Criptografía

Practica 2: Criptosistema DES

ULPGC 2011-2012

Implementación del algoritmo DES para la encriptación de texto, en una aplicación Android para dispositivos móviles

Gabriel Fernández Díaz
David Morales Sáez

1. Introducción

Para el desarrollo de esta práctica, se ha implementado el clásico algoritmo de encriptación DES. Para ello hemos usado la tecnología Android, y por consiguiente, JAVA.

2. Trasfondo Teórico

El algoritmo DES fue desarrollado en Estados Unidos en 1976 para un concurso de la NSA, tuvo mucha aceptación y se uso por todo el mundo durante mucho tiempo. Esta fama hizo que fuese estudiado ampliamente por académicos y cripto-analistas. En la actualidad es un algoritmo inseguro, ya que sus claves de 56 Bits pueden ser vulneradas en menos de 24 horas.

Este cripto-sistema se basa en el cifrado por bloques. Se sirve de una serie de fases de transformación y desplazamiento, concretamente consta de una fase PI, 16 fases F y una fase PF. La fase PI toma el mensaje sin encriptar en bloques de 64 bits y la fase PF da el mensaje encriptado en bloques de 64 bits. Estas dos fases son inversas entre si. En el párrafo anterior se menciono que la clave usada por este algoritmo está formada por 56 bits, pero en realidad se expanden hasta tener 64 bits para usarla.

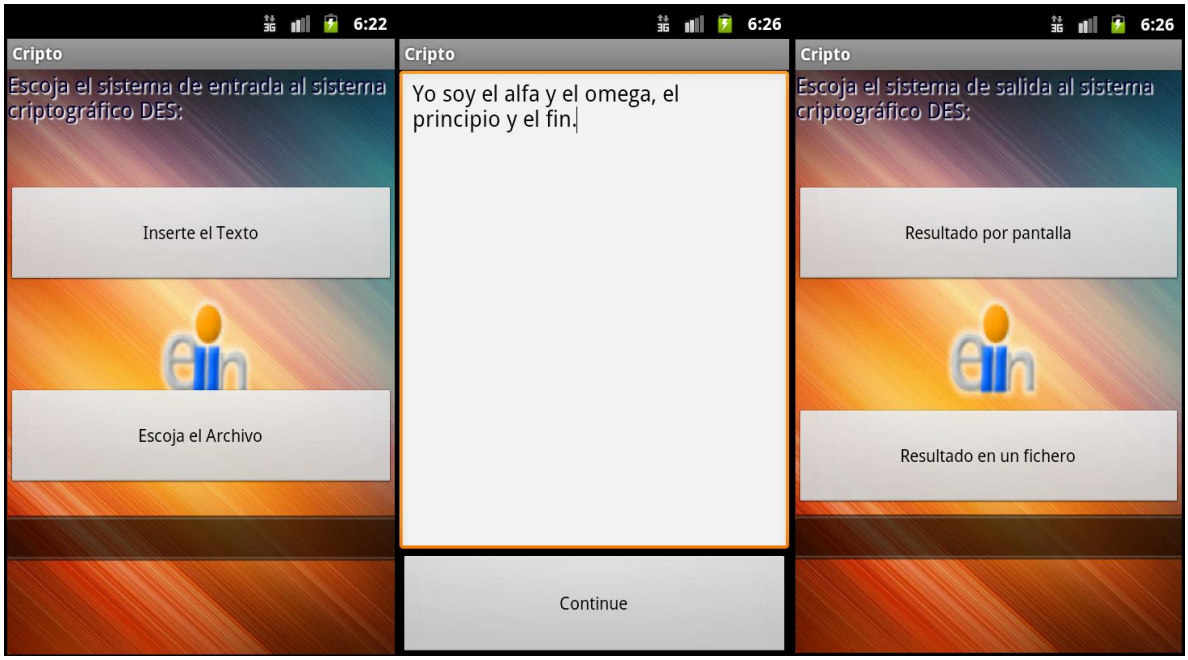
3. Implementación

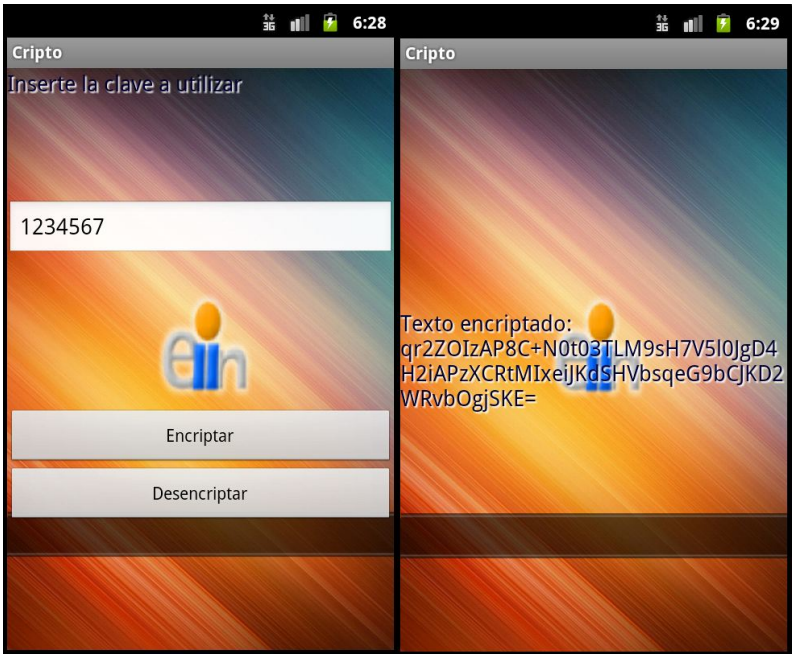
Para la implementación de esta práctica se ha añadido a la aplicación desarrollada para la práctica anterior, la funciones necesarias permitirán introducir un texto, bien por teclado o bien por fichero, una clave de un máximo de 7 caracteres, y encriptarla o desencriptarla usando el algoritmo DES. El tamaño de la clave se restringe, debido a la limitación impuesta por el DES (7 caracteres * 8 Bites/carácter = 56 bits).

4. Uso del programa

Para el correcto uso de la aplicación el proceso de uso es el siguiente:

1. Apretar el botón “DES”
2. Seleccionar como insertar el texto
    a. Apretar “Inserte el Texto” para introducir el texto por pantalla, y luego presionar “Continue”
    b. Apretar “Escoja el Archivo” para introducir el texto desde un fichero, seleccionar el fichero origen y pulsar “Seleccionar”.
3. Seleccionar como mostrar el texto resultante
    a. Apretar “Resultado por pantalla” para mostrar el texto por pantalla.
    b. Apretar “Resultado en un fichero” para que el texto se guarde en un fichero, seleccionar el fichero destino y pulsar “Seleccionar”.
4. Introducir una clave de hasta 7 caracteres
5. Pulsar “Encriptar” o “Desencriptar” según se deseé.


6:22
Cripto
Escoja el sistema de entrada al sistema criptográfico DES:
Inserte el Texto
Escoja el Archivo
6:26
Cripto
Yo soy el alfa y el omega, el principio y el fin.
Continue
6:26
Cripto
Escoja el sistema de salida al sistema criptográfico DES:
Resultado por pantalla
Resultado en un fichero


6:28
Cripto
Inserte la clave a utilizar
1234567
Encriptar
Desencriptar
6:29
Cripto
Texto encriptado:
qr2ZOIzAP8C+N0t03TLM9sH7V5l0JgD4H2iAPzXCRtMIxeiJKdSHVbsqeG9bCJKD2WRvbOgjSKE=