Activitat

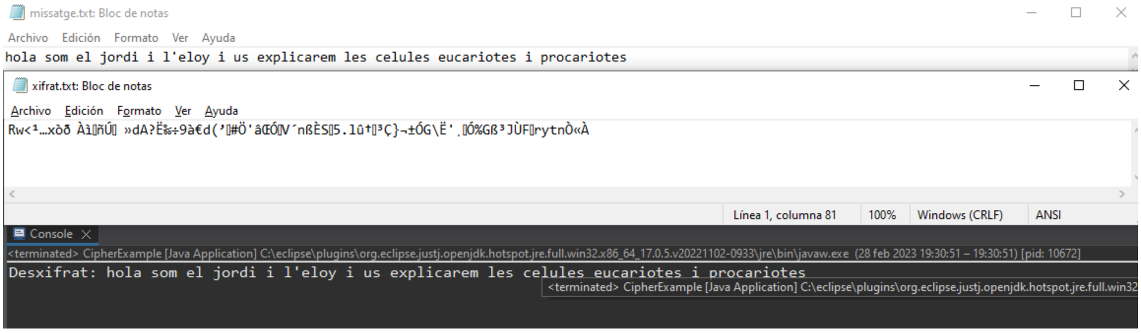
Classe on xifrem:

```
import java.io.File;

import java.io.FileOutputStream;

import java.io.ObjectOutputStream;

import java.nio.file.Files;

import java.security.SecureRandom;


import javax.crypto.Cipher;

import javax.crypto.KeyGenerator;

import javax.crypto.SecretKey;

import javax.crypto.spec.IvParameterSpec;


public class Xifrar {


      public static void main(String[] args) throws Exception {

          String inputFile = "missatge.txt";

          String outputFile = "xifrat.txt";

          String keyFile = "clau.txt";

          SecretKey secretKey = null;

          byte[] iv = new byte[8];

          KeyGenerator keyGen = KeyGenerator.getInstance("DES");

          SecureRandom random = new SecureRandom();

          secretKey = keyGen.generateKey();


          FileOutputStream keyFileStream = new
FileOutputStream(keyFile);

          ObjectOutputStream keyOutStream = new
ObjectOutputStream(keyFileStream);
```

```
        keyOutStream.writeObject(secretKey);
        keyOutStream.writeObject(secretKey.getAlgorithm());
        keyOutStream.writeObject(secretKey.getEncoded());
        keyOutStream.close();

        Cipher desCipher =
Cipher.getInstance("DES/CBC/PKCS5Padding");
        random.nextBytes(iv);
        desCipher.init(Cipher.ENCRYPT_MODE, secretKey, new
IvParameterSpec(iv));

        byte[] input = Files.readAllBytes(new
File(inputFile).toPath());

        int paddingLength = 8 - (input.length % 8);
        byte[] paddedInput = new byte[input.length + paddingLength];
        System.arraycopy(input, 0, paddedInput, 0, input.length);

        byte[] output = desCipher.doFinal(paddedInput);

        byte[] outputWithIV = new byte[iv.length + output.length];
        System.arraycopy(iv, 0, outputWithIV, 0, iv.length);
        System.arraycopy(output, 0, outputWithIV, iv.length,
output.length);

        FileOutputStream outputFileStream = new
FileOutputStream(outputFile);
        outputFileStream.write(outputWithIV);
        outputFileStream.close();
    }
}
```

Classe on desxifrem:

```
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.ObjectInputStream;
import java.nio.file.Files;
import java.security.spec.KeySpec;

import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;
import javax.crypto.spec.IvParameterSpec;

public class DesXifrar {

      public static void main(String[] args) throws Exception {
          String inputFile = "xifrat.txt";
          String outputFile = "desxifrat.txt";
          String keyFile = "clau.txt";
          byte[] iv = new byte[8];

          FileInputStream keyFileStream = new
FileInputStream(keyFile);
          ObjectInputStream keyInStream = new
ObjectInputStream(keyFileStream);
          SecretKey secretKey = (SecretKey) keyInStream.readObject();
          String algorithm = (String) keyInStream.readObject();
          byte[] encoded = (byte[]) keyInStream.readObject();
          keyInStream.close();
          KeySpec keySpec = new DESKeySpec(encoded);
          SecretKeyFactory keyFactory =
SecretKeyFactory.getInstance(algorithm);
          SecretKey reconstructedKey =
keyFactory.generateSecret(keySpec);

          Cipher desCipher =
Cipher.getInstance("DES/CBC/PKCS5Padding");
          FileInputStream ivStream = new FileInputStream(inputFile);
          ivStream.read(iv);
          ivStream.close();
          desCipher.init(Cipher.DECRYPT_MODE, reconstructedKey, new
IvParameterSpec(iv));

          byte[] input = Files.readAllBytes(new
File(inputFile).toPath());
          byte[] output = desCipher.doFinal(input, 8, input.length -
8);

          FileOutputStream outputFileStream = new
FileOutputStream(outputFile);
          outputFileStream.write(output);
          outputFileStream.close();
      }
}
```



missatge.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

```
hola som el jordi i l'eloy i us explicarem les celules eucariotes i procariotes
```

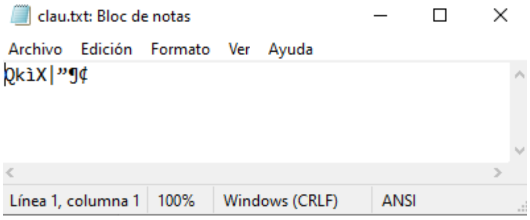
xifrat.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda

```
Rw<¹…xòð Àì▯ñÚ▯ »dA?Ë‰÷9à€d(’▯#Ö'âŒÓ▯V´nßÈS▯5.1û†▯³Ç}¬±ÓG\Ë'¸▯Ó%Gß³JÙF▯rytnÒ«À
```

Línea 1, columna 81
100%
Windows (CRLF)
ANSI
Console

```
<terminated> CipherExample [Java Application] C:\eclipse\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64_17.0.5.v20221102-0933\jre\bin\javaw.exe  (28 feb 2023 19:30:51 – 19:30:51) [pid: 10672]
Desxifrat: hola som el jordi i l'eloy i us explicarem les celules eucariotes i procariotes
```

En aquesta captura podem veure el missatge normal, el missatge xifrat i el missatge desencriptat per terminal



```
QkìX|”¶¢
```

En aquesta captura podem veure quina es la clau que ha fer servir per a encriptar i desencriptar el fitxer

Autoavaluació:

Creiem que ho tenim tot be ja que ens xifra i ho desxifra amb la clau transparent que s'ha creat.

1. Genera bé la clau i ho llegeix bé el fitxer on hi surt el missatge a encriptar 2/2

2. Encripta el fitxer i ho guarda en un altre 2/2

3. Es guarda bé les dades de la clau en un altre fitxer 2/2

4. Hem fet el codi de desencriptar i ens retorna bé el missatge desencriptar i es el mateix que l'original 2/2

5. Comentat el codi amb imatges que funciona l'aplicació 1/1