Tarea para PSP07.

Detalles de la tarea de esta unidad.

Enunciado.

Ejercicio 1.

De igual manera a lo visto en el tema, ahora te proponemos un ejercicio que genere una cadena de texto y la deje almacenada en un fichero encriptado, en la raíz del proyecto hayas creado, con el nombre `fichero.cifrado`.

Para encriptar el fichero, utilizarás el algoritmo `Rijndael` o AES, con las especificaciones de modo y relleno siguientes: `Rijndael/ECB/PKCS5Padding`.

La clave, la debes generar de la siguiente forma:

- Obtener un hash de un password (un String) con el algoritmo "SHA-256".
- Copiar con el método Arrays.copyOf los 192 bits a un array de bytes (192/8 bytes)
- Utilizar la clase SecretKeySpec para generar una clave a partir del array de bytes.

Para probar el funcionamiento, el mismo programa debe acceder al fichero encriptado para desencriptarlo e imprimir su contenido.

Criterios de puntuación. Total 10 puntos.

Total 10 puntos.

Se tendrá en cuenta:

- El funcionamiento correcto del programa.
- El uso adecuado del API criptográfico.
- Tratamiento adecuado de posibles excepciones.

Recursos necesarios para realizar la Tarea.

Los contenidos y ejemplos realizados en la Unidad.

Consejos y recomendaciones.

Ninguno en particular.

Indicaciones de entrega.

Elabora un documento con un procesador de texto donde expliques cómo has realizado los dos ejercicios de la tarea. El documento debe tener tamaño de página A4, estilo de letra Times New Roman, tamaño 12 e interlineado normal.

Debes enviar el informe, y los dos proyectos, comprimidos en un fichero.