



Universidad Nacional Autónoma
de México



Facultad de Ingeniería

Cifrado por bloques

Sistemas operativos 2022-1

Grupo 6

Tafolla Rosales Esteban

Vazquez Sanchez Erick Alejandro

Profesor: Gunnar Eyal Wolf Iszaevich



ÍNDICE

CIFRADO POR BLOQUES	2
Criptografía y cifrado	3
Algoritmos de cifrado simétricos	4
Cifrado por bloques	4
DES (Data-encryption Standard)	5
Permutación inicial y final	6
Generador de llaves	7
Rondas Feistel	7
F (Función Feistel)	8
Triple DES	8
AES (Advanced Encryption Standard)	8
Para finalizar	11
Referencias	11

CIFRADO POR BLOQUES

La seguridad de un sistema no solo depende de la protección que este implementa, también se debe considerar el ambiente al que va a estar expuesto, sin embargo en una red de computadoras no se puede conocer con exactitud si el mensaje es legítimo o fue alterado en el trayecto por algún atacante, quien tratará de obtener la información intercambiada para manipularla maliciosamente.

En la presente investigación nos centraremos en definir la forma en que el sistema implementa la criptografía para establecer una conexión segura, en donde los atacantes no puedan tener acceso a los mensajes intercambiados entre dos computadoras y en concreto revisaremos los algoritmos de cifrado simétricos basados en el cifrado por bloques.

Criptografía y cifrado

Para poder empezar, es importante entender en qué consiste la criptografía. La criptografía es lo que hace posible a un sistema olvidarse por completo de confiar en una red, pues en la criptografía existe una y una sola llave que permite conocer el mensaje enviado a otro sistema, por lo que el sistema de origen y el de destino deberán de conocer exactamente la misma llave para poder leer el contenido del mensaje. Hasta aquí todo viento en popa, pero ¿cómo es que las dos computadoras conocen la misma llave para descifrar un mensaje en común sin exponer esa llave a través de una red insegura?

Los algoritmos de cifrado serán los encargados de cifrar un mensaje e intercambiar la llave empleada entre un sistema y otro para que los mensajes compartidos mediante una red no segura no puedan ser descifrados por ningún atacante. Estos algoritmos se utilizan en todas partes para mantener una comunicación secreta, ya sea para mandar un mensaje mediante whatsapp o para hacer una copia de un repositorio de git desde github.

Un algoritmo de cifrado está compuesto por 3 propiedades principales:

- una llave;

- una función que genera un mensaje cifrado;
- una función que descifra un mensaje

y se puede categorizar en dos ramas, simétricos y asimétricos, pero para nuestro propósito nos centraremos en los algoritmos de cifrado simétricos.

Algoritmos de cifrado simétricos

Un algoritmo de cifrado simétrico es empleado en sistemas que utilizan la misma llave para cifrar y descifrar un mensaje. Sin embargo en estos algoritmos la seguridad se basa en la complejidad de la llave, pues si alguien la descubre, independientemente del algoritmo que se esté empleando para cifrar los mensajes, será muy fácil descubrir el contenido. Por lo tanto el principal inconveniente en este tipo de algoritmos es el intercambio de la llave entre dos sistemas, ya que para un atacante es más sencillo interceptar el intercambio de la llave en una red que tratar de descifrarla.

Cifrado por bloques

En algunos algoritmos de cifrado simétrico se emplea el cifrado por bloques. Para el cifrado por bloques la información se divide en grupos de longitud estática llamados bloques los cuales se les aplica una transformación mediante una función biyectiva.

(Diagrama 1.1)

Para hacer un cifrado por bloques efectiva, se deben cumplir los siguientes requisitos:

1. El tamaño de la llave debe ser lo suficientemente grande para que el poder computacional necesario para atacar y romperla sea ridículo.
2. De preferencia cada entrada debe de dar una salida distinta.

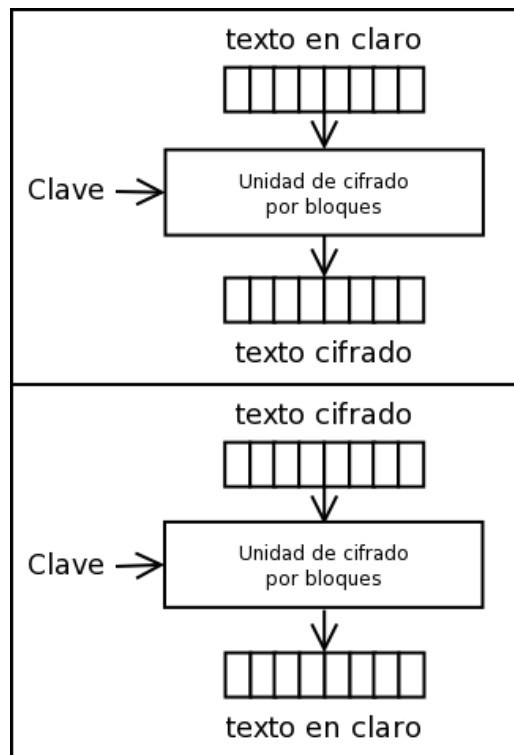


Diagrama 1.1 - Cifrado por bloques

Ilustrando lo anterior, entraremos a detalle en dos algoritmos de cifrado simétrico basados en el cifrado por bloques, DES y AES.

DES (Data-encryption Standard)

DES es un algoritmo que implementa el cifrado por bloques, publicado por el Instituto Nacional de Tecnología Estándar (NIST) en Estados Unidos. De manera general, este algoritmo está basado en las rondas de feistel y funciona tomando un valor de 64 bits del mensaje original, y una llave de 56 bits para cifrar un bloque.

El algoritmo DES está conformado de tres especificaciones principales:

- una función de ronda;
- una llave;
- permutación inicial y final;

y su estructura se muestra en el *Diagrama 1.2*.

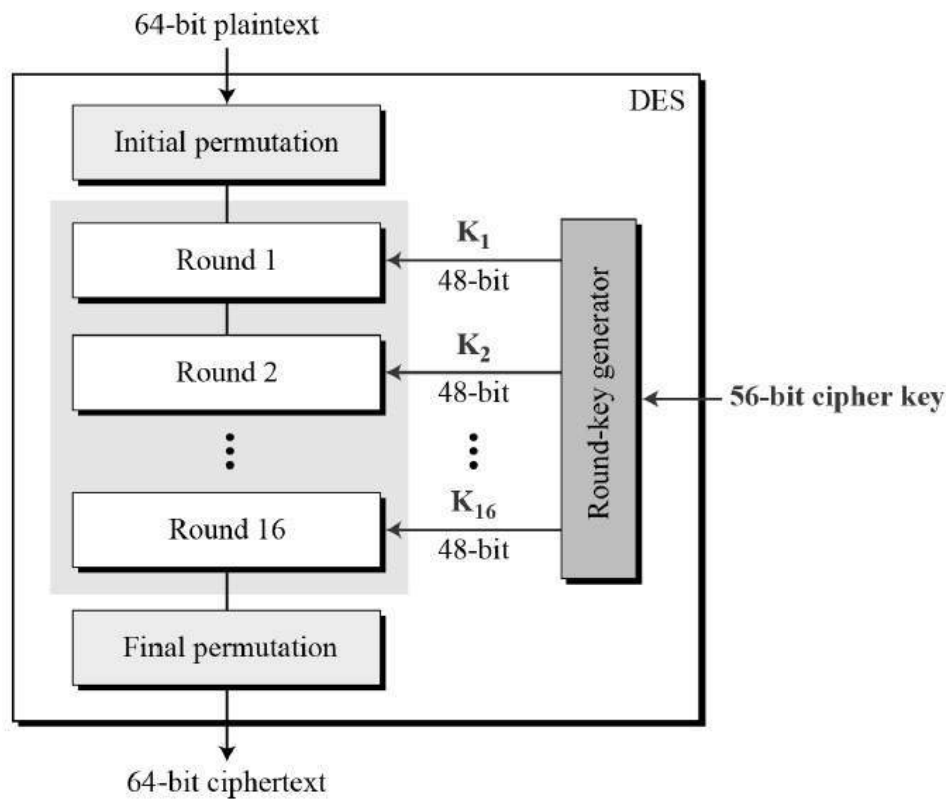


Diagrama 1.2 - Esquema DES

Permutación inicial y final

Estas permutaciones obtienen de una entrada una salida desplazando x valores los bits. (Diagrama 1.3)

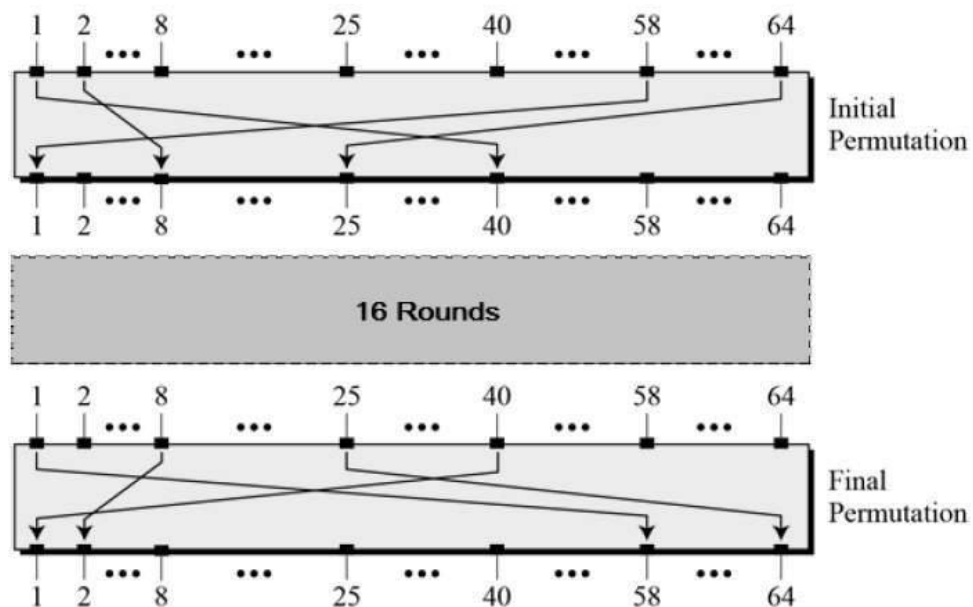


Diagrama 1.3 - Permutación inicial y final

Generador de llaves

Partiendo de la clave de 56 bits del comienzo, en cada una de las 16 rondas se genera una llave de 48 bits.

Rondas Feistel

El algoritmo DES consiste en realizar 16 rondas Feistel que siguen la estructura del *diagrama 1.4*, donde observamos que se reciben dos bloques, uno izquierdo y uno derecho.

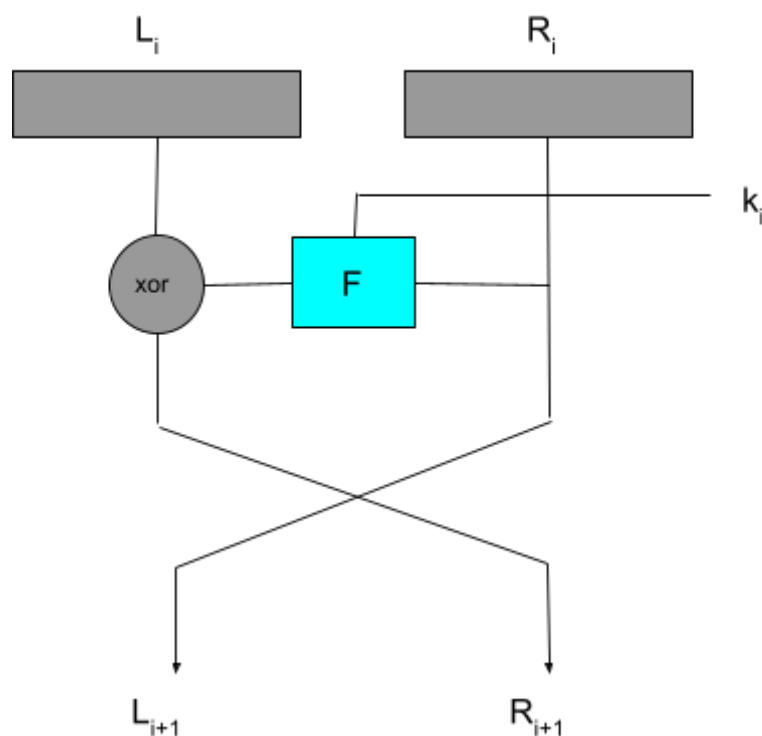


Diagrama 1.4 - Función de ronda

Partiendo del diagrama, la ronda de Feistel funciona de la siguiente manera: como entrada se reciben dos bloques de 32 bits (L_0 y R_0), el bloque derecho es procesado mediante una función F y la salida de esta función se combina mediante una operación lógica, xor, con el bloque izquierdo. Por último, se intercambian los resultados obtenidos, el bloque derecho pasa al izquierdo y viceversa, dando la entrada a una nueva ronda.

F (Función Feistel)

A la función F se le manda como argumentos una llave de 48 bits y un bloque (R_i) de 32 bits. Lo primero que se hace es realizar una permutación de expansión al bloque para convertir esos 32 a 48 bits, esta operación ya está predefinida por el estándar de DES y lo que se hace es repetir algunos bits para rellenar los espacios faltantes. (*Diagrama 1.4*)

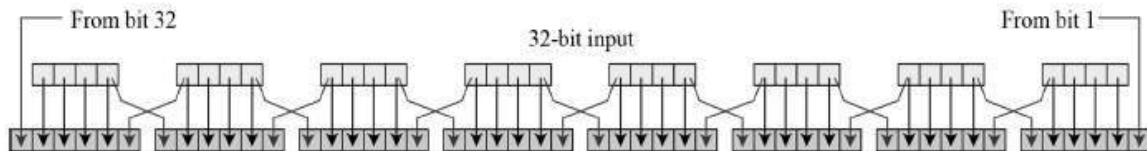


Diagrama 1.4 - Permutación de expansión

Después de esto se realiza una operación lógica, xor, combinando la llave y el bloque, y por último, se realizará la última permutación dentro de la función para convertir la salida de 48 bits en una de 32 bits.

Triple DES

En la actualidad el algoritmo DES no es un método seguro para el cifrado de información, pues mediante fuerza bruta se puede encontrar la llave de 56 bits (porque es una longitud relativamente pequeña).

Debido a este problema Triple DES fue elegido para suplantarlo al algoritmo DES. Este algoritmo consiste en realizar 3 veces el cifrado de la información mediante DES, obteniendo una llave de 168 bits y haciéndolo mucho más seguro. Sin embargo, no entraremos en detalle con este algoritmo.

AES (Advanced Encryption Standard)

AES nace de la búsqueda de un nuevo algoritmo de cifrado para sustituir a DES e implementa el cifrado por bloques del tamaño de 128 bits con llaves de longitud de 128, 192 o 256 bits. El algoritmo se basa en una matriz de tamaño 4 x 4 donde a sus celdas se le aplican sustituciones, permutaciones y transformaciones lineales.

Dependiendo del tamaño de la llave será en número de vueltas que se realizarán al algoritmo

- 128 bits se hacen 10 vueltas al algoritmo
- 192 bits se hacen 12 vueltas al algoritmo
- 256 bits se hacen 14 vueltas al algoritmo

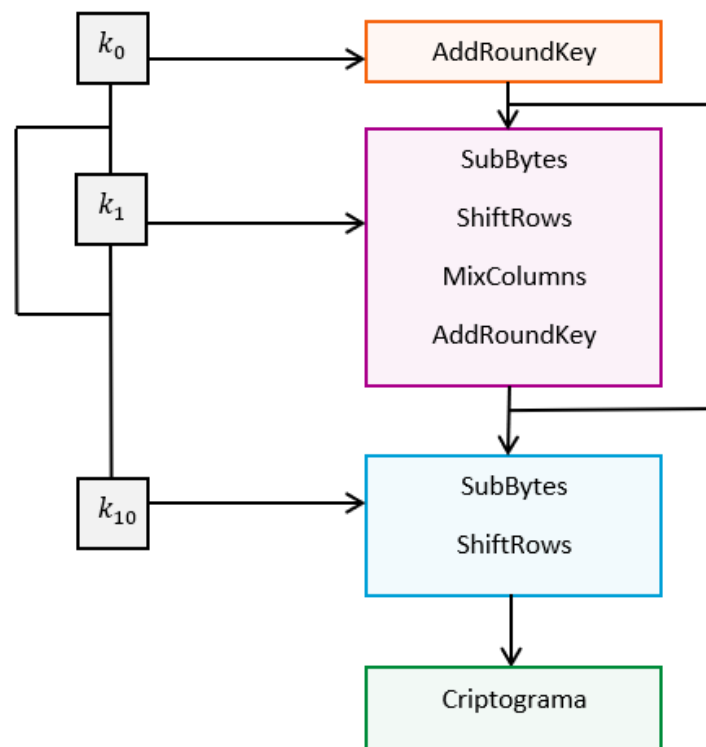


Diagrama 1.5 - Cálculo del criptograma

La matriz 4 x 4 se llena de arriba hacia abajo y de izquierda a derecha con el bloque 128 bits del mensaje.

AddRoundKey

Realiza la operación XOR entre la matriz obtenida de la llave obtenida durante la vuelta.

SubBytes

Se realiza una sustitución de los elementos de la matriz por otra de una tabla de búsqueda.

ShiftRows

Ejecuta permutaciones de las filas del estado donde el primer elemento no rota ninguno, el segundo uno, el tercero dos y el cuarto tres.

MixColumns

Opera las columnas con una transformación lineal.

Para cada vuelta se genera una llave distinta a partir de la llave inicial.

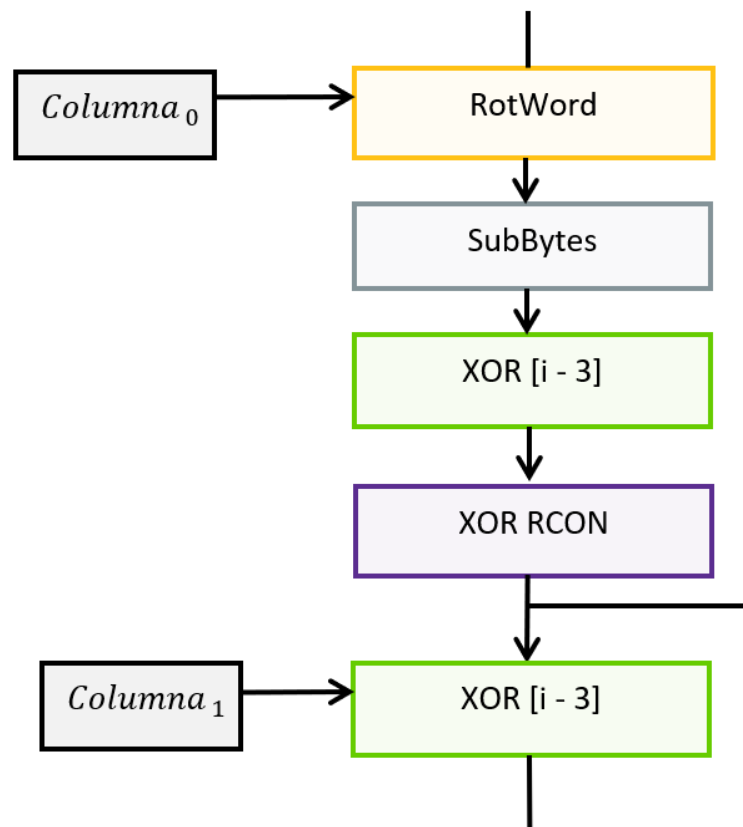


Diagrama 1.6 Cálculo de las Subclaves

RotWord

Mueve el primer elemento de la última columna al final de la columna

XOR [i-3]

Se le aplica XOR con la última columna de la matriz y la columna que se encuentra tres posiciones detrás

XOR RCON

A la columna se le aplica un XOR con el vector RCON el cual es diferente para cada vuelta de la llave.

Después de realizar las operaciones en la columna se inserta al final de la matriz.

Para el primer elemento de la matriz se hacen cuatro operaciones, para las otras tres columnas solo se aplica la operación XOR [i-3]

Para finalizar

Recapitulando lo visto, sabemos que la criptografía hace posible enviar mensajes sin que nadie pueda descifrarlos, y para encriptar estos mensajes se puede hacer uso de algoritmos simétricos y asimétricos. Dentro de los algoritmos simétricos encontramos algoritmos como el DES y el AES, los cuales están basados en el cifrado por bloques, resultando así en un mensaje encriptado.

Referencias

- Silberschatz, A. Galvin, P. Gagne, G. (2005, pp. 559 - 573, 576 - 579). Operating System Concepts. Estados Unidos : 7ma Edición.
- MDN contributors (27 Nov 2021), Criptografía de clave simétrica, MDN Web Docs. Recuperados de:
https://developer.mozilla.org/es/docs/Glossary/Symmetric-key_cryptography
- Ramírez R. (2015), ALGORITMOS SIMÉTRICOS, CRIPTOGRAFIA. Recuperado de: <https://criptografia.webnode.es/algoritmos-simetricos/>
- Anónimo. (2007), Cifrado por bloques - Sección Redes, de GlosarioIT Sitio web: https://www.glosarioit.com/Cifrado_por_bloques
- Redondo A. (11 Oct 2016), AES (Advanced Encryption Standard) [Presentación PowerPoint], Ingeniería en Computación, Centro Universitario

UAEM Zumpango

<https://ri.uaemex.mx/bitstream/handle/20.500.11799/64476/secme-35753.pdf?sequence=1&isAllowed=y>

- Anónimo. (2006). Data Encryption Standard, de tutorialspoint Sitio web: https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm
- Wikipedia (15 feb 2021), Cifrado por bloques, Wikipedia. Recuperado de : https://es.wikipedia.org/wiki/Cifrado_por_bloques#:~:text=En%20criptograf%C3%ADa%2C%20una%20unidad%20de,bloques%2C%20aplic%C3%A1ndoles%20una%20transformaci%C3%B3n%20invariante.&text=Para%20cifrar%20mensajes%20m%C3%A1s%20largos.utiliza%20un%20modo%20de%20operaci%C3%B3n.
- shubhamupadhyay. (8 Nov 2021). Data encryption standard (DES), de GeeksforGeeks Sitio web: <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>
- Saenz, E. [Derivando] (29 Abr 2015). Cómo funciona la criptografía [Video]. Youtube. <https://www.youtube.com/watch?v=Q8K311s7EiM>
- Enoc.[Gina Tost] (22 Ene 2019). SECRETOS de la Criptografía ¿Cómo funciona? ¿Hay tipos? | Gina Tost [Video]. Youtube <https://www.youtube.com/watch?v=RtPm9ub2RIY>
- [Unidad de Innovación UMU] (22 Jun 2015). Módulo 1- Data Encryption Standard (DES) [Video]. Youtube. <https://www.youtube.com/watch?v=5R6iTmawrR0>
- Ramió, J [UPM](2 Nov 2015). Píldora formativa 30: ¿Cómo se cifra con el algoritmo AES? [Video]. Youtube. <https://www.youtube.com/watch?v=tzj1RoqRnv0>