Planteamiento

Tal y como se expuso en el guion general de prácticas, la emisión del voto se hará cifrado con un sistema híbrido, utilizando como esquema asimétrico RSA y simétrico AES, que ya habrá sido implementado en una práctica anterior. En ésta implementaremos el cifrado asimétrico adecuado para nuestra planificación inicial y conforme a los certificados emitidos. Partiremos de que el contenido que se va a cifrar está escrito en un fichero.

Otra función que debemos implementar es la del descifrado RSA que me permita deshacer la operación anterior.

Trabajo a realizar durante la práctica

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

- Implementar la función de descifrado RSA, que al igual que la función de cifrado, lea el contenido del fichero Clave_cifrada.DAT, tomando como entrada el nombre de dicho fichero y la clave privada adecuada guardada en un fichero de claves creado en la práctica anterior de certificados (y los parámetros que exija el método de descifrado); para que escriba el resultado en otro fichero llamado clave_descifrada.DAT.

- 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.