

Memoria Algoritmo S-DES

Algoritmo S-DeS realizado en C

Jorge Bolado Campo | Criptografía y seguridad en redes | 15/12/2021

# Bibliotecas necesarias:

Para realizar el código necesitaremos las siguientes bibliotecas:

* <stdio.h>
* <stdlib.h>
* <stdint.h>
* <unistd.h> 🡪 La usaremos para especificar los parámetros de entrada dentro de la terminal de linux

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

## Funciones Que ulilizaremos:

* K\_extraccion\_Clave
  + K1: Variable de entrada y salida ( puntero ) es la primera subclave
  + K2: Variable de entrada y salida ( puntero ) es la segunda subclave
  + Contrasena: clave maestra a apartir de la cual obtenemos las dos subclaves
* M\_Cifrado :
  + Palabra: Palabra a encriptar
  + K1: variable de entrada y salida subclave a utilizar
  + Palabra\_codigo: variable en la que almacenamos el resultado de aplicar la función f(k)
* Permutacion\_IP
  + Palabra: palabra a la entrada a la que vamos a aplicar la permutacion
  + Palabra\_codigo: variable en la que almacenamos la permutación
* Permutacio\_IP\_IP:
  + Palabra\_codigo: variable de entrada y salida en la que inveertimos la permutación anterior para que pueda ser desencriptado
* Elevado:
  + Base: valor al que vamos a elevar a la exponente potencia
  + Exponente: exponente al que elevar la base
  + Puente: valor entrada y salida en la que almacenamos el resultado de base ^exponente
* Sacar\_contrasena:
  + Cambio: variable en la que introducimos las claves maestras
  + Contrasena :variable en la que alamcenamos las claves maestras en binario , 2ª y 3ª clave en el triple S-DES

Texto

Descripción generada automáticamente

Imagen que contiene Texto

Descripción generada automáticamente

Mediante el uso de todas esas funciones he podido lograr encriptar mediante el algoritmo DES Simplified ficheros de tipo docx , pdf , jpg y txt. A continuación muestro el tipo de sentencia utilizada para su ejecución

Texto

Descripción generada automáticamente

Situamos el ejecutable en el mismo directorio que los archivos que queremos encriptar.

Acontinuación debemos llamar al ejecutable ( PruebaFinalExe ) con su método particular:

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

Dentro de la ejecución observamos tres parametros:

* -m: hace referencia al tipo de método que seguiremos.
  + 0 🡪 Encriptar
  + 1 🡪 Desencriptar
* -e: entrada, es decir, nombre del fichero a encriptar y nombre del fichero encriptado
* -k: clave maestra para realizar la encriptación.

Tras la ejecución debería aparecer el archivo encriptado, si quisieramos desencriptarlo para ver la validez de nuestro algoritmo deberíamos repetir los pasos anteriores.

Texto

Descripción generada automáticamente

Para comprobar la validez de nuestra encriptación lo mejor que podemos hacer es realizar el Has de ambos archivos, el original y el desencriptado para ver si es correcto su funcionamiento.

Texto

Descripción generada automáticamente

En caso de que queramos realizar un triple encriptado lo que debemos hacer es seguir el mismo procedemiento pero usando tres claves maestras en lugar de una. Ahora lo realizaremos con el propio guión de la practica.

Texto

Descripción generada automáticamente

En caso de que olvidasemos como se ejcuta el programa deberiamos pedir ayuda mediante el comando -h

Pantalla negra con letras blancas

Descripción generada automáticamente