Planteamiento

Tal y como se expuso en el guion general de prácticas, la emisión del voto se hará garantizando el anonimato a través de una firma ciega. Bajo este protocolo se encuentra la firma RSA. En esta práctica implementaremos la firma RSA que deberemos aplicar dos veces en el protocolo de votaciones: Para que el votante demuestre su identidad ante la Autoridad Electoral y para que ésta le firme de forma ciega lo que será el hash del voto.

De forma complementaria, otra función que debemos implementar es la de la verificación de la firma RSA que me permita comprobar su validez.

Trabajo a realizar durante la práctica

- Implementar la función de firma RSA para que lea el hash de un texto de un fichero resumen.DAT, tomando como entrada el nombre de dicho fichero, una clave leída de un fichero adecuado (y los parámetros que exija el método de firma); para que escriba la firma en otro fichero llamado firma.DAT.

- Implementar la función de verificación de firma RSA, que lea el contenido del fichero firma.DAT, tomando como entrada el nombre de dicho fichero y la clave pública adecuada guardada en un certificado creado en una práctica anterior (y los parámetros que exija el método de descifrado) y que dé como salida el valor 'true' si la verificación es correcta y 'false' en cualquier otro caso.

- Un informe descriptivo de las dos tareas anteriores en el que se argumente las decisiones tomadas.

- Se deberá entregar a través de Moodle dos ficheros:

    a. El informe descriptivo de la práctica.

    b. El código fuente.