2º C.F.G.S. desarrollo de aplicaciones multiplataformas

PEN EVAL - Encriptación

Modelo híbrido

Rubén Arcos Ortega

PENEVAL - Encriptación

Objetivo

He realizado la división de la funcionalidad de la práctica en tres fases, realizando en la primera la codificación de un fichero, en la segunda la codificación de la clave de la primera fase y en la última la descodificación de la clave de la segunda, para con la clave resultante decodificar el fichero de la primera fase que fue encriptado.

Estructura y funcionalidad[1]

- Fase 1: consta de la encriptación de un fichero de texto plano denominado "fichero_original.txt" mediante la codificación de clave simétrica, en este caso se ha elegido el algoritmo de codificación DES y el almacenamiento de la clave utilizada en otro fichero de texto denominado "fichero_clave_privada.txt" y dando como resultado un último fichero nombrado como "fichero_codificado.txt" que consiste en la codificación del fichero "fichero_original.txt".
- Fase 2: realiza la codificación de la clave privada DES obtenida y almacenada en la fase anterior mediante la codificación de clave pública con el algoritmo RSA. "En esta fase se almacenarán dos ficheros, uno con la clave pública RSA resultante como "fichero_clave_privada.txt" y la clave privada DES de la fase 1 codificada mediante esta clave RSA y almacenada como "fichero_clave_codificado.txt".
- Fase 3: su funcionalidad se divide en tres partes, una primera que realiza la localización de los ficheros necesarios para el proceso a realizar: la clave RSA generada en la fase 2 y el fichero generado en la fase 2 resultante de la codificación de la clave DES de la fase 1. Una vez indicadas las ubicaciones correspondientes, se procede a la localización del fichero que se codificó en la primera fase, el cual contiene el mensaje original, y se procede a la segunda parte de proceso: la decodificación del fichero de la fase 2 que contiene la clave privada de la fase 1 codificada, una vez descodificado, ya se dispone de la clave privada DES de la fase 1, por lo cual se puede pasar a la última fase, la descodificación del fichero con el mensaje original.

Conclusión

Con esta práctica he aprendido la funcionalidad y realización de un modelo híbrido, adquiriendo a su vez los conocimientos necesarios para la realización de un sistema de encriptación/desencriptación mediante un algoritmo de clave privada o simétrica, también de un sistema de clave pública o asimétrica como los diferentes algoritmos que pueden ser utilizados en cada caso.

[1] En todos los casos tanto los nombres de los fichero son sugerencias, con fines orientativos, en todo el proceso de la aplicación puede ser indicado otro nombre de fichero y ruta para su almacenamiento con en el proceso de localización y selección de los ficheros de lectura necesarios.