DATOS DEL ALUMNO

Nombre y apellidos:

D.N.I.:

Grado:

TRABAJO FINAL
SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

OBJETIVO

Los servicios de contraespionaje han conseguido detener a un espía que se disponía a desencriptar una serie de mensajes utilizando unas claves que intentó destruir en el momento de su detención.

Nuestros agentes consiguieron apagar un papel ardiendo en el que parecía habían escrito una secuencia de números. Por desgracia el fuego destruyó parte de la última fila. Los datos que conseguimos salvar son los siguientes:

9D2AEA59EC1C7B5A

D91687BF6C825862

F76B8E9F23XXXXX

Sospechamos que son claves de encriptación simétrica, en concreto del 3DES.

Además del papel que intentó destruir, ocultaba en su boca un pen-drive, que cuando lo hemos introducido en nuestro sistema, contenía dos ficheros

DOCUMENTO1.DAT:

6jTT5bXT5TAea+qqkFK/Vs8DYIhfjWBl0UvjE8+ImP1eXI4efHGOnOSwbyAaIF1SXyHP0LWpWF3Ec bKkKXyecPukYp0XIlhGdL8yAVUtstloCcpJL2C1bZYb3782WrlnldLtTgCpG0wGN4hCdTX196f0ioUG vGfrDSPhbcU1sXxODjBmrukCOfYk4rwYR2DJ

DOCUMENTO2.DAT

RsBLF6KboTcTp1Ov/R8wrmkWpapYmTZRasIwF6jH5E42lSoxVk1b/zBt5/nk270aTlFmN2uxckG7 zrdom3Vy/w==

El contenido de esos ficheros es completamente ilegible, pero tenemos la corazonada que contiene información relevante.

Se requiere de la pericia de un ingeniero informático que sea capaz de averiguar el resto de la clave, y desencriptar el primer fichero (DOCUMENTO1.DAT). Creemos que ese fichero puede contener información transcendental para descifrar el segundo fichero (DOCUMENTO2.DAT).

El trabajo que se deberá presentar es el siguiente:

1. Programa que mediante cualquier mecanismo de hacking sea capaz de reconstruir las claves de 3DES y desencriptar el mensaje oculto en el DOCUMENTO1.
2. Analizado el primer mensaje, la implementación de un programa que en base a la información oculta en el primer mensaje, desencripte el segundo mensaje (DOCUMENTO2.DAT).

El desarrollo se ha de realizar en C#, y se recomienda el uso de la librería *System.Security.Cryptography*. Este trabajo tendrá un máximo de 4 puntos sobre los 10 reservados para el examen final de la asignatura.

El trabajo ha de contener:

1. **UNA MEMORIA**, que contenga.
    - Descripción clara de los pasos que va a realizar. Esquema de proyecto, en el que se especifique los diferentes módulos que va a implementar, sistema de almacenamiento de pruebas, análisis posterior.
        i. Estimación del tiempo que le llevará a ejecutar cada uno de ellos.
        ii. Tiempo real empleado.
    - Mecanismo empleado para guardar los resultados de cada clave probada hasta dar con la correcta.
    - Primer Mensaje desencriptado.
    - Segundo Mensaje desencriptado.
    - Código fuente claramente documentado.

2. **UN PROGRAMA EJECUTABLE**.

Se ha de presentar el código fuente y un ejecutable que funcione en Windows 10, que al menos contemple:

- Método empleado para averiguar las variables.
- Lugar de almacenamiento de los resultados de las pruebas (log).
- Resultado del primer desencriptado una vez obtenida la clave.
- Resultado del segundo desencriptado una vez descifrado el primer mensaje.

3. **LA FORMA DE VALORAR** el trabajo, se seguirá según los siguientes criterios:

   - Memoria descriptiva y código fuente: Máximo 5,0 puntos.
   - El programa se ejecuta: 1,0 puntos
   - El programa encuentra las claves del doc 1 1,0 puntos
   - El programa desencripta el documento 1 1,0 punto.
   - El programa desencripta el documento 2: 2,0 punto.

Los puntos se irán acumulando de fase en fase, es decir, si el programa se ejecuta, pero no encuentra las claves, no se comprueba el resto de puntos. Si no se ejecuta, la nota máxima sería la obtenida en la memoria y el código fuente (máximo 5,0).