Criptografía: Data Encryption Standard

M. en C. Víctor M. Silva G.,
M. en C. Eduardo Rodríguez Escobar,
M en C. Eduardo Vega Alvarado.
Profesores del CIDETEC-IPN.

Desde la época del imperio romano, los hombres de estado deseaban enviar mensajes, ya sea al frente de batalla o a algún personaje importante, donde la condición era que el mensaje fuese secreto, esto es, que nadie aparte de ellos dos, el que envía y el que recibe, se enterara del contenido. En aquellos tiempos la encripción y la desencripción se trabajaba de forma manual y se hacía por medio de mascarillas, corrimiento de las letras del alfabeto, etc. En general se puede afirmar que hay tres tipos de elementos en todo proceso criptológico, llamémoslos A, B y C. El elemento A es el que desea enviar el mensaje, el elemento B el que lo recibe y C es el que desea conocer el contenido del mensaje que A envía a B.

En este trabajo se describe un criptosistema ampliamente utilizado en el mundo cuyo nombre es DES (Data Encryption Standard), siendo nuestro interés meramente educativo y con el fin de despertar en el alumnado la curiosidad por la Criptografía.

El criptosistema DES fue desarrollado por IBM y sale a la luz el 15 de enero de 1977, siendo revisado cada cinco años por el Buró Nacional de Normas de USA.

DESCRIPCIÓN DEL ALGORITMO

Se empezará con una descripción de alto nivel, consistente en presentar los aspectos importantes del criptosistema de una forma general y detallar mas adelante la mayoría de ellos. Por sencillez y para la mayor comprensión de DES, se considerará como texto claro a una cadena de 64 bits, tomando cuatro bits para cada carácter del sistema hexadecimal.

El algoritmo procede de acuerdo a los siguientes tres pasos:

Paso 1.- Se contará con una matriz PI de 8x8 (fija) la cual efectuará una permutación inicial sobre una cadena de texto claro X de 64 bits:

PI(X) = X_o .

La cadena X_0 se divide en dos subcadenas de 32 bits, pudiéndose representar como:

$X_o = L_o\ R_o$;

L_0 son los primeros 32 bits y R_0 son los 32 bits restantes.

Paso 2.- Se calcularán las subcadenas L_i, R_i en 16 iteraciones de acuerdo a la siguiente regla:

$L_i = R_{i-1}$ y

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Aquí, $\oplus$ representa la operación de "o exclusivo".

La representación gráfica de un ciclo de encripción DES se muestra en la **figura 1**.

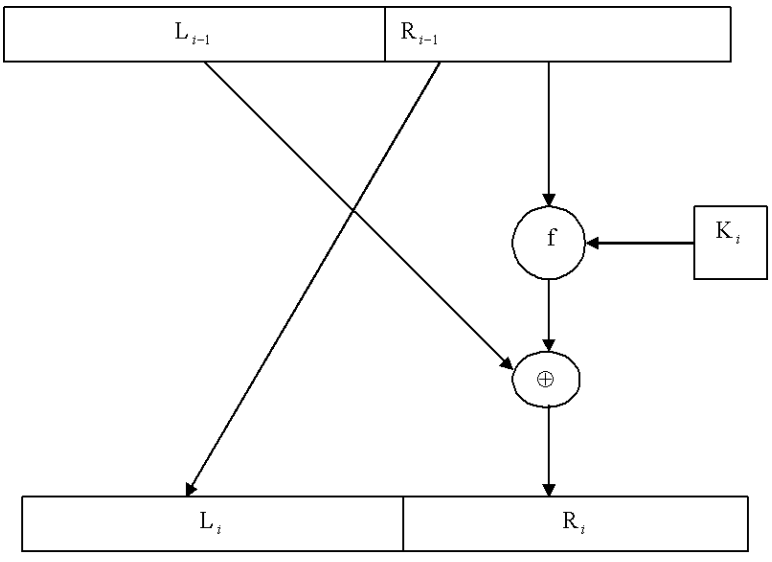


Figura 1. Representación gráfica de un ciclo de encripción DES.

Paso 3.- Al resultado del ciclo 16 se invertirá el orden de aparición de las subcadenas $L_{16}R_{16}$; quedando la cadena $L_{16}R_{16}$, por último, se aplica la permutación inversa PI^{-1} a la cadena $R_{16}L_{16}$ para obtener finalmente el texto cifrado

$Y=PI \quad (R_{16}, L_{16})$

La Función $f(R_{i-1}, K_i)$

Como se observó en el encabezado, la función f tiene dos argumentos R_{i-1}, K_i ; R_{i-1} es una cadena de 32 bits y K_i es una cadena de 48 bits. La función f produce a su vez una cadena de 32 bits. Sin que por el momento expliquemos como se obtiene la cadena de 48 bits de K_i, se describirán los cuatro pasos que se ejecutan para calcular el resultado de f (R_{i-1}, K_i).

Paso 1.- El primer argumento de f, R_{i-1}, es expandido –permutado a una cadena de 48 bits. La función que expande y permuta E (R_{i-1}) es fija.

Paso 2.- Se efectúa la operación

$E(R_{i-1}) \oplus K$

y el resultado se puede pensar como una concatenación de 8 cadenas de 6 bits cada una. Entonces se puede escribir a

$E(R_{i-1}) \oplus K$ como:

$B=B_1\ B_2\ B_3\ B_4\ B_5\ B_6\ B_7\ B_8$

Donde B_i es una cadena de 6 bits, con $1 \leq i \leq 8$

Paso 3.- Se contará con 8 cajas (matrices) de 4 x 16; S_1, S_2,..., S_8. Los renglones de cada una de estas matrices será una permutación de los números enteros entre 0,15, además, estos arreglos cumplen con algunas otras propiedades que no mencionaremos en este artículo. Con esta información se procederá de la siguiente manera:

Para cada B_i dada, el 1° y 6° bit definen el renglón de la matriz S_i y del 2° al 5° bit definen la columna de la matriz S_i. El resultado de esta operación es una sustitución, la cual se expresará como $C_i = S_i(B_i)$.

Como un ejemplo para ilustrar lo anteriormente mencionado, suponga que i = 1 con B_1 = 101101 y que la matriz S_1 está dada por:

$$S_1 = \begin{bmatrix} 14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\ 15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{bmatrix}$$

Entonces $C_1 = S_1(101101) = 0001$

Paso 4.- La cadena $C = C_1\ C_2 \ldots C_8$ de longitud 32 bits es permutada por P (una matriz de permutación fija). El resultado P(C) es definido como f (R_{i-1}, K_i) para el ciclo i.

Las Llaves Programadas K_1, K_2,..., K_{16}

En esta parte se verá como se obtienen las llaves K_1, K_2,....,K_{16} a partir de una llave K de 64 bits.

Paso 1.- Dada una llave K de 64 bits, se desechan los bits 8, 16,..., 64 (8 en total), los cuales se conocen como bits de paridad, a los restantes 56 bits se les aplica una permutación PC-1 (fija), de hecho el orden del número de llaves es de 2^{56}. La cadena de 56 bits resultante se separa en dos subcadenas de 28 bits cada una, esto es,

PC-1 (K) = $C_0\ D_0$.

Paso 2.- Para $1 \leq i \leq 16$ se evalúan las siguientes expresiones :

$C_i = LS_i\ (C_{i-1})$

$D_i = LS_i\ (D_{i-1})$

y K_i = PC-2 ($C_i\ D_i$)

LS_i representa un corrimiento a la izquierda de una o dos posiciones dependiendo del valor de i. Un caso particular sería correr una posición a la izquierda cuando i = 1,2,9,16 y dos posiciones de otra manera. PC-2 es otra permutación fija.

Una mención importante:

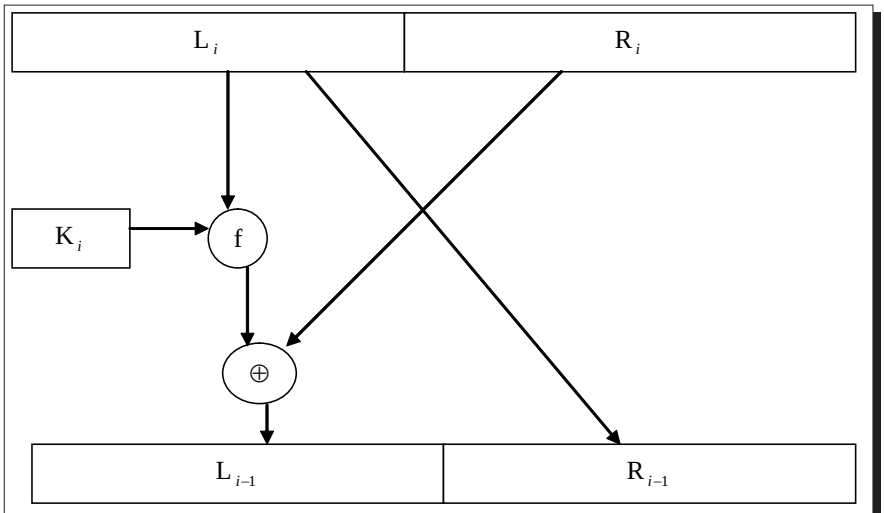
La permutación PC-1 se lleva a cabo en 56 bits y la permutación PC-2 desecha 8 bits y permuta los 48 restantes.

En este punto se ha descrito como procede DES para encriptar un texto claro, así como la forma de obtener las llaves programadas de 48 bits dada una llave de 64 bits; falta por describir como se desencripta un texto cifrado, lo cual se muestra en la **figura 2**.

A continuación se darán los resultados de encriptar varios textos claros, dos de ellos servirán para verificar que el programa que desarrollemos se ajusta a la norma internacional del criptosistema DES. Las cajas y permutaciones que se utilizaron están descritos en el trabajo [2].

Ejemplos:

TEXTO CLARO	LLAVE	TEXTO ENCRIPTADO
0123456789ABCDE	133457799BBCDFF1	85E813540F0AB405
8787878787878787	0E329232EA6D0D73	0000000000000000
SALVADOR	133457799BBCDFF1	8B2411C7EBCABAAF



Representación Gráfica del i-ésimo Ciclo para Desencriptar

Si el texto claro "SALVADOR" se desea expresar en código ASCII el resultado es el siguiente :

Ï $ Ä% Ã Ù i% Q% «

Conclusiones

Actualmente el criptosistema DES se considera poco seguro, claro está, si el valor de la información que se desea encriptar no pasa de determinada cantidad, se podría considerar a DES aún seguro, porque para encontrar la llave (2^{56} posibilidades) por el procedimiento exhaustivo, se necesitaría una supercomputadora con un valor de alrededor de un millón de dólares y la cual se llevaría un tiempo aproximado de 30 minutos. Una solución para resolver esta debilidad de DES es aplicar dos llaves como sigue: Se utiliza una primera llave K_1 para un texto claro dado y la salida de este proceso se toma nuevamente como texto claro para aplicar una llave K_2. Por último, al resultado de este segundo proceso se le aplica la primera llave k_1, el número de llaves posibles en esta situación es de 2^{112}.

Bibliografía

[1] Douglas R. Stinton, *"CRIPTOGRAPHY: Theory and practice"*, CRC Press, 1995, USA.

[2] Orlin Grabbe, *"Data Encripyption Standard: The DES algorithm Ilustrated"*, Laissez faire City Times Vol. 2, número 28, 2003. Página Web del autor: olingrabbe.org

[3] Cevallos Fco. Javier, *"C++: Enciclopedia del lenguaje"*, Alfaomega Ra-Ma, 2004, México.

[4] Schildt Herbert, *"LENGUAJE C : Programación Avanzada"*, Osborne / Mc Graw-Hill, 1987, México.