

Universidad Rafael Landívar

Facultad de Ingeniería

Estructuras de datos II

Sección: 03

Catedrático: Ing. Boris José Búcaro Pazzetti

Lab 4:

Encriptación DES

Dereck Alexander Cabrera Ng – 1177223

21 de octubre de 2024

Explicación del algoritmo.

Este algoritmo se divide en el generador de llaves y en 16 rondas.

Antes de empezar es necesario dividir los datos a cifrar en bloques de datos (64 bits), los cuales se ingresarán al algoritmo y obtendremos los datos encriptados en 64 bits.

Para el generador de llaves se utiliza una llave inicial de 64 bits, después de eliminar 8 bits de paridad terminamos con 56 bits, los cuales son divididos en un par de 28 bits cada uno (llamémoslos left half y right half respectivamente), luego se realiza un Left Shift a cada elemento del par. Ahora juntamos left half con right half obteniendo una llave de 56 bits, luego se realiza permutación con contracción la cual reduce el tamaño a 48 bits, siendo esta la primera clave a utilizar. Con left half y right half realizamos el proceso nuevamente (Left Shift, juntar los lados y permutación con contracción), así repetidamente hasta que generamos las 16 claves.

Si estamos encriptando utilizamos las llaves según las fuimos generando, para desencriptar las utilizamos en orden inverso.

Al bloque de datos realizamos una permutación inicial, el cual será el “input” para la ronda 1. Al “input” de la ronda lo dividimos en 2 (left half y right half), right half será el left half del “output” de la ronda. Para el right half del “output”, expandimos right half por medio de permutación con expansión (obteniendo 48 bits) a este resultado realizamos la operación XOR con la llave de la ronda, posteriormente utilizamos sustitución por S-Box y luego permutación por P-Box, a este resultado realizamos XOR con left half, obteniendo right half del “output”. Este proceso se realiza de la ronda 1 hasta la 15.

Para la ronda 16 el proceso es prácticamente el mismo, con la ligera diferencia de que lo que era el left half y right half del “output” será ahora el right half y left half del “output”, es decir, lo que antes era right half será ahora left half y lo que antes era left half ahora será right half.

Este proceso se repite con cada uno de los bloques de datos hasta obtener los datos encriptados/desencriptados.

Explicación del algoritmo.

Tras abrir el ejecutable "Ejecutable.exe" se le presentara lo siguiente:

```
Enter the path to the .csv file(relative path)
```

Tras escribir la ruta relativa del archivo que contiene los métodos a realizar, se realizaran dichos métodos para posteriormente aparecer lo siguiente en pantalla:

```
Enter the path to the .csv file(relative path)
5lab01_books.csv
Execution time: 35.20µs
Enter the path with the search methods(relative path)
```






Aparece el tiempo de ejecución y pedirá al usuario la ruta relativa con el archivo con los métodos de búsqueda.

```
Enter the path to the .csv file(relative path)
5lab01_books.csv
Execution time: 35.20µs
Enter the path with the search methods(relative path)
5lab01_search.csv
```

Después de ingresar el archivo, el programa mostrara el resultado.

```
Enter the path to the .csv file(relative path)
5lab01_books.csv
Execution time: 35.20µs
Enter the path with the search methods(relative path)
5lab01_search.csv
{"isbn":"9781839046407","name":"Walk set design deal next off sell foot reach car official skin current change bank some
one daughter process attorney collection likely name prove simply themselves.","author":"Thomas Jackson MD","category":"
Romance","price":"92.05","quantity":"460"}
{"isbn":"9781147811407","name":"Dark environmental more appear.","author":"Gloria Garcia","category":"Science Fiction","
price":"60.72","quantity":"498"}
{"isbn":"9780856397349","name":"Then go hope attention friend peace create each.","author":"Eric Fleming","category":"Bi
ography","price":"74.60","quantity":"690"}
Searching time: 22.34ms
Generated file output.txt and encrypted. Press Enter to exit
```

El programa generará 2 archivos en el directorio en el que se encuentra: output.txt y encrypted.

 5lab01_books.csv	10/10/2024 1:49 PM	Microsoft Excel C...	2 KB
 5lab01_search.csv	10/10/2024 1:37 PM	Microsoft Excel C...	1 KB
 Ejecutable.exe	10/20/2024 2:28 PM	Application	503 KB
 encrypted	10/20/2024 5:51 PM	File	1 KB
 output.txt	10/20/2024 5:51 PM	Text Document	1 KB

output.txt es el resultado tras realizar la búsqueda por nombre de los libros, encrypted contiene la información de output.txt de forma encriptada por el algoritmo DES.