

## SGSSI-23.Laboratorio6 (A.7.1)

### 1. Objetivos

Profundizar en el uso del *hash* criptográfico como soporte a la tecnología *blockchain*. Se seguirá trabajando su inclusión en el código y su uso dentro del contexto del minado de las cadenas de bloques (*blockchain*) SGSSI-23.CB.

Para las personas que completaron las actividades básicas del Lab05, se trata de recuperar esos contenidos, revisarlos y profundizar en nuevos aspectos.

Para las personas que no completaron las actividades del Lab05, o que tuvieron que pasar demasiado deprisa por ellas, sin asimilar lo realizado, es una oportunidad para terminar y consolidar lo trabajado, como paso previo a abordar las actividades propias del Lab06.

### 2. Desarrollo

Se podrá optar por trabajar individualmente o en grupo, pero siempre se elaborará y entregará un informe individual, sin perjuicio de que se puedan compartir contenidos, pruebas, etc. Si se trabaja en grupo, tendrá que ser de modo síncrono, esto es, con todas las personas del grupo trabajando en el mismo marco horario. Se podrá intercambiar y reutilizar el código de otros grupos/compañeros siempre que se respeten las exigencias de reconocimiento de los desarrolladores originales y/o se indique la fuente utilizada.

Se partirá de los informes elaborados y de los programas que se desarrollaron en los laboratorios anteriores (Lab04 y 05).

Tomando como punto de partida el que se alcanzó al final del [Lab05](#), se completarán, al menos, las actividades 1 y 2 (actividad 0 del presente). A continuación se irán realizando las actividades 1, 2 y 3 de este laboratorio.

Terminado el periodo de realización del laboratorio (o previamente) se realizará la entrega del [informe de realización del laboratorio](#) por medio de egela.

#### Actividad 0. Hash criptográfico y minado de bloques

Tomando como punto de partida los resultados del [Lab05](#), se completarán, al menos, las actividades 1 y 2 (preferiblemente, también la 3).

Ejecutar el programa desarrollado en la Actividad 2 (Lab05) tomando como entrada el fichero [SGSSI-23.CB.03.txt](#). Se nombrará al fichero resultante de la siguiente forma: SGSSI-23.CB.03.[0-9a-f]{2}.txt (siendo los dos caracteres el identificador personal en la *blockchain* SGSSI-23.CB). Aunque se haya realizado el laboratorio en grupo, cada persona deberá entregar su propio fichero.



**Actividad 1. Realizar un programa que, tomando como entrada un fichero de texto (con la forma que caracteriza a los *candidatos* de nuestra cadena de bloques) y un directorio que contiene ficheros de texto, obtiene como salida:**

1. La relación de ficheros contenidos en el directorio que cumplen (con respecto al fichero de entrada) las condiciones establecidas en la Actividad 3 del Lab05. Cada fichero debe tener asociada la longitud del prefijo de 0's de su resumen SHA-256.
2. El fichero, de entre los que contiene el directorio y cumplen las condiciones marcadas, cuyo resumen SHA-256 comienza por la secuencia de 0's más larga. En caso de empate, utiliza un criterio de tu elección, para seleccionar uno de los empatados

**Probar el funcionamiento tomando como entrada el fichero [SGSSI-23.CB.03.txt](#) y la carpeta [SGSSI-23.Lab06.CB.03.Candidatos](#).**

## **Actividad 2**

Crear un repositorio o un fichero con el código fuente desarrollado hasta el momento.

Crear un documento que incluya las instrucciones para descargar, compilar (si fuera necesario) y ejecutar el código fuente anterior. Se podrá incluir también una licencia que establezca limitaciones sobre el uso del código en cuestión.

## **Actividad 3 (opcional, sólo si se puede realizar en el marco de dedicaciones previstas)**

Versionar el programa resultante de la Actividad 1 para que el fichero seleccionado, de entre los que cumplen las condiciones, se obtenga como resultado de **un sorteo** entre las alternativas válidas. Puedes, adicionalmente, añadir una ponderación de las probabilidades de elección en función de la carga de trabajo incorporada (número de ceros del prefijo) o del número de *ehuskoin*s que corresponden, en ese bloque, al *minero-proponente*.