Planteamiento

Hasta ahora ya tenemos todas las herramientas básicas del protocolo de votación y el esquema del mismo definido en el guion general de prácticas. El último paso será la implementación de la interfaz y de las funciones criptográficas.

En lo referente a la interfaz, se deja vía libre al alumno para incluir la que más le convenga. Las interfaces no han sido parte del contenido de esta asignatura, así que no será evaluada en su calidad. Sin embargo, si será exigible que tenga una.

Por su parte, las funciones criptográficas han de tener como esquema de fondo las tres transmisiones que se han de hacer en el protocolo y la comprobación final:

(i) Identificación y propuesta de firma ciega

(ii) Comprobación de la identificación:
   a. Si ésta es negativa, se dará un mensaje advirtiéndolo y se cortará el flujo del programa.
   b. Si es positiva, se responderá adecuadamente.

(iii) Comprobación de la corrección de la respuesta de la Autoridad Electoral:
   a. Si la respuesta no corresponde con una firma ciega se dará un mensaje advirtiéndolo y se cortará el flujo del programa.
   b. Si la respuesta se corresponde con la firma ciega, se terminará de construir y se añadirá a la emisión del voto cifrado.

(iv) Validación de la corrección del voto:
   a. Si la información recibida no es coherente, se dará un mensaje advirtiendo de la falta de coherencia y el motivo de la misma.
   b. Si la respuesta es coherente, se almacenará el voto descifrado en un fichero que albergue todos los votos emitidos.

Trabajo a realizar durante la práctica

- Se deberá entregar a través de Moodle dos ficheros:

    a. Un breve manual de usuario que explique cómo usar la interfaz para acceder y hacer uso de los programas implementados.

    b. El código fuente.