**Práctica 2 - Algoritmos de cifrado simétrico. DES.**

**Autores**: Carlos González Recio.

Ernesto Boado Moreira.

**Asignatura**: Seguridad Informática.

# Descripción de la Práctica

Diseñar un programa en C llamado criptoDES que funcione en el modo ECB y que sirva para:

* Cifrar.
* Descifrar.
* Atacar.

Para cifrar es necesario solicitar al usuario el texto en claro, la clave y algún parámetro adicional que se pueda necesitar. Se debe proporcionar además el nombre de un fichero para almacenar la información cifrada (v.g., el criptograma).

Para descifrar se debe solicitar al usuario el nombre del fichero que contiene el criptograma, la clave y algún parámetro adicional que se pudiera necesitar. La información descifrada se debe mostrar en la pantalla.

Finalmente, el ataque a implementar será de fuerza bruta suponiendo que se

conocen los primeros cuatro caracteres del texto en claro. Presentar aquellos

candidatos en los que los caracteres conocidos coincidan con los obtenidos en

el criptoanálisis.

Para el proceso de cifrado y descifrado se utilizará la librería **rpc/des\_crypt**

del entorno Linux.

# Funcionamiento del programa

## Encriptado.

1. Se lee el mensaje a encriptar (fichero o línea de comandos).
2. Encriptado utilizando la función ecb\_crypt (con DES\_ENCRYPT).
3. Se guarda el mensaje encriptado en un fichero.

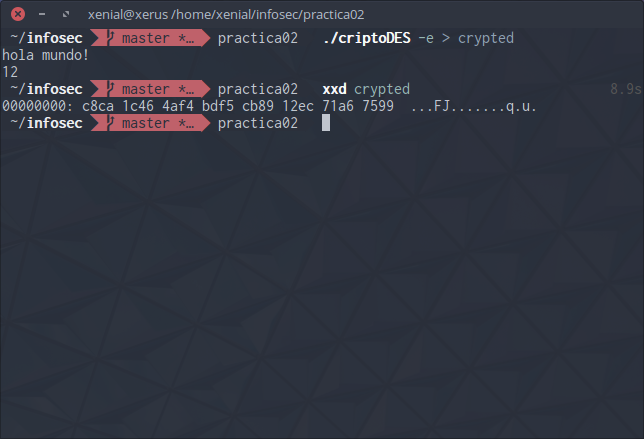
## Desencriptado.

1. Se lee el mensaje encriptado de fichero.
2. Desencriptado utilizando **ecb\_crypt** (con DES\_DECRYPT).
3. Se muestra el mensaje desencriptado por pantalla.

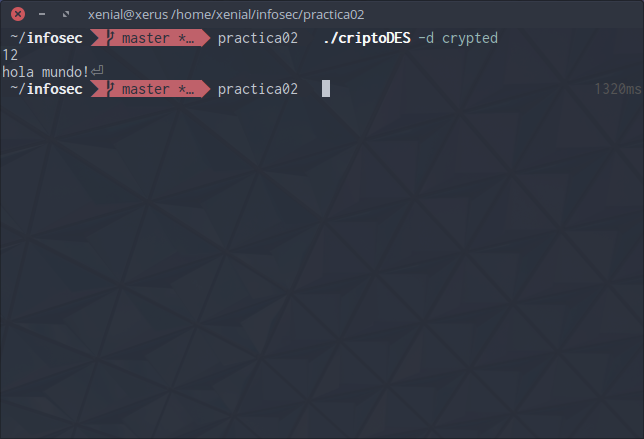
## Ataque

* Se van creando en un bucle todas las claves posibles.
* Se utiliza cada clave generada para descifrar mensaje cifrado.
* Se compara el mensaje descifrado con el conocido.
* Si la clave es válida se muestra por pantalla.

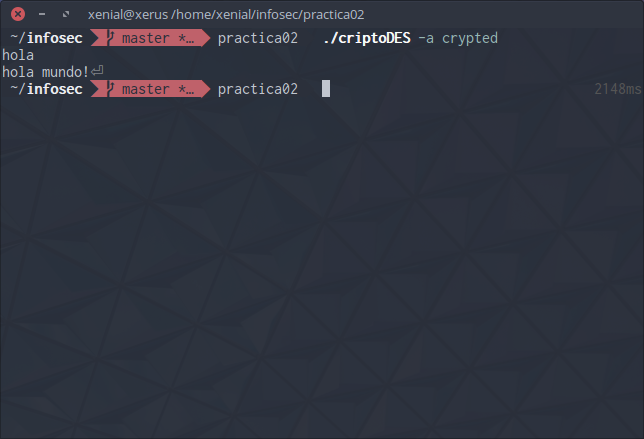
## Capturas



Encriptado. Mensaje: “hola mundo!”; clave: “12”



Desencriptado. Clave: “12”



Ataque. Caracteres conocidos: “hola”

## Conclusiones.

El método de ataque por fuerza bruta es inviable utilizando un ordenador personal, ya que, el récord de menor tiempo está en 22 horas utilizando un sistema multiprocesador especialmente diseñado para la tarea.