Escuela Politécnica Superior de Elche
Grado en Ingeniería Informática en Tecnologías de la Información
Área de Arquitectura y Tecnología de Computadores

Seguridad en Sistemas Informáticos

Práctica 2 (sesión 1)

Utilización de una librería criptográfica (Crypto++)

Introducción

Actualmente, uno de los dispositivos donde más se usan los algoritmos criptográficos es el ordenador. La mayoría de las soluciones de seguridad están basadas en la criptografía. Existen multitud de *librerías de programación* criptográficas que implementan los algoritmos de cifrado/descifrado que permiten realizar programas que incorporen características de seguridad sin tener que programar dichos métodos. En esta práctica se utilizará la librería criptográfica denominada Crypto++.

Objetivos de la práctica

- Conocer la librería criptográfica Crypto++.
- Utilizar dicha librería dentro de un programa.

Tareas a realizar

- Descargar e instalar la librería Crypto++.
- Compilar y ejecutar el programa de ejemplo.
- Modificar el programa de ejemplo añadiendo las opciones indicadas más abajo.
- Obtener ficheros encriptados utilizando el programa de ejemplo modificado.

Memoria de la práctica

En esta práctica se entregará el código fuente del programa, así como los ficheros encriptados, todos juntos en un fichero comprimido (.zip).

Los ficheros que hay que entregar dentro del archivo comprimido son los siguientes:
`test.cpp, usage2.dat, DES-claro.txt, DES-clave.txt, DES-cifrado.txt, AES-claro.txt, AES-clave.txt, AES-VI.txt, AES-cifrado.txt, texto-B64.txt`

No es necesario entregar una memoria en PDF como en otras prácticas.

Características

Para el desarrollo de la práctica se utilizará el compilador Microsoft Visual C++. Este compilador es gratuito para los estudiantes de la UMH.

Desarrollo

Los pasos a realizar para el desarrollo de la práctica son los siguientes:

• Descargar e instalar Crypto++.
Entrar en la página web https://www.cryptopp.com leer la descripción y los componentes que incluye y descargar la librería Crypto++. La versión actual (Marzo'2024) es la 8.9.0. Una vez descargada se deberá descomprimir en una carpeta (preferiblemente en una ruta que no incluya espacios en blancos, ni la letra "ñ", ni letras con acento).

• Compilar el programa de ejemplo y ejecutarlo.
Abrir el fichero cryptest.sln con Microsoft Visual C++. Generar (compilar) la solución (*una "solución" es un conjunto de proyectos*). Antes de compilarla, se debe configurar la solución en modo "release". Una vez generada la solución, buscar el ejecutable cryptest.exe y ejecutarlo (sin parámetros) desde una consola de comandos (cmd). Aparecerá un mensaje de error (en inglés) indicando que no se puede mostrar el mensaje de ayuda porque no se ha encontrado el fichero usage.dat. Para que el programa muestre la ayuda por pantalla debemos copiar el fichero cryptest.exe en el directorio raíz de la librería o bien copiar el fichero usage.dat en la ruta en la que el programa espera encontrarlo (mirar en el código fuente test.cpp). Ejecutar cryptest.exe de nuevo y leer el mensaje de ayuda. Probar el funcionamiento del programa de ejemplo con alguna de las opciones que tiene (p.ej.: V, v, g, r, t, b, ...).

• Añadir opciones al programa de ejemplo.
Añadir opciones nuevas al programa:

- Opción "des_DES". Descifra un texto cifrado con Triple-DES (DES-EDE) en modo CBC *(Cipher Block Chaining)*. Debe pedir por pantalla la "passphrase" y el texto cifrado y mostrar el texto descifrado. Tomar como modelo la opción ya implementada "t" y, además, usarla para generar previamente un texto cifrado (para las comprobaciones).

- Opción "enc_DES_fich". Cifra un texto almacenado en un fichero con Triple-DES (DES-EDE) en modo CBC *(Cipher Block Chaining)* y lo almacena en otro fichero. Debe pedir por pantalla la "passphrase", el nombre del fichero a leer con el texto en claro y el nombre del fichero a grabar.

- Opción "des_DES_fich". Descifra un texto cifrado con Triple-DES (DES-EDE) en modo CBC *(Cipher Block Chaining)* desde un fichero y el resultado lo almacena en otro fichero. Debe pedir por pantalla la "passphrase", el nombre del fichero con el texto cifrado y el nombre del fichero a grabar.

- Opción "des_AES". Descifra un texto cifrado con AES en modo CTR *(Counter)*. Esta opción tomará directamente de la línea de comandos los parámetros que necesite. Tomar como modelo la opción "ae" y usarla para generar previamente un texto cifrado (para las comprobaciones). En el fichero de ayuda del programa de ejemplo (usage.dat) la opción "ae" no está correctamente documentada. Hay que mirar en el código fuente del programa cuál es el número de parámetros requeridos y qué es cada uno de ellos.

Estas opciones se deben documentar adecuadamente en la parte final del fichero usage2.dat para que, cuando se ejecute cryptest.exe sin parámetros, aparezca el funcionamiento de las nuevas opciones.

• Utilizar el programa para generar tres textos cifrados.
Escribir dos frases en castellano (de entre 10 y 30 palabras cada una) relacionadas con la noticia "El grupo cibercriminal chino Earth Krahang viola la seguridad de 70 organizaciones en 23 países" (disponible en la página "Una al Día" de Hispasec, 21 de Marzo de 2024). No utilizar IA. Sí utilizar IN (Inteligencia Natural). Codificar la primera frase usando DES-EDE en modo CBC. Codificar la segunda frase usando AES en modo CTR. Usar la opción correspondiente del programa para convertir al formato base 64 la frase "AES ES UN ALGORITMO DE CIFRADO POR BLOQUES Y CTR ES UN MODO DE OPERACION" (sin las comillas y en mayúsculas).

En el apartado "Memoria de la práctica" se han indicado los ficheros que se deberán entregar. En el apartado "Notas adicionales" se explica con detalle qué debe contener cada fichero.

Notas adicionales

A continuación se explica con detalle el contenido de cada uno de los ficheros a entregar.

`test.cpp` - código fuente modificado con las nuevas opciones añadidas
`usage2.dat` - fichero de ayuda modificado para incluir las nuevas opciones

`DES-claro.txt` - ejemplo de texto en claro para cifrarlo con DES-EDE
`DES-clave.txt` - passphrase utilizada para cifrar el texto con DES-EDE
`DES-cifrado.txt` - resultado de cifrar el texto claro con la passphrase

`AES-claro.txt` - ejemplo de texto en claro para cifrarlo con AES
`AES-clave.txt` – clave utilizada para cifrar el texto con AES
`AES-VI.txt` – vector de inicialización para cifrar el texto con AES
`AES-cifrado.txt` - resultado de cifrar el texto claro con la clave y el vector de inicialización

`texto-B64.txt` - resultado de convertir la frase indicada a formato base 64

Para la codificación/descodificación de los textos con AES se debe utilizar como clave el valor `8787AEA112456FFD3B21265482118404` y como vector de inicialización del contador el valor `38D8430274AFFD4DF282218BF4DB4059` (128 bits en formato hexadecimal).

Reflexiona: ¿Opinas que era necesario implementar la opción "des_AES"? ¿Se podría utilizar algún método alternativo para poder descifrar el contenido del fichero `AES-cifrado.txt` teniendo en cuenta el modo de operación con el que ha sido encriptado?