PRÁCTICA 4

FIRMA DIGITAL

En esta práctica hay que implementar el sistema de firma digital y verificación de la firma DSS (si se quiere, se puede implementar el sistema ECDSA).

Hay que realizar tres tareas: generación de claves, firma de documentos y verificación de la firma.

En la generación de claves debe devolver dos ficheros de texto: uno con la clave pública y otro con la clave privada. Los distintos parámetros de las claves aparecerán en líneas diferentes.

Para la generación de la firma se le introducirá un mensaje (bien por teclado, bien un fichero), el fichero con las claves (pública y privada), y deberá generar una firma que se guardará en un fichero de texto. Cada uno de los dos parámetros de la firma estará en una línea diferente.

Puesto que lo que se firma en verdad es un resumen del fichero (o del mensaje), hay que generar un resumen del mensaje. Para esto emplearemos la función SHA2 (si se quiere además usar alguna otra, puede hacerse). Puede emplearse cualquier librería o cualquier aplicación que calcule esta función.

Para la verificación de la firma se introduce el mensaje (por teclado o en un fichero) que se ha firmado, un fichero con la firma (con el mismo formato que el generado en el apartado anterior) y un fichero con la clave pública. Deberá responder si la firma es válida o no.