**ACTIVIDAD 2**

**Enunciado**

Realiza un programa en Java que verifique la validez de un fichero de firma previamente generado. A modo orientativo, la estructura del programa podría ser la siguiente:

* Leer la clave pública del fichero a verificar. Dicha clave está dentro de un fichero de nombre *Clave.publica* disponible en la plataforma.
* Recuperar la clave pública desde los datos codificados en formato X509 y mediante el algoritmo *DSA*.
* Leer el fichero que contiene la firma. Dicho fichero se llama *FICHERO.FIRMA* y está disponible en la plataforma.
* Inicializar el objeto *Signature* con la clave pública que se va a usar para verificar la validez del fichero y mediante el algoritmo *SHA1withDSA.*
* Leer el fichero que contiene los datos a verificar (*FICHERO.DAT*), el cual está disponible en la plataforma.
* Verificar la firma de los datos leídos del fichero *FICHERO.DAT.*
* Comprobar la verificación de los datos leídos. Si la verificación es correcta se mostrará el mensaje “LOS DATOS SE CORRESPONDEN CON SU FIRMA”. En caso contrario, se mostrará este otro mensaje: “LOS DATOS NO SE CORRESPONDEN CON SU FIRMA”.

El programa gestionará las posibles excepciones que se puedan producir durante su ejecución.

El nombre de la clase principal será Actividad2.

**Solución**

package ACT2;

import java.io.BufferedInputStream;

import java.io.File;

import java.io.FileInputStream;

import java.io.IOException;

import java.security.InvalidKeyException;

import java.security.KeyFactory;

import java.security.NoSuchAlgorithmException;

import java.security.PublicKey;

import java.security.Signature;

import java.security.SignatureException;

import java.security.spec.InvalidKeySpecException;

import java.security.spec.X509EncodedKeySpec;

public class Actividad2 {

public static void main(String[] args) {

// Abrimos los archivos en el try, para que se cierren solos

try (

// Clave publica

FileInputStream fisPublica = new FileInputStream(new File("UD5/ACT2/Clave.publica"));

// Fichero con la firma

FileInputStream fisFirma = new FileInputStream(new File("UD5/ACT2/FICHERO.FIRMA"));

) {

// Leemos la clave publica y la ponemos en un buffer

byte[] bufferPublica = new byte[fisPublica.available()];

fisPublica.read(bufferPublica);

// Ponemos la clave en formato x509

X509EncodedKeySpec clavePublicaSpec = new X509EncodedKeySpec(bufferPublica);

KeyFactory keyDSA = KeyFactory.getInstance("DSA");

PublicKey clavePublicaKey = keyDSA.generatePublic(clavePublicaSpec);

// Leemos la firma

byte[] bufferFirma = new byte[fisFirma.available()];

fisFirma.read(bufferFirma);

// Verificamos la clave publica con SHA1withDSA

Signature signature = Signature.getInstance("SHA1withDSA");

signature.initVerify(clavePublicaKey);

// Leemos los datos

// Fichero con la información

BufferedInputStream bisDat = new BufferedInputStream(new FileInputStream(new File("UD5/ACT2/FICHERO.DAT")));

byte[] bufferDatos = bisDat.readAllBytes();

System.out.println(new String(bufferDatos));

signature.update(bufferDatos);

// Verificamos si los datos que tenemos y los que nos llegan son los mismos

if (signature.verify(bufferFirma)) {

System.out.println("LOS DATOS SE CORRESPONDEN CON SU FIRMA");

} else {

System.out.println("LOS DATOS NO SE CORRESPONDEN CON SU FIRMA");

}

} catch (IOException | NoSuchAlgorithmException | InvalidKeySpecException | InvalidKeyException | SignatureException e) {

e.printStackTrace();

}

}

}

**Resolución de problemas**

**CRITERIOS DE CORRECCIÓN**

1. Nivel de ajuste a la nomenclatura de objetos definida en el enunciado de la actividad y nivel de ajuste al almacenamiento de la información requerida en las subcarpetas definidas para la actividad y unidad didáctica correspondientes (15%).
2. Hacer lo que se indica en el enunciado (55%).
3. Claridad del código Java (15%).
4. Documentación del código Java (15%).
5. Explicación detallada de cómo se han resuelto problemas que hayan podido surgir en la realización de la actividad (hasta un 15% adicional sobre la nota obtenidaVariables no usadas (-15%).
6. Librerías no usadas (-15%).