

Act5.2. Almacenamiento seguro

Francisco José García Cutillas | 2FPGS_DAM

Índice

Ejercicio 1	3

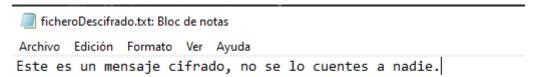
Ejercicio 1

Almacenamiento seguro

Programar una aplicación Java que reciba como parámetros de entrada un fichero y una contraseña, cifre el contenido utilizando AES, almacene el resultado con un nombre de fichero distinto y borre el fichero original.

Programar también la aplicación que realice la transformación inversa.

En el raíz de nuestro proyecto vamos a crear el fichero "ficheroDescifrado.txt", que será el que vamos a cifrar.



Lo primero que vamos a hacer es ejecutar el método "cifrar", introduciéndole por parámetros la ruta del fichero original, la del fichero a generar cifrado y una key que vamos a generar con el método "obtenerClave" que recibe una contraseña de tipo String.

```
package com.mycompany.pap_acts_2;

| import java.io.FileInputStream; | import java.io.FileInputStream; | import java.io.FileInputStream; | import java.corpto.Cipher; | import java.corpto.CipherinputStream; | import java.corpto.CipherinputStream; | import java.corpto.CipherinputStream; | import java.corpto.CipherinputStream; | import java.corpto.Sepressepec; | import javax.corpto.Sepressepec; | import javax.corpto.Sepressepec.Sepressepec; | import javax.corpto.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepressepec.Sepres
```

```
//Método para cifrar un fichero. Recibe la ruta del fichero a cifrar, la del nuevo licheto cifrado y una x
private static void cifrar (String ficheroSinCifrar, String nombreFicheroCifrar, Key key) throws Exception(
        Cipher cipher = Cipher.getInstance( transformation: "AES"); cipher.init( opmode: Cipher.ENCRYPT_MODE, key);
        FileInputStream fis = new FileInputStream(name:ficheroSinCifrar);
FileOutputStream fos = new FileOutputStream(name:nombreFicheroCifrar);
CipherOutputStream cos = new CipherOutputStream(os:fos, c:cipher);
        Cipher cipher = Cipher.getInstance( transformation: "AES");
cipher.init(opmode:Cipher.DECRYPT_MODE, key);
        FileInputStream fis = new FileInputStream(name:ficheroCifrado);
FileOutputStream fos = new FileOutputStream(name:nombreFicheroSinCifrar);
CipherInputStream ois = new CipherInputStream(is:fis, c:cipher);
```

Este será ahora nuestro fichero cifrado.

ficheroCifrado.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda |-0ÓE[pddâ1&ŒĐĐπȵÅÖ[]³š"g!Žeh`upïº?15µÝËñÄ5∅³äå)[w|.[ðY¢HR Ú‱

Vamos ahora a volverlo a descifrar.

```
public static void main(String[] args) {
    try {
        Key claveCifrado = obtenerClave(password: "estoesunacontraseña", longitud: l6);
        //cifrar("ficheroDescifrado.txt", "ficheroCifrado.txt", claveCifrado);

        descifrar(ficheroCifrado: "ficheroCifrado.txt", nombreFicheroSinCifrar: "ficheroDescifrado.txt", key: claveCifrado);
    } catch (Exception ex) {
        System.out.println("Error: " + ex.getMessage());
    }
}
```

Volvemos a tener el fichero descifrado.

ficheroDescifrado.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

Este es un mensaje cifrado, no se lo cuentes a nadie.