DIGITALIZACIÓN - CIBERSEGURIDAD

Trabajo práctico

Se realizará un trabajo en grupo (4 alumnos MÁX) relacionado con la seguridad de la información que será preferentemente práctico y deberá implementarse en un lenguaje de programación que permita la ejecución en WINDOWS.

Se realizará la siguiente propuesta:

- Implementación de un servicio seguro de contenidos multimedia
  - En una **primera fase** se debe diseñar e implementar un sistema que cifre un conjunto de, al menos, 6 archivos multimedia con AES128 de manera que se utilice para cada uno con una clave diferente generada aleatoriamente que será almacenada en un archivo o en una base de datos, para poder descifrar los archivos multimedia.
  - En una **segunda fase** se debe diseñar e implementar un sistema para autentificar al administrador del servicio de contenidos y generar un par de claves, pública y privada, con RSA. Se hará uso de la clave pública para cifrar las claves AES alamacenadas en la primera fase, de manera que no queden expuestas. Se debe proteger, también la clave privada del administrador.
  - En una **tercera fase** se hará uso de RSA para generar un par de claves, pública y privada, para cada usuario que desee acceder a los contenidos multimedia. Se diseñará e implementará un sistema para poder acceder a los contenidos cifrados. Se podrá mejorar el sistema de autenticación.

Se hará un seguimiento de los trabajos en las clases de prácticas de los meses de septiembre, octubre y noviembre (orientación, sugerencias, etc.) a fin de mejorar aquellos aspectos que lo necesiten.

- **El trabajo definitivo (tercera fase) será entregado antes de las 23:59 h. del día 15 de diciembre de 2025;** Se entregará un archivo comprimido conteniendo la versión ejecutable y el código fuente, además de la correspondiente memoria que no excederá de 25 folios por una cara y debe contener al menos los siguientes apartados:
  - Índice
  - Contenido del archivo comprimido (breve descripción)
  - Manual de usuario (instrucciones de uso, ejemplos, etc.)
  - Documentación sobre la implementación (software y librerías utilizadas, descripción del programa, funciones utilizadas y/o creadas, comentarios, etc.)
  - Un capítulo específico en el que se traten los aspectos relacionados con la seguridad en el que se utilizará una notación correcta que permita la interpretación inequívoca de las operaciones realizadas en los distintos procesos seguros.

PUNTUACIÓN:

15% Primera fase
20% Segunda fase
65% Tercera fase
35 % Memoria del trabajo definitivo.
65 % Versatilidad, complejidad, posibilidades, etc.; del trabajo en general.