DES (Estándar de Cifrado de Datos), descifrado de la clave secreta

El 15 de mayo de 1973, el **NBS** (*National Bureau of Standars, en castellano: Agencia Nacional de Normalización*) hoy en día denominada *NIST* (*National Institute of Standars and Technology, en castellano: Instituto Nacional de Normalización y Tecnología*), hizo un llamamiento en el *Federal Register (el equivalente en España del Boletín Oficial del Estado)* para la creación de un algoritmo de cifrado que cumpliera con los siguientes requisitos:

* ofrecer un alto nivel de seguridad relacionado con una pequeña clave utilizada para cifrado y descifrado
* ser comprensible
* no depender de la confidencialidad del algoritmo
* ser adaptable y económico
* ser eficaz y exportable

A finales de 1974, IBM propuso "Lucifer", que gracias a la NSA (National Standard Agency, en castellano: Agencia Nacional de Seguridad) fue modificado el 23 de noviembre de 1976, convirtiéndose en **DES** (*Data Encryption Standard, en castellano: Estándar de Cifrado de Datos*). El DES fue aprobado por el NBS en 1978. El DES fue estandarizado por el *ANSI* (*American National Standard Institute, en castellano: Instituto Nacional Americano de Normalización*) bajo el nombre de *ANSI X3.92*, mas conocido como *DEA*(*Data Encrytion Algorithm, en castellano: Algoritmo de Cifrado de Datos*).

Principio de funcionamiento del DES

Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que [8 bits](http://es.kioskea.net/contents/base/binaire.php3) (un byte) se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad (1 cada 8 bits) se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar de "1" dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud "útil" de 56 bits, es decir, realmente sólo se utilizan 56 bits en el algoritmo.

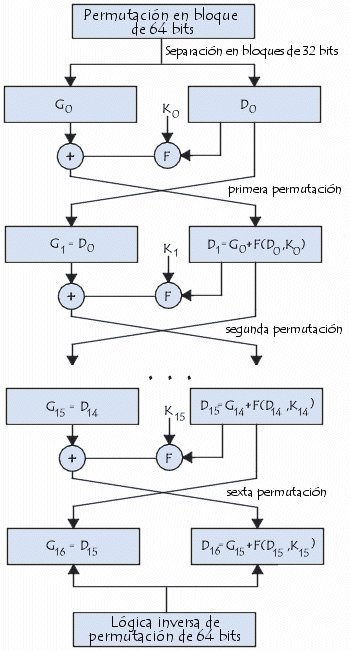
El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado). La combinación entre sustituciones y permutaciones se llama **cifrado del producto**.

La clave es codificada en 64 bits y se compone de 16 bloques de 4 bits, generalmente anotadas de *k1* a*k16*. Dado que "solamente" 56 bits sirven para el cifrado, ¡puede haber hasta 256 (o 7.2\*1016) claves diferentes!

El algoritmo DES

Las partes principales del algoritmo son las siguientes:

* fraccionamiento del texto en bloques de 64 bits (8 bytes),
* permutación inicial de los bloques,
* partición de los bloques en dos partes: izquierda y derecha, denominadas *I* y *D* respectivamente,
* fases de permutación y de sustitución repetidas 16 veces (denominadas **rondas**),
* reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.



Fraccionamiento del texto

Permutación inicial

En primer lugar, cada bit de un bloque está sujeto a una permutación inicial, que puede representarse mediante la siguiente matriz de permutación inicial (*anotada como PI*):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | |

Esta tabla de permutación muestra, al leerla de izquierda a derecha y de arriba a abajo, que el 58o bit de un bloque de 64 bits está en la primera posición, el 50o está en la segunda posición y así sucesivamente.

División en bloques de 32 bits

Una vez que la permutación inicial se completó, el bloque de 64 bits se divide en dos bloques de 32 bits denominados **I** y **D** respectivamente (para izquierda y derecha, siendo la anotación en anglo-sajón L y R por Left y Right). El estado inicial de estos dos bloques se denomina **L**0 y **R**0:

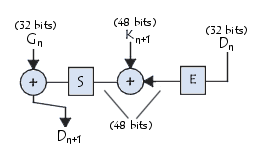
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L**0 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 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 | |

|  |
| --- |
|  |
| **R**0 | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | |

Es interesante observar que **L**0 contiene todos los bits que se encuentran en posición par en el mensaje inicial, mientas que **R**0 contiene los bits en posición impar.

Rondas

Los bloques **L**n y **R**n están sujetos a un conjunto de transformaciones iterativas denominadas *rondas*, que se muestran en este esquema y que detallamos a continuación:



Función de expansión

Los 32 bits del bloque **R**0 se expanden a 48 bits gracias a una tabla (matriz) llamada*tabla de expansión*(que se anota como **E**), en la que los 48 bits se mezclan y 16 de ellos se duplican:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 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 | |

Así, el último bit de **R**0 (es decir, el 7o bit del bloque de origen) se convierte en el primero, el primero en el segundo, etc.   
Además, los bits 1,4,5,8,9,12,13,16,17,20,21,24,25,28 y 29 de **R**0 (respectivamente los bits 57, 33, 25, l, 59, 35, 27, 3, 6l, 37, 29, 5, 63, 39, 31 y 7 del bloque de origen) son duplicados y diseminados en la matriz.

OR exclusiva con la clave

La tabla resultante de 48 bits se denomina **D'**0 o **E**[**D**0]. El algoritmo DES aplica después *OR exclusivas*entre la primera clave **K**1 y **E**[**D**0]. El resultado de este *OR exclusivo* es una tabla de 48 bits que, por comodidad, llamaremos **D**0 (¡no es la **D**0 inicial!).

Función de sustitución

Después, **D**0 se divide en 8 bloques de 6 bits, denominado **D**0i. Cada uno de estos bloques se procesa a través de **funciones de selección** (a veces llamadas *cajas de sustitución* o *funciones de compresión*), denominadas generalmente **S**i.   
Los primeros y últimos bits de cada **D**0i determinan (en valor binario) la línea de la función de selección; los otros bits (2, 3, 4 y 5 respectivamente) determinan la columna. Como la selección de la línea se basa en dos bits, existen 4 posibilidades (0,1,2,3). Como la selección de la columna se basa en 4 bits, existen 16 posibilidades (0 a 15). Gracias a esta información, la función de selección "selecciona" un valor cifrado de 4 bits.

Esta es la primera función de sustitución, representada en una tabla de 4 por 16:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**1 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 | | **1** | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 | | **2** | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 | | **3** | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 | |

Sea **R**01 igual a *101110*. El primer y último bit dan *10*, es decir, 2 en valor binario. Los bits 2,3,4 y 5 dan*0111*, o 7 en valor binario. Por lo tanto, el resultado de la función de selección es el valor ubicado en la línea nº 2, de la columna nº 7. Es el valor *11* o *111* en binario.

Cada uno de los 8 bloques de 6 bits pasa a través de la función de selección correspondiente, dando un resultado de 8 valores con 4 bits cada uno. A continuación están las otras funciones de selección:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**2 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 | | **1** | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 | | **2** | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 | | **3** | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**3 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 | | **1** | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 | | **2** | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 | | **3** | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**4 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 | | **1** | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 | | **2** | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 | | **3** | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**5 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 | | **1** | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 | | **2** | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 | | **3** | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**6 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 | | **1** | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 | | **2** | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 | | **3** | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**7 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 | | **1** | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 | | **2** | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 | | **3** | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S**8 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | | **0** | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 | | **1** | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 | | **1** | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 | | **1** | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 | |

Por lo tanto, cada bloque de 6 bits se sustituye por un bloque de 4 bits. Estos bits se combinan para formar un bloque de 32 bits.

Permutación

Finalmente, el bloque de 32 bits se somete a una permutación **P**. A continuación, mostramos la tabla:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **P** | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 | | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 | | 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 | | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 | |

OR exclusivo

El conjunto de estos resultados salidos de **P** están sujetos a un *OR exclusivo* con **I**0 inicial (como se muestra en el primer esquema) para devolver D1, en tanto que la **D**0 inicial devuelve **I**1.

Iteración

El conjunto de los pasos anteriores (*rondas*) se reitera 16 veces.

Permutación inicial inversa

Al final de las iteraciones, los dos bloques **L**16 y **R**16 se vuelven a conectar y se someten a una permutación inicial inversa:

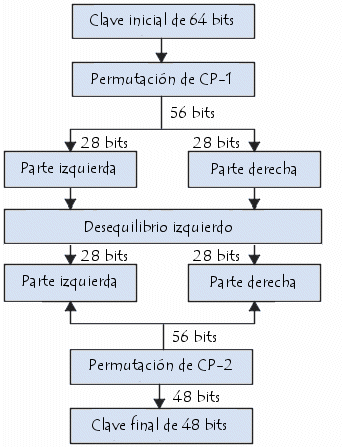
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | |

¡El resultado que surge es un texto cifrado de 64 bits.

Generación de claves

Dado que el algoritmo DES mencionado anteriormente es público, toda la seguridad se basa en la complejidad de las claves de cifrado.

El algoritmo que sigue a continuación muestra cómo obtener a partir una clave de 64 bits (compuesta por cualquier de los 64 caracteres alfanuméricos), 8 claves diferentes de 48 bits, cada una de ellas utilizadas en el algoritmo DES:



En primera instancia, se eliminan los bits de paridad de la clave para obtener una clave que posea una longitud de 56 bits.

El primer paso es una permutación denominada **PC-1**, cuya tabla se presentará a continuación:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PC-1** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 58 | 50 | 42 | 34 | 26 | 18 | | 10 | 2 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 60 | 52 | 44 | 36 | | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 | 30 | 22 | | 14 | 6 | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 | |

Esta matriz puede escribirse en forma de dos matriz **L**i y **R**i (para la izquierda y la derecha respectivamente), cada una ellas de 28 bits:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L**i | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 57 | 49 | 41 | 33 | 25 | 17 | 9 | | 1 | 58 | 50 | 42 | 34 | 26 | 18 | | 10 | 2 | 59 | 51 | 43 | 35 | 27 | | 19 | 11 | 3 | 60 | 52 | 44 | 36 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **R**i | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 63 | 55 | 47 | 39 | 31 | 23 | 15 | | 7 | 62 | 54 | 46 | 38 | 30 | 22 | | 14 | 6 | 61 | 53 | 45 | 37 | 29 | | 21 | 13 | 5 | 28 | 20 | 12 | 4 | |

El resultado de esta primera permutación se denomina **I**0 y **D**0.

Luego, estos dos bloques se rotan hacia la izquierda, de manera que los bits que estaban en la segunda posición pasan a la primera, aquellos que estaban en tercera posición pasan a la segunda, etc.   
Los bits que estaban en la primera posición se mueven hacia la última posición.

Los dos bloques de 28 bits se agrupan en un bloque de 56 bits. Este pasa por una permutación, denominada **PC-2**, dando como resultado un bloque de 48 bits que representa la clave **K**i.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **pc-2** | |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 | 6 | 21 | 10 | | 23 | 19 | 12 | 4 | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 | | 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 | | 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 | |

Realizando iteraciones del algoritmo es posible obtener las 16 claves **K**1 a **K**16 utilizadas en un algoritmo DES.

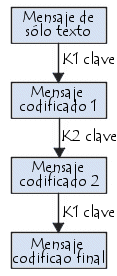
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **LS** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 28 | |

TDES (en castellano: Triple Estándar de Cifrado de Datos), una alternativa para DES

En 1990, Eli Biham y Adi Shamir desarrollaron el criptoanálisis diferencial, que buscaba pares de textos planos y pares de textos cifrados. Este método funciona con un máximo de 15 rondas, mientras que en el algoritmo presentado anteriormente admite 16 rondas.

Por otro lado, aunque una clave de 56 bits ofrece una enorme cantidad de posibilidades, muchos procesadores pueden calcular más de 106 claves por segundo. Con lo que, cuando se utilizan al mismo tiempo una gran cantidad de máquinas, es posible que un gran organismo (un Estado, por ejemplo) encuentre la clave correcta...

Una solución a corto plazo requiere que se encadenen tres cifrados DES mediante dos claves de 56 bits (esto equivale a una clave de 112 bits). Este proceso se llama **Triple DES**, denominado *TDES* (algunas veces *3DES* o *3-DES*).



El **TDES** permite aumentar de manera significativa la seguridad del DES, pero posee la desventaja de requerir más recursos para el cifrado y descifrado.

Por lo general, se reconocen diversos tipos de cifrado triple DES:

* DES-EEE3: Cifrado triple DES con 3 claves diferentes,
* DES-EDE3: una clave diferente para cada una de las operaciones de triple DES (cifrado, descifrado, cifrado),
* DES-EEE2 y DES-EDE2: una clave diferente para la segunda operación (descifrado).

En 1997, el*NIST* lanzó una nueva convocatoria para que desarrollar el **AES** (*Advanced Encryption Standard, en castellano: Estándar de Cifrado Avanzado*), un algoritmo de cifrado cuyo objetivo era reemplazar al *DES*.

El sistema de cifrado *DES* se actualizaba cada 5 años. En el año 2000, durante su última revisión y después de un proceso de evaluación que duró 3 años, el *NIST* seleccionó como nuevo estándar un algoritmo diseñado conjuntamente por dos candidatos belgas, el Sr. *Vincent Rijmen* y el Sr. *Joan Daemen*. El nuevo algoritmo, llamado por sus inventores **RIJNDAEL** reemplazará, de ahora en adelante, al DES.

Más información

* <http://csrc.nist.gov/encryption/tkencryption.html> - Especificaciones de los algoritmos DES, TDES y AES (Sitio Web del *NIST*);
* [RFC 2420](http://www.ietf.org/rfc/rfc2420.txt) El Protocolo de cifrado Triple DES (3DESE) PPP