UNIVERSIDAD DE LA SABANA

Cifrado DES

Seguridad Informática, 7598-2

Robinson Muñoz (0000146502)

robinsonmu@unisabana.edu.co

Chía-Cundinamarca

*Abstract*—The DES product cipher or standard encryption standard studied in this report, takes a 64-bit key and a 64-bit text due to being a bit-oriented cipher, where substitutions and translations are made through 16 rounds to the plain text and the key from which a subkey is generated for each round to be used in the calculation of the internal function of this cipher. The internal function f is where the majority of the work occurs, because in it expansions, substitutions and permutations are made, then only do XOR operations and advance those values until reaching the end.

*Index Terms*—Security, computing, DES, standard, encryption, data, cryptanalysis

I. OBJETIVOS

# A. General

Explorar la operación del algoritmo DES mediante el rastreo de la ejecución. Esto mediante el cálculo de una ronda de forma manual, para posteriormente explorar los diferentes modos de uso del cifrado de bloques.

# B. Específicos

Realizar un análisis interno por cada una de las rondas del algoritmo DES, analizando las salidas de cada ronda.

Comprender los efectos de cambiar bits en los datos de entrada para el algoritmo DES, tales como la clave y texto plano y como esos efectos están relacionados con el efecto avalancha.

Realizar el cifrado manualmente según los procedimientos de DES, para así entender todos los pasos y resultados que se generan en este cifrador de bloque.

II. INTRODUCCIÓN

El cifrado de producto DES o estándar de cifrado estándar estudiado en este informe, toma una clave de 64 bits y un texto de 64 bits debido a que es un cifrado orientado a bits, donde las sustituciones y traslaciones se aplican a través de 16 rondas al texto plano y la clave de la cual se´ genera una subclave para cada ronda, siendo utilizada en el cálculo de la función interna de este cifrador. La función interna f, es donde ocurre la mayoría del trabajo, porque en ella se realizan expansiones, sustituciones y permutaciones, para después solo realizar operaciones XOR y avanzar esos valores hasta llegar al final. En DES se observan fenómenos como la avalancha, al alterar los bits de la clave o texto plano, ya que es un cifrador que trabaja con bits en donde el cambio de un valor puede hacer que ocurra una cadena de cambios en las siguientes rondas.

III. NUCLEO DEL CIFRADOR DE BLOQUES

Para el análisis del algoritmo de cifrado DES, se utiliza una clave dada en hexadecimal, un texto o dato en hexadecimal que se quiere cifrar y el texto cifrado, para así poder corroborar que todos los procedimientos de criptoanálisis lleven a ese texto cifrado y viceversa. Los datos con los que se desarrolló todo el procedimiento son los siguientes.

* Texto Claro: a0 b4 ab 23 3e d1 f6 07
* Clave: e4 c3 ee 7c ec 1e 17 3c
* Texto Cifrado: 51 d7 38 25 10 b9 f4 96

# A. Salidas de cada ronda

Al cifrar el texto plano con la clave usando la Calculadora de DES, se identifica la salida de cada una de las rondas en hexadecimal, más sin olvidar que DES es un algoritmo orientado a bits, ya que con estos se realizan las operaciones y se trabaja en hexadecimal por comodidad como se puede observar en la tabla I. Para la realización de los cálculos se utilizó la calculadora DES, con los siguientes valores iniciales.

|  |  |
| --- | --- |
| *L*0 = 6072*d*2*ac* | (1) |
| *R*0 = 675*f*14*dc* | (2) |

Con lo anterior, en la ronda 5 se tienen los datos de C5=L5R5 con el valor en hexadecimal de 199E1A2F12754629 el cual en binario de 64 bits es correspondiente a la concatenación de L5 = 11001100111100001101000101111 y R5 con el valor de 10010011101010100011000101001, por lo tanto el valor de los datos al inicio de la ronda 5 para producir C5 son; la clave SK5=35 14 1f 3a 2d 3e 0a 1f y el valor de R4, los cuales se usan en la función f pasando SK5 a decimal y luego otra vez a hexadecimal en base 16, f tiene como resultado en hexadecimal el valor de 85e0cc05 el cual se opera en xor con el valor de L5=12754629 para calcular el siguiente R.

# A screenshot of a cell phone Description automatically generated

# B. Alteración de bits en texto plano.

Se procede a cambiar el bit número 10 en la cadena del texto plano, por lo tanto, se pasa de a0b4ab233ed1f607 a a0f4ab233ed1f607 al solo cambiar un bit, con esto se puede identificar que, entre rondas al cambiar un bit en el texto plano, ocurre un efecto avalancha [1] como se puede observar en la tabla II, debido a que en las primeras rondas comienzan a cambiar más y más bits hasta la ronda 10 en este caso.

TABLA II

COMPARACIÓN DE CAMBIOS AL ALTERAR EL TEXTO

|  |  |  |  |
| --- | --- | --- | --- |
| Ronda | C (Texto sin alterar) | C’ (1 bit alterado) | # Cambios |
| 1 | 675f14dc40C07C02 | 675f14dc42C07C02 | 1 |
| 2 | 40C07C02BFDA44F5 | 42C07C02BFDA04E5 | 3 |
| 3 | BFDA44F597958A2C | BFDA04E59E9182AD | 8 |
| 4 | 97958A2C199E1A2F | 9E9182AD70611D77 | 24 |
| 5 | 199E1A2F12754629 | 70611D774BF1F1E | 32 |
| 6 | 1275462941565F5A | 4BF1F1EBB26F6EE | 33 |
| 7 | 41565F5ABE43A19A | BB26F6EE43458DA8 | 32 |
| 8 | BE43A19A9D1555B5 | 43458DA8FA2C3F22 | 33 |
| 9 | 9D1555B529902960 | FA2C3F22F59D2162 | 28 |
| 10 | 29902960D074386 | F59D2162A75E401B | 31 |

# C. Generación de subclaves de cada ronda

En DES, a partir de la clave de 64 bits, se genera por cada ronda una subclave que será utilizada en la función f y así ir cifrando el texto. Al inicio del algoritmo se genera un plan de las claves a usar, iniciando por una permutación PC-1 a la clave de 64 bits que dará como resultado una cadena de 56 bits con 8 de paridad. Así, la clave pasa de e4c3ee7cec1e173c a 171f9de66fdbc8. Luego, se divide la clave en dos grupos C y D de 28 bits cada uno, y a estos se les aplica un corrimiento LS a la izquierda dependiendo de la ronda en la que se está, uno para i= 1, 2, 9, 16 y dos en otro caso [1]. Después de los corrimientos, se toma CiDi de 56 bits para realizarle una permutación PC-2 y ese será el valor de la subclave para la ronda i como se puede visualizar en la Fig.1.

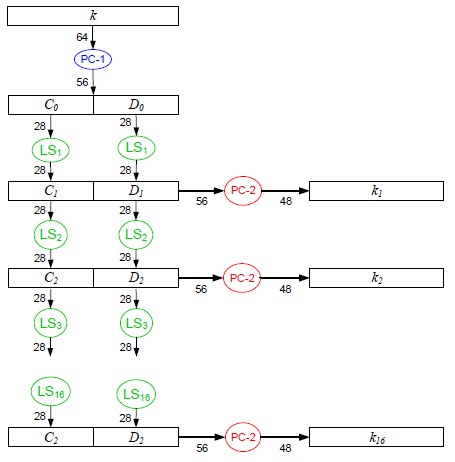


Fig. 1. Diagrama para generación de subclaves para cada ronda de DES. Fuente: [1]

# D. Alteración de bits en la clave

Se procede a cambiar el bit número 20 de la clave de izquierda a derecha, por lo tanto, se pasa de e4c3ee7cec1e173c a e4c3fe7cec1e173c al solo cambiar un bit, con esto se puede identificar que, entre rondas al cambiar un bit en la clave, ocurre un efecto avalancha [1] como se puede observar en la tabla III, debido a que en las primeras rondas comienzan a cambiar más y más bits hasta la ronda 10 en este caso.

TABLE III

COMPARACION DE CAMBIOS AL ALTERAR CLAVE

|  |  |  |  |
| --- | --- | --- | --- |
| Ronda | C Sin cambiar clave | C’ clave cambiada | # Cambios |
| 1 | 675f14dc40C07C02 | 675f14dc42D07802 | 3 |
| 2 | 40C07C02BFDA44F5 | 42D078021BBF056D | 15 |
| 3 | BFDA44F597958A2C | 1BBF056DFBED5422 | 29 |
| 4 | 97958A2C199E1A2F | FBED542252A72F27 | 30 |
| 5 | 199E1A2F12754629 | 52A72F273323883 | 33 |
| 6 | 1275462941565F5A | 33238838FF601D | 31 |
| 7 | 41565F5ABE43A19A | 8FF601D7F2E2460 | 34 |
| 8 | BE43A19A9D1555B5 | 7F2E246043C78247 | 38 |
| 9 | 9D1555B529902960 | 43C7824764C76A47 | 37 |
| 10 | 29902960D074386 | 64C76A47CE46D072 | 31 |

# E. Confusión y difusión en DES.

DES es conocido como un cifrador de producto, por lo tanto, usa transposición y sustituciones para así tener un cifrado más robusto [2]. Con lo anterior, al crear relaciones´ complejas entre el valor cifrado y la clave se cumple con la propiedad de la confusión, en cuanto a la difusión en DES, se disipan las propiedades estadísticas del texto plano haciendo permutaciones de este por cada ronda.

La propiedad de la difusión en algoritmos como DES se ve en al inicio con la permutación inicial y al final, con la última permutación. Más dentro del algoritmo, esta característica, se puede observar en la función interna f, al expandir el valor de Ri-1 de 32 bits a 48. Así el valor de Ro=675f14dc de 32 bits, pasa a ser 30eafe8a96f8 de 48 bits disipando las propiedades estadísticas del texto plano. La propiedad de la confusión en DES, se ve en cuanto a cómo se generan las claves y en como estas tienen relaciones complejas con el valor cifrado. De esta forma, se observa que en DES, las claves pasan por varios pasos para ser utilizadas en una ronda, estos son; empezando por la permutación inicial para la clave, los desplazamientos que dependen de la ronda y la permutación PC-2 que une los bloques C y D´ de la clave, por lo que la clave se genera aparte del cifrado. Por lo tanto, a la clave e4c3ee7cec1e173c se le aplica una permutación inicial la cual la convierte en 171f9de66fdbc8 de 56 bits para luego ser rotada a la izquierda 1 vez en la ronda 1 quedando como 2e3f3bccdfb790.

IV. RONDA DEL CIFRADOR DE BLOQUE

Datos iniciales de la ronda 2 obtenidos de la calculadora DES, texto sin modificar con la clave la cual se pasó a decimal y luego a binario con el uso de la calculadora converter.eu de hexadecimal a decimal, tomando pares los pares de valores de hexadecimal.

*R*1 = 40*c*07*c*02 (3)

*SK*2 = 2*d*0*d*3*c*07061*f*0*c*37 = *B*4*DF*0719*F*337 (4)

*L*2 = 675*f*14*dc* (5)

*f*(*R*1*,SK*1) = *d*8855029 (6)

Con todos los valores anteriores, se procede con el cálculo del valor de la función interna usando los valores de ec. 3.´ Por lo tanto, de acuerdo con la definición de la función interna´ f, se debe de realizar una expansión de los bits de eq.3 para´ luego realizar un XOR con la clave y tener una cadena de 48 bits agrupados de a 6. De esta forma para expandir se usa la configuración presente en la tabla IV.

TABLE IV

TABLA DE FUNCION DE EXPANSIÓN A 48 BITS.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |

Una vez se realizada la expansión como se observa en la tabla V, el cual tiene un valor en hexadecimal de 2016003F8004. Ya con este valor, se procede a realizar la operación de XOR con el valor de la clave para la ronda 2 ec. 4, esto dando como resultado el valor de ec. 7.

*E XOR SK*2 = 94*c*907267333 *HEX* (7)

TABLE V

TABLA DE BITS DE R1 EXPANDIDOS A 48 BITS.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 |

El valor de ec. 7 en binario tiene 48 bits, los cuales se agrupan en 8 grupos de a 6 cada uno. Para así realizar las sustituciones con las cajas S correspondientes en donde cada salida de cada caja será de 4 bits para que con los 8 grupos se formen los 32 bits que serán permutados, finalizando la función interna de DES. En las sustituciones, a cada grupo de 7 bits se les aplica una caja de sustituciones, tomando los bits 1 y 6 para saber en qué fila está el valor a sustituir y los demás valores desde los bits 2 al 5, son para la columna. Al realizar las sustituciones en cada grupo, los nuevos valores de C son 10000011010001010100110010001100 una vez se unen los grupos sustituidos, ver sección de apéndice al final. Para cada una de las sustituciones en el Excel página Parte B. Después, para finalizar la función interna f, se procede a calcular la última permutación la cual está presente en la tabla. VI, luego de expandir la tabla a lo largo, queda una cadena de 32 bits equivalente al valor de la función generado por la calculadora es decir d8855029.

TABLE VI

TABLA DE PERMUTACION FINAL EN LA FUNCIÓN INTERNA .

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |

Con el valor de ec. 6 se procede a realizar la operación´ XOR con el valor de ec. 5 la cual da como resultado la ec. 8 la cual se usa en la ronda 3 como parámetro para la función´ interna f.

*R*2 = *bfda*44*f*5 (8)

Con lo anterior el valor cifrado al de la ronda 3 es L2R2 es decir el valor de BFDA44F597958A2C en hexadecimal. Finalmente, comprobando que los valores generados por la caculadora en la ronda 3 coinciden con los que se calcularon manualmente.

V. CONCLUSIONES

* El desarrollo de algoritmos de encriptación como DES, contribuyo inmensamente a la evolución de los algoritmos para la seguridad informática como lo es el AES, el cual reemplazo DES.
* Con el pasar del tiempo y la creación de nuevas y m´ as´ sofisticadas técnicas de cifrado, los algoritmos actuales´ se pueden quedar obsoletos y tendrán que ser renovados, para con ello satisfacer nuevas necesidades en sistemas de información.
* Para contribuir a la robustez de un algoritmo de cifrado, se deben de considerar características como la confusión y la difusión para que el posible rompimiento de este´ sea difícil de realizar, esto usando cifradores donde se usen traslaciones y sustituciones, es decir cifradores de producto como DES.

REFERENCIAS

[1] Ferney A. Maldonado PhD, Cifradores de bloque(presentación), 2020. [2] M. Bishop, *Computer Security, 2nd Edition*. Pearson Education, 1996.

APPENDIX

Archivo Excel con cálculo de rondas a partir del uso de la calculadora DES: shorturl.at/EKNW3