



Mòdul 9
DAM 2

Autor

Unitat formativa

Pràctica

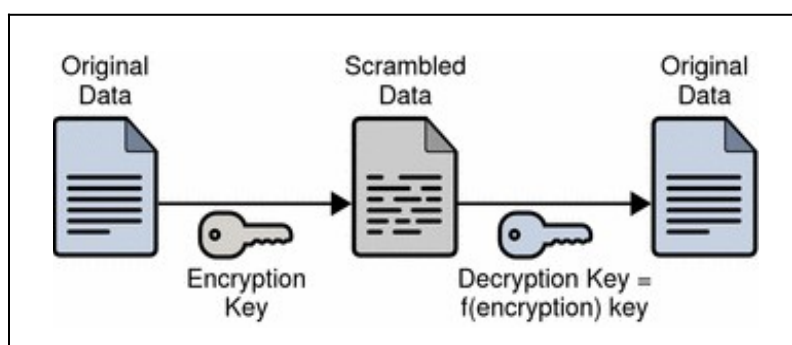
Programació de serveis i
processos

Helena Madrenys Planas

UF1 – Programació d'adaptacions segures en
xarxa

Examen – 18/01/2022

Examen UF1





Índex

Codi Complert.....	3
Package, author i imports.....	3
Funció Main.....	3
Funció per generar clau.....	4
Funció per encriptar.....	5
Funció Desencriptar.....	6
Output.....	7
Consola Eclipse.....	7
Link del Video.....	7

Codi Complert

Package, author i imports

```
1 package madrenys.helena.uf1.examen;
2
3 // @author: Helena Madrenys Planas
4
5 import java.io.File;
6 import java.io.FileWriter;
7 import java.io.IOException;
8 import java.security.MessageDigest;
9 import java.util.Arrays;
10 import java.util.Base64;
11 import java.util.Scanner;
12
13 import javax.crypto.Cipher;
14 import javax.crypto.SecretKey;
15 import javax.crypto.spec.SecretKeySpec;
16
```

Funció Main

Primer de tot farem la part per crear el fitxer i el seu contingut xifrat. Anirem cridant les funcions pertinents per a fer cada acció i al final, crearem un «FileWriter» per a escriure el contingut del fitxer.

```
17 public class MadrenysHelenaEx1a {
18     public static void main(String[] args) throws IOException {
19         // Creem el fitxer-----
20         // Creem el missatge
21         String missatge = "Helena Madrenys Planas";
22         System.out.println("El missatge és: " + missatge);
23
24         // Creem la contrassenya
25         String contrassenya = "333";
26         System.out.println("La contrassenya serà: " + contrassenya);
27
28         // Generar les claus simètriques a partir de contrassenya
29         SecretKey clauS = generarClauContrassenya(contrassenya, "SHA-256", "AES", 128);
30
31         // Encriptem el missatge
32         String encriptat = encriptar(clauS, missatge);
33         System.out.println("Al fitxer s'hi ha escrit: " + encriptat);
34
35         // Posem el missatge en un fitxer
36         FileWriter myWriter = new FileWriter("missatge.dat");
37         myWriter.write(encriptat);
38         myWriter.close();
39         System.out.println("S'ha omplert el fitxer correctament.");
40     }
41 }
```

A continuació llegirem el fitxer línia a línia amb un «while», demanarem la contrasenya, la farem servir per obtenir el «SecretKey» i desencritparem usant la funció pertinent.

```
41 //Llegim el fitxer-----
42 File fitxer = new File("missatge.dat");
43 Scanner scFitxer = new Scanner(fitxer);
44 String contXifrat = "";
45 while (scFitxer.hasNextLine()) {
46     contXifrat += scFitxer.nextLine();
47 }
48 scFitxer.close();
49 System.out.println("El contingut del fitxer xifrat és:" + contXifrat);
50
51 //Demanem la contrassenya i creem la clau
52 System.out.println("Escriu la contrassenya del fitxer:");
53 Scanner sc = new Scanner(System.in);
54 String decryptPsswd = sc.nextLine();
55 sc.close();
56 SecretKey decryptKey = generarClauContrassenya(decryptPsswd, "SHA-256", "AES", 128);
57 //Desxifrem i mostrem
58 try {
59     String contDesxifrat = descriptar(decryptKey, contXifrat);
60     System.out.println("El contingut desxifrat és: " + contDesxifrat);
61 } catch (Exception e)
62 {
63     System.out.println("Clau incorrecte.");
64 }
65
66 //Text interceptat: wgX/X/Dzp8qtHRI7KZE/7KucmtNIAqAzoxWTSOJw1AQA=
67 //Contrassenya: 333
68 }
```

Funció per generar clau a partir de contrasenya

Per a generar la clau a partir de contrasenya primer de tot passarem aquesta a bytes «getBytes()». Després fent servir la classe «MessageDigest» obtindrem el resum, i amb «SecretKeySpec» obtindrem la clau.

```
70 //Funció generar clau a partir de contrassenya
71 public static SecretKey generarClauContrassenya(String text, String alHash, String algorisme, int keySize)
72 {
73     SecretKey sKey = null;
74     try
75     {
76         byte[] data = text.getBytes("UTF-8");
77         MessageDigest md = MessageDigest.getInstance(alHash);
78         byte[] hash = md.digest(data);
79         byte[] key = Arrays.copyOf(hash, keySize/8);
80         sKey = new SecretKeySpec(key, algorisme);
81     }
82     catch (Exception e)
83     {
84         System.err.println("Hi ha hagut un error " + e);
85         return null;
86     }
87     return sKey;
88 }
```

Funció per encriptar

Per a encriptar, farem ús de la classe «Cipher» amb els paràmetres demanats per l'exercici: AES, ECB i PKCS5Padding.

```
88 //Funció per encriptar-----
89 public static String encriptar(SecretKey sKey, String missatge) {
90     //Creem l'array on hi col·locarem les dades encriptades
91     byte[] encriptat = null;
92     try {
93         //Creem un objecte cipher amb els paràmetres desitjats
94         Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
95
96         //L'inicialitzem amb el mode d'encriptació i la clau generada anteriorment
97         cipher.init(Cipher.ENCRYPT_MODE, sKey);
98
99         //Encriptem
100         encriptat = cipher.doFinal(missatge.getBytes());
101     } catch (Exception ex) {
102         System.err.println("Error xifrant les dades.");
103     }
104
105     //Passem el missatge de byte[] a String i el retornem
106     String txtreturn = Base64.getEncoder().encodeToString(encriptat);
107     return txtreturn;
108 }
```



Funció Desencriptar

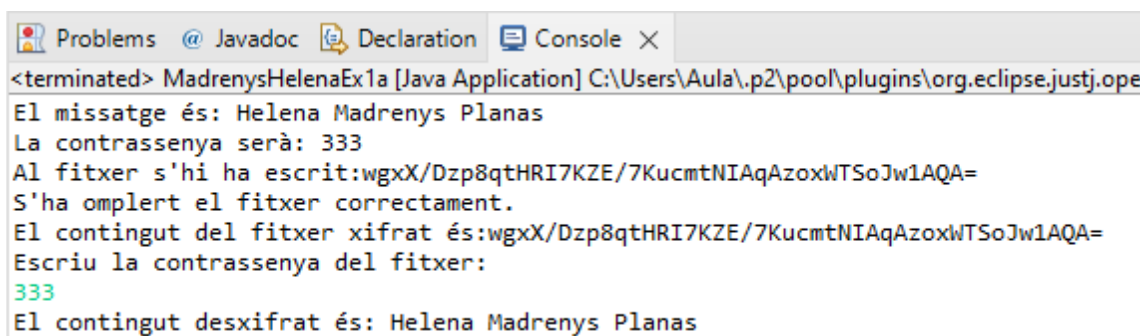
Per a desencriptar farem el mateix procés però farem servir el mode «Decrypt_Mode».

```
109 //Funció per desencriptar-----
110 public static String desencriptar(SecretKey sKey, String missatge) {
111     //Creem l'array on hi col·locarem les dades desencriptades
112     byte[] desencriptat = null;
113     try {
114         //Creem un objecte cipher amb els paràmetres desitjats
115         Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
116
117         //L'inicialitzem amb el mode de desenccriptació i la clau generada anteriorment
118         cipher.init(Cipher.DECRYPT_MODE, sKey);
119
120         //Desencriptem
121         desencriptat = cipher.doFinal(Base64.getDecoder().decode(missatge));
122     } catch (Exception ex) {
123         System.out.println("Error desxifrant les dades.");
124     }
125
126     //Passem el missatge de byte[] a String i el retornem
127     String txtreturn = new String(desencriptat);
128     return txtreturn;
129 }
130 }
```



Output

Consola Eclipse



```
<terminated> MadrenysHelenaEx1a [Java Application] C:\Users\Aula\.p2\pool\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64.jdk-11.0.10\bin\java.exe
El missatge és: Helena Madrenys Planas
La contrassenya serà: 333
Al fitxer s'hi ha escrit:wgxX/Dzp8qtHRI7KZE/7KucmtNIAqAzoxWTS0Jw1AQA=
S'ha omplert el fitxer correctament.
El contingut del fitxer xifrat és:wgxX/Dzp8qtHRI7KZE/7KucmtNIAqAzoxWTS0Jw1AQA=
Escriu la contrassenya del fitxer:
333
El contingut desxifrat és: Helena Madrenys Planas
```