Planteamiento

Tal y como se expuso en el guion general de prácticas, la emisión del voto se hará cifrado con un sistema simétrico, concretamente AES. Partiremos que el voto es un texto contenido en un fichero. Tendremos que buscar librerías que implementen el cifrado de dicho texto y elegir aquélla función que consideremos más adecuada (modo cbc, ecb, etcétera).

Otras de las funciones que debemos implementar es la del cálculo del hash de dicho voto. También deberemos elegir de entre todas las posibilidades (MD5, SHA1, SHA256, SHA3, RIPEMD, …)

Trabajo a realizar durante la práctica

- Implementar la función de cifrado AES para que lea el voto de un fichero VOTO.DAT, tomando como entrada el nombre de dicho fichero, una clave longitud adecuada (y los parámetros que exija el método de cifrado); para que escriba el voto cifrado en otro fichero llamado cifrado.DAT.

- Implementar la función de descifrado AES para que lea el voto cifrado de un fichero cifrado.DAT, tomando como entrada el nombre de dicho fichero, una clave longitud adecuada (y los parámetros que exija el método de descifrado); para que escriba el voto descifrado en otro fichero llamado descifrado.DAT.

- Implementar la función hash que se haya elegido, que al igual que la función de cifrado, lea el voto de VOTO.DAT, tomando como entrada el nombre de dicho fichero (y los parámetros que exija la función de hash, si es que los hay); para que escriba el resultado en otro fichero llamado resumen.DAT.

- Un informe descriptivo de las tres tareas anteriores en el que se argumente las decisiones tomadas a la hora de elegir el modo de cifrado y la función hash.

- Se deberá entregar a través de Moodle dos ficheros:

    a. El informe descriptivo de la práctica.

    b. El código fuente.