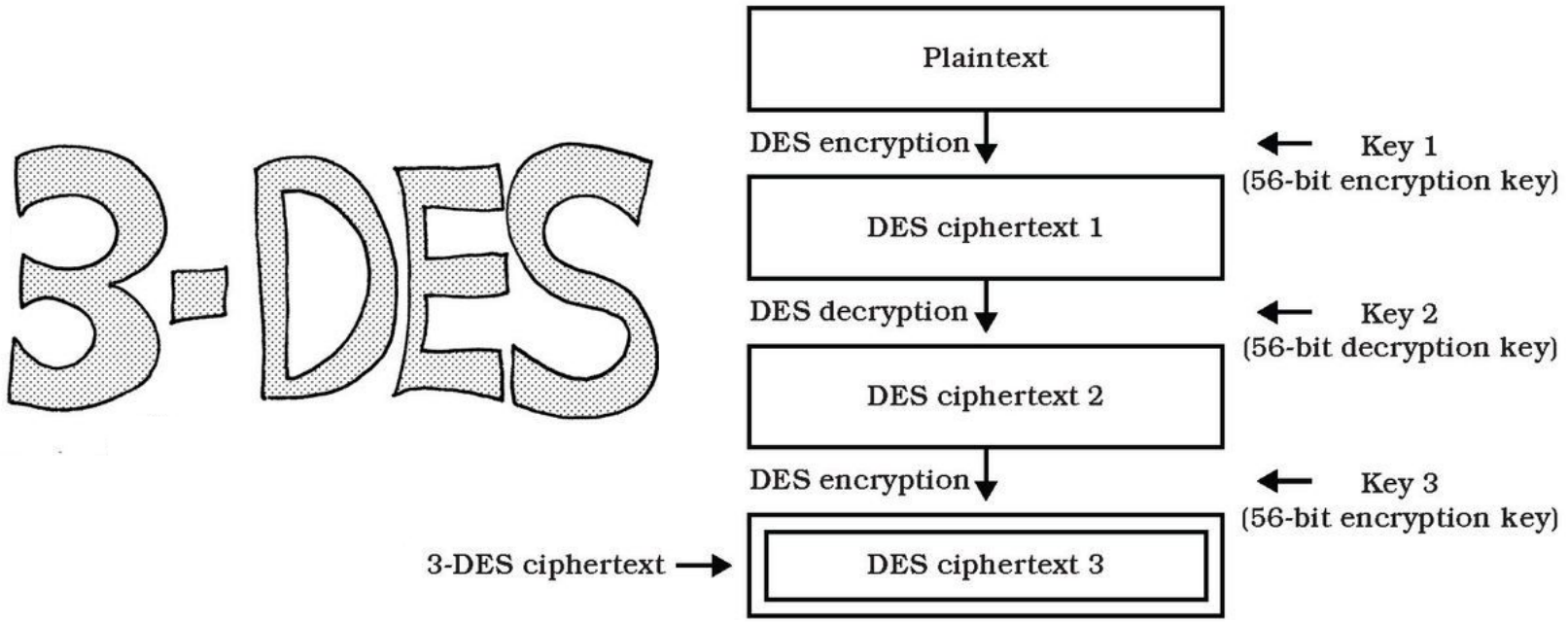
Ataques de Fuerza Bruta



Chip "Deep Crack" de la EFF

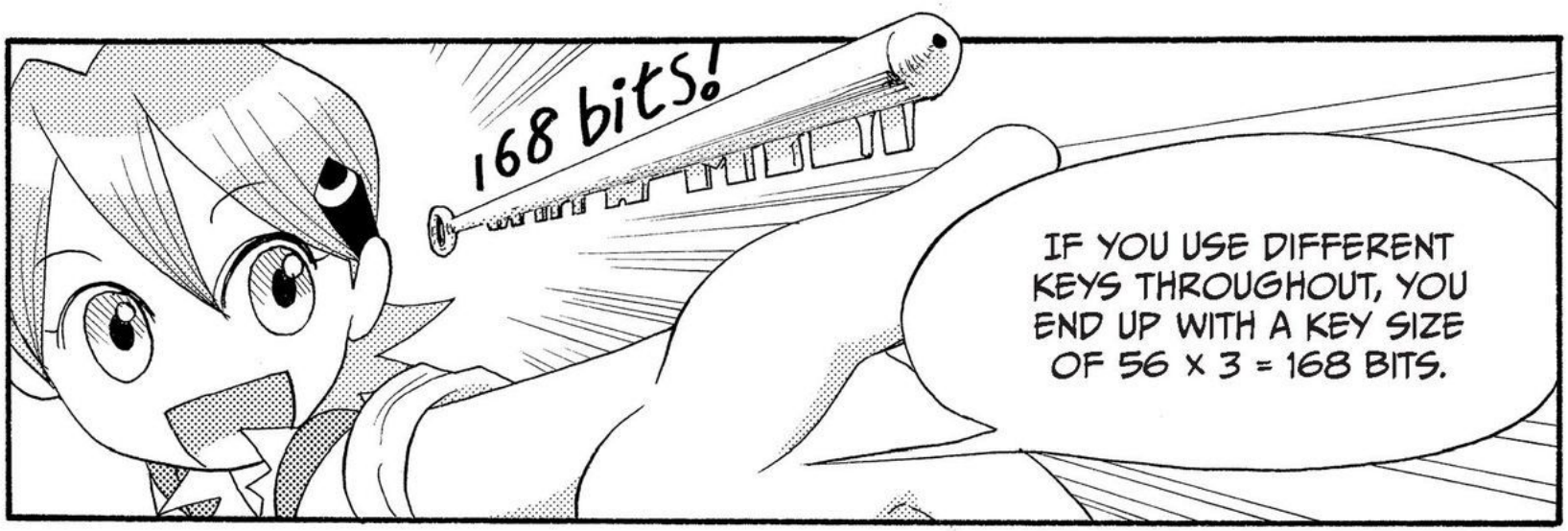


Triple-DES



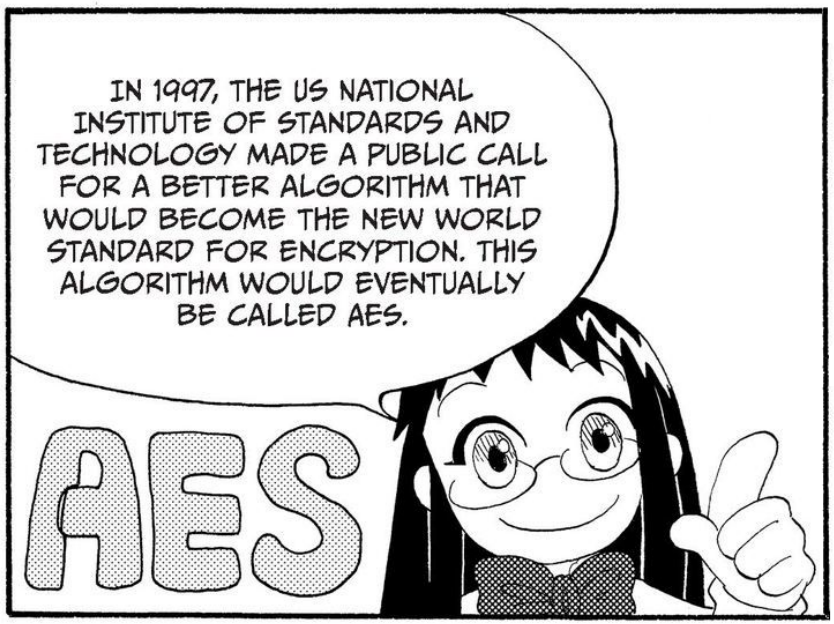
¿Por que la segunda etapa es un desencriptado?

Espacio de Claves en Triple-DES

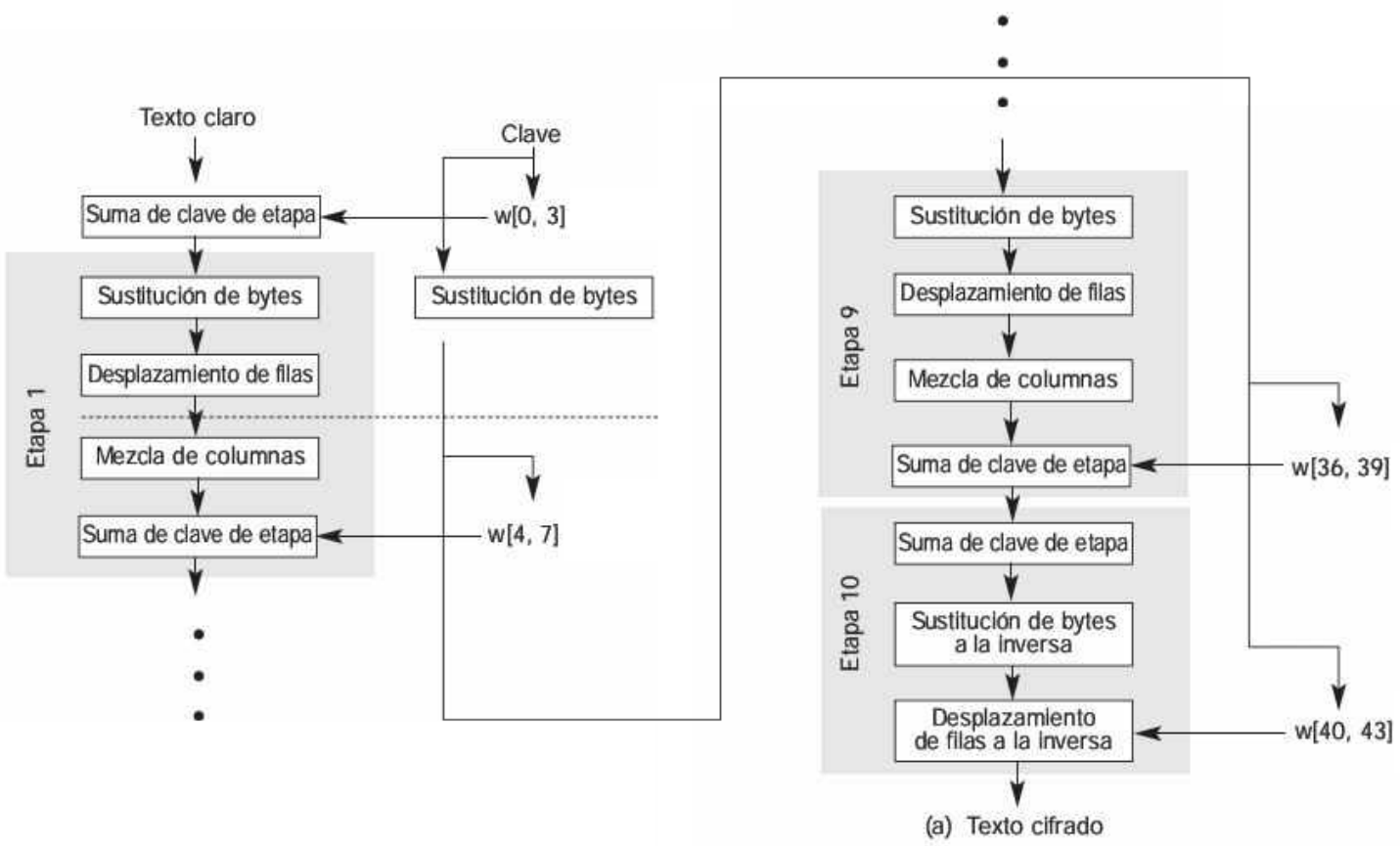


Advanced Encryption Standard - AES

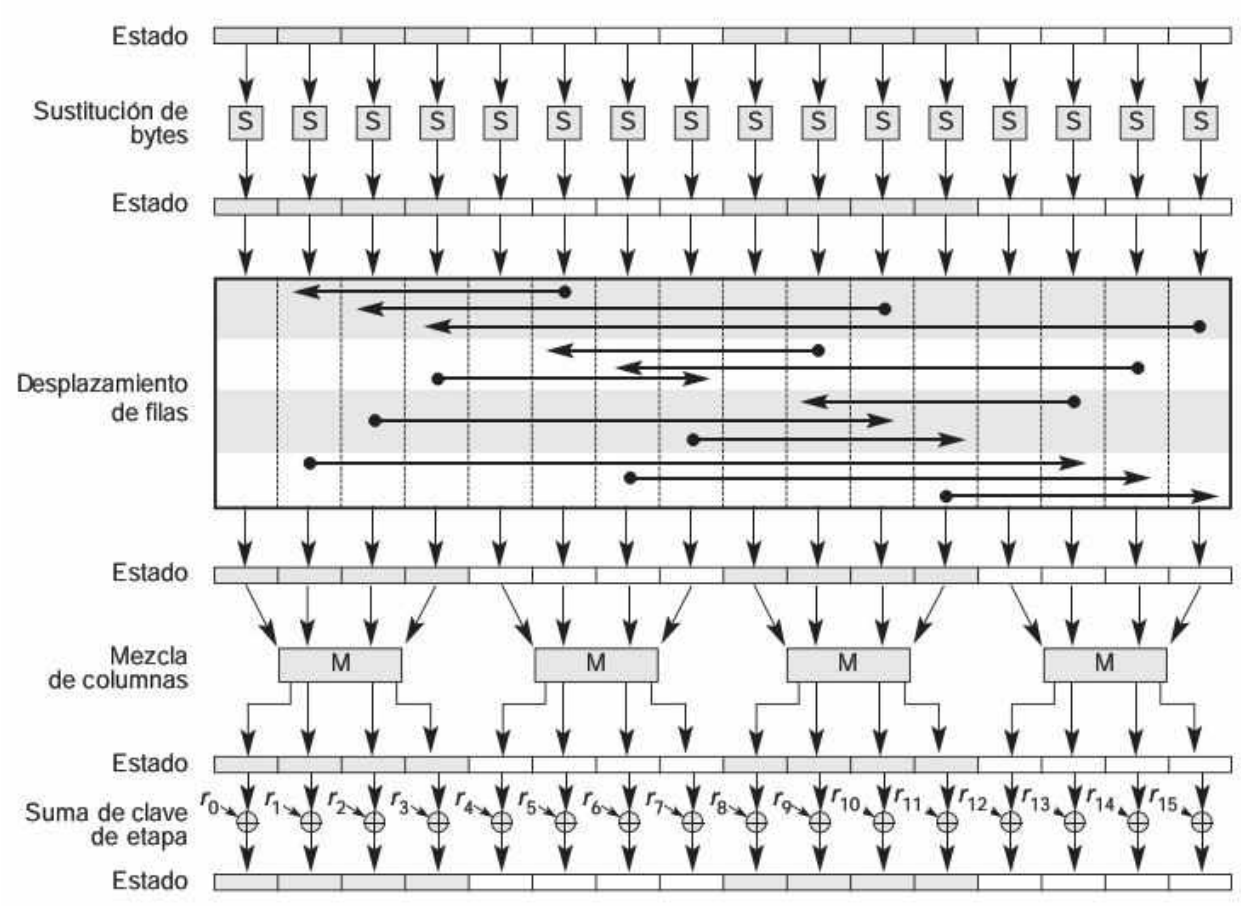
- Especificación del Algoritmo Rijndael.
- Inventado por Daemen y Rijmen en 1997.
- Cifrado de Bloques de 128 bits.
- Tres longitudes de clave:
  - 128 bits.
  - 192 bits.
  - 256 bits.
- Cifrado oficial del gobierno de Estados Unidos.



Etapas de AES



Funcionamiento de Cada Etapa



Conclusiones

- El cifrado simétrico por computadora puede funcionar de dos maneras distintas:
  - Cifrado de flujos.
  - Cifrado de bloques.
- Las técnicas clásicas de sustitución y transposición siguen en uso.
- RC4 es un cifrado de flujo sencillo pero influyente.
- DES demuestra la importancia de diseñar bien todos los criterios de un algoritmo de cifrado.
- Triple-DES y AES son muy sofisticados y robustos.

Próxima Clase

- Distribución de Claves.
- Algoritmo Diffie-Helman.
- Generación de Números Aleatorios.
- Esteganografía.

¿Preguntas?