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:

- A partir de un número aleatorio con semilla la cadena del nombre de usuario + password.
- Con una longitud o tamaño 128 bits.

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.

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.

El envío se realizará a través de la plataforma de la forma establecida para ello, y el archivo se nombrará siguiendo las siguientes pautas:

apellido1_apellido2_nombre_SIGxx_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la séptima unidad del MP de PSP**, debería nombrar esta tarea como...

sanchez_manas_begona_PSP07_Tarea

Memoria

Ejercicio01

El proyecto se ubica en el paquete01/Principal.java
He comenzado el proyecto dividiendo el programa en 4 partes:

Parte 01:
Me sirvo del método creaSemilla(Scanner sc) para solicitar el usuario y la contraseña y generar la semilla.

Parte 02:
Me sirvo del método generaClaveAES(String semilla) para generar una clave basada en el algoritmo AES, con una longitud de 128 y basada en un SecureRandom a partir de la semilla.

Parte 03:
Me sirvo del método escribeCifrado(SecretKey clave, Scanner sc) que solicita un mensaje al usuario, y lo escribe cifrado en un fichero de salida llamado Archivo.txt en la carpeta raíz del proyeto.

Parte 04:
Me sirvo del método leeDescifrado(SecretKey clave) para leer el fichero cifrado Archivo.txt de la carpeta raíz del proyecto, lo descifra y lo muestra por consola.

He envuelto todo en un try/catch para controlar cada una de las excepciones posibles de manera precisa.

Además del proyecto he creado otras dos clases, una para crear archivos cifrados (Cifrador.java) y otra para descifrarlos (Descifrador.java), he probado a crear un archivo cifrado, enviarlo por email a otra persona y que esa persona lo descifrara con el usuario y contraseña, y funciona ☺