DATOS DEL ALUMNO

Nombre y apellidos:

D.N.I.:

Grado:

TRABAJO FINAL
SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

OBJETIVO

El alumno desarrollará un sistema que permita comunicarse con otra aplicación, utilizando un sistema de clave pública-clave privada para intercambiarse una clave, que posteriormente será utilizada para encriptar/desencriptar en bloque.

El algoritmo a emplear en la encriptación en bloque es el sistema de criptografía simétrica de bloque TDES.

El algoritmo de encriptación de clave pública/privada empleada para el intercambio de la clave calculada para el TDES, será el RSA.

El desarrollo se ha de realizar en JAVA o en C#, a elección del alumno. Este trabajo tendrá un máximo de 4 puntos sobre los 10 reservados para el examen final de la asignatura.

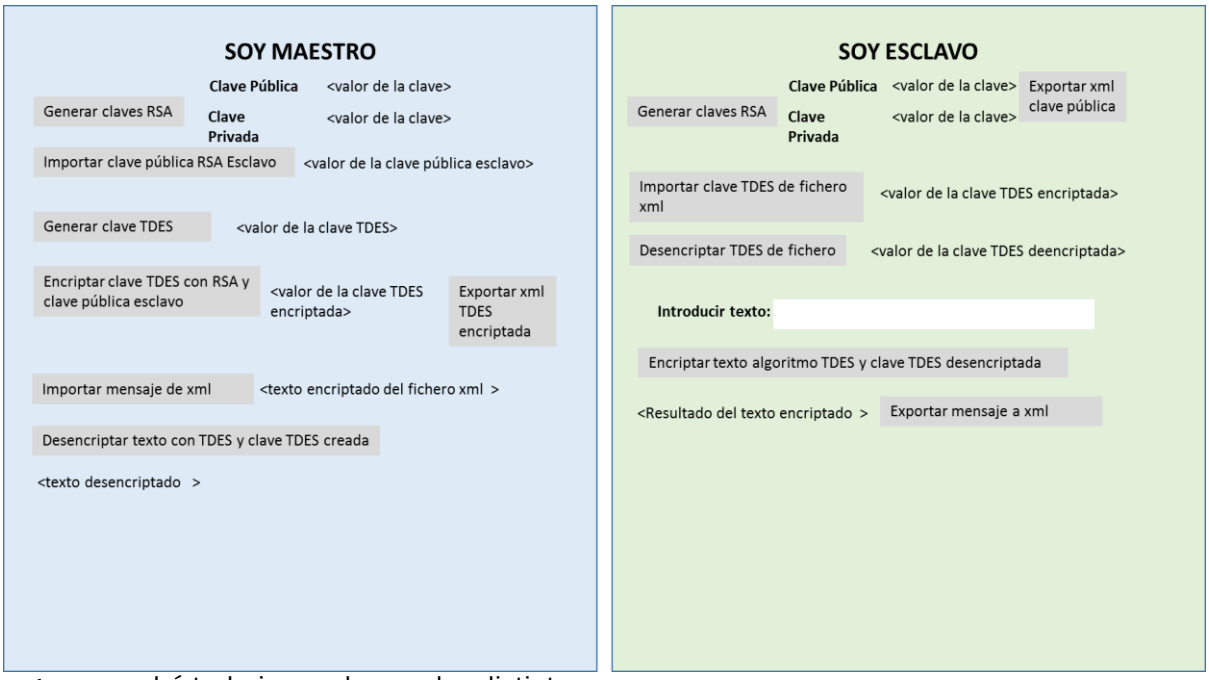
El trabajo ha de contener:

1. **UNA MEMORIA**, que contenga.
    - Tecnologías, entornos de ejecución e implementación. Una breve descripción que contenga:
        - Tecnologías utilizadas (Java, c#, css, php, y cualquier librería incorporada).
        - Entorno de ejecución (Sistema operativo, servidor web (si es preciso),…).
        - Herramientas de desarrollo. (Visual studio, Java,…).

2. **UN PROGRAMA EJECUTABLE**.

Se ha de presentar el código fuente y un ejecutable que funcione en Windows 10, con el interfaz y funciones definidas a continuación:

2.1. La interfaz del programa creado, ha de tener el siguiente aspecto:



El programa podrá trabajar en dos modos distintos:

- **Como maestro**: Quiere decir que tendrá que realizar las siguientes funciones:
  - Crear la clave de transferencia en bloque.
  - Leer la clave pública del esclavo.
  - Encriptar la clave de transferencia en bloque con esa clave pública, y volcarla a un fichero xml.
  - Recibir un mensaje encriptado del esclavo.
  - Desencriptarlo y mostrarlo.

- **Como esclavo**: Quiere decir que tendrá que realizar las siguientes funciones.
    - Crear una clave pública-privada, y volcar la clave pública en un fichero xml.
    - Recibir un fichero con una clave encriptada.
    - Desencriptar esa clave con mi clave privada. Esta clave será la del algoritmo de encriptación en bloque.
    - Recibir un mensaje y encriptarlo con esa clave recibida.
    - Volcar el mensaje encriptado a un fichero xml.

En cualquier momento, un programa puede pasar de esclavo a maestro, por lo que necesitan tener codificados todos los algoritmos.

Las funciones a desarrollar, reflejadas en los botones de la aplicación, son las siguientes:

Generar claves RSA	Invocará a las librerías del algoritmo RSA, y generará las claves públicas y privadas. Las mostrará en las etiquetas <valor de la clave>. NOTA. Al pulsarlo, se han de rellenar las 4 etiquetas, por lo que daría lo mismo pulsar el botón de generar claves RSA en el maestro o en el esclavo.
Exportar xml clave pública	Genera un fichero xml denominado cp_esclavo, con la siguiente estructura: <clavepublica></clavepublica>, donde se almacenará el valor de la clave pública calculado.
Importar clave pública RSA Esclavo	Al pulsar este botón, nos aparecerá el gestor de archivos, para que seleccionemos un archivo xml. Una vez elegido, buscaremos la etiqueta <clavepublica>, y el valor de esa etiqueta lo mostraremos en <valor de la clave pública esclavo>.
Generar clave TDES	Al pulsar este botón, generaremos las claves necesarias siguiendo el algoritmo TDES(tres).
Encriptar clave TDES con RSA y clave pública esclavo	Al pulsar este botón, encriptaremos las tres claves de TDES siguiendo el algoritmo RSA, con la clave pública que tenemos en <valor de la clave pública esclavo>.
Exportar xml TDES encriptada	Al pulsar este botón, crearemos un fichero xml denominado tdesencriptado.xml, que contendrá las claves TDES encriptadas con el formato: <tdes1></tdes1> <tdes1></tdes1> <tdes1></tdes1>

Importar clave TDES de fichero xml	Al pulsar este botón, nos aparecerá el gestor de archivos, para que seleccionemos un archivo xml. Una vez elegido, buscaremos las etiquetas <tdes1>,<tdes2> y <tdes3> y el valor de esa etiqueta lo mostraremos en <valor de la clave TDES encriptada>.
Desencriptar TDES de fichero	Al pulsar este botón, y empleando nuestra clave privada del algoritmo RSA, desencriptaremos las tres variables de TDES encriptadas, obteniendo las 3 claves TDES originales. Las presentaremos en la esiqueta <valor de la clave TDES desencriptada>.
Encriptar texto algoritmo TDES y clave TDES desencriptada	Al pulsar este botón, el texto introducido en el campo de texto, será encriptado usando el algoritmo TDES, y las claves desencriptadas del punto anterior. Se mostrará el resutlado en <Resultado del texto encriptado>.
Exportar mensaje a xml	Al pulsar este botón, se generará un fichero xml llamado textoencriptado.xml, que contendrá el valor <Resultado del texto encriptado>, etiquetado con la etiqueta <textoe></textoe>
Importar mensaje de xml	Al pulsar este botón, nos aparecerá el gestor de archivos, para que seleccionemos un archivo xml. Una vez elegido, buscaremos la etiqueta <textoe> y el valor de esa etiqueta lo mostraremos en <texto encriptado del fichero xml>.
Desencriptar texto con TDES y clave TDES creada	Al pulsar este botón, y empleando las claves del algoritmo TDES creadas, se desencriptará el mensaje y el resultado se mostrará en <texto desencriptado>

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

   - Memoria descriptiva y código fuente: Máximo 2,5 puntos.
   - El programa se ejecuta: 0,5 puntos
   - El programa genera claves:
     - RSA 0,5 punto.
     - TDES 0,5 punto.
   - El programa Exporta a ficheros xml: 1,0 punto.
   - El programa Importa de ficheros xml: 1,0 punto.
   - El programa Encripta/Desencripta correctamente:
     - COMO MAESTRO: 1,0 punto.
     - COMO ESCLAVO: 1,0 punto.

- El programa funciona conversando con otra aplicación. 2,0 puntos.

Los puntos se irán acumulando de fase en fase, es decir, si el programa se ejecuta, pero no genera 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 2,5).