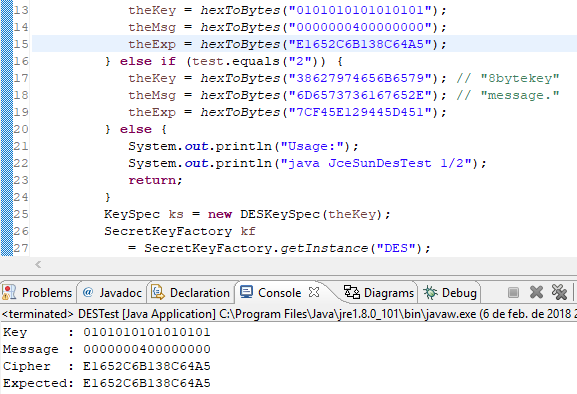
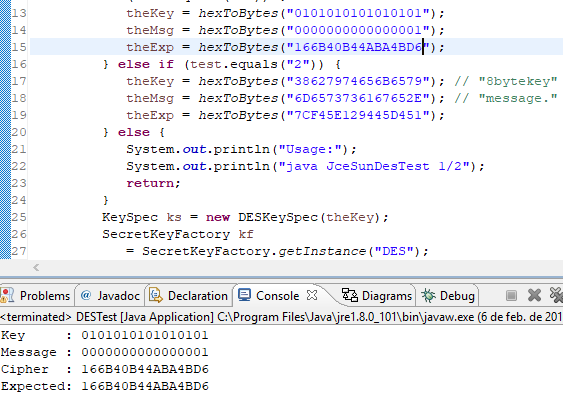
Eileen Guerrero Gomez

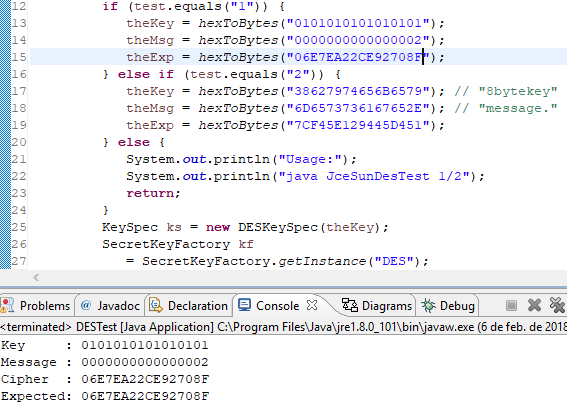
Código: A00021576

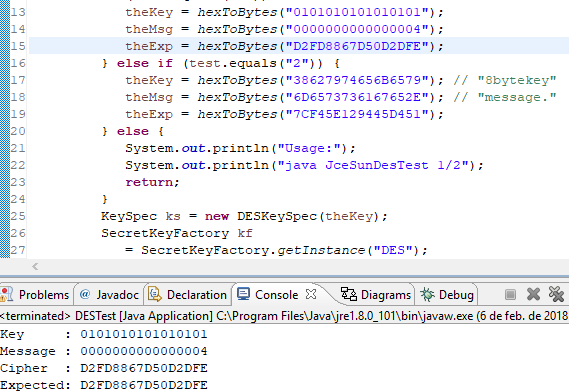
**Pruebas de la API de criptografía de Java**

**Parte 1**



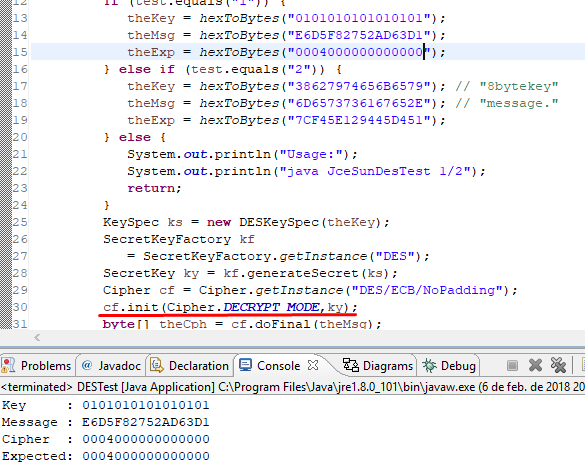


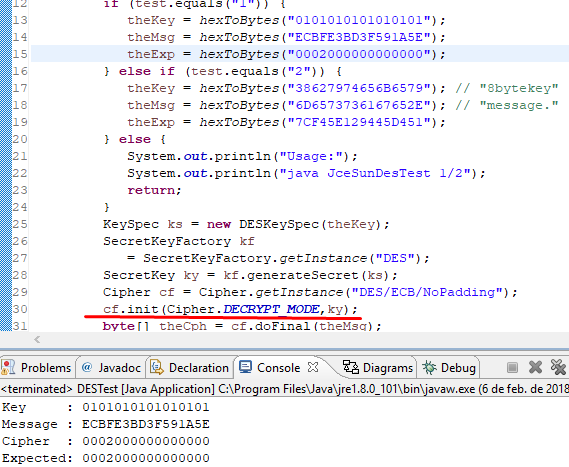


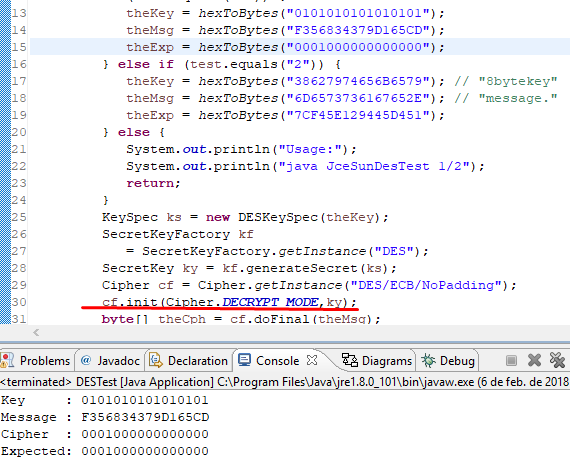


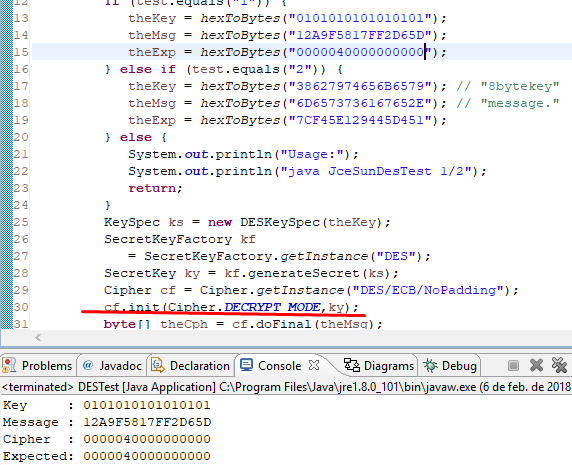
**Parte 2**

Para esta segunda parte solo le cambie la línea subrayada en color rojo.



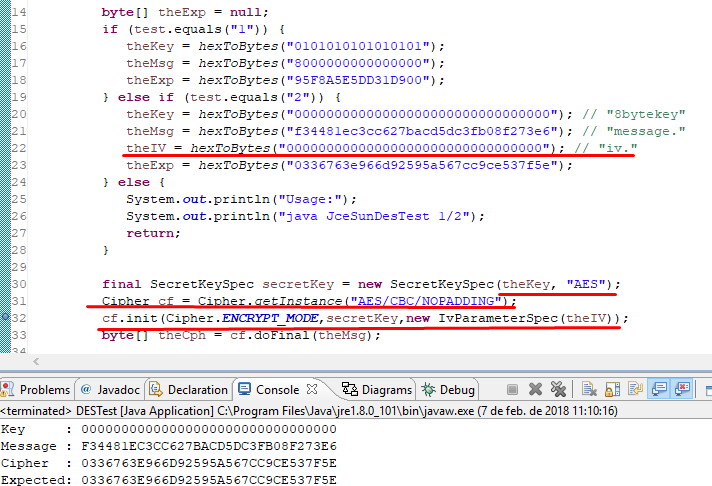


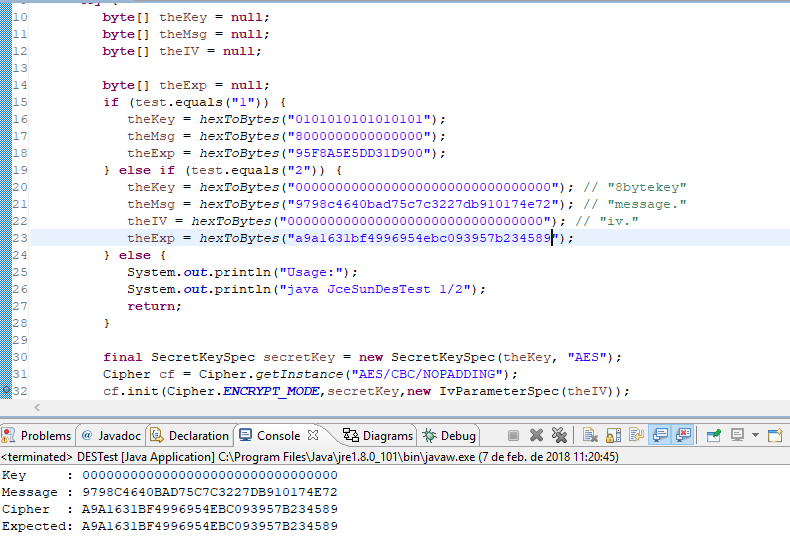


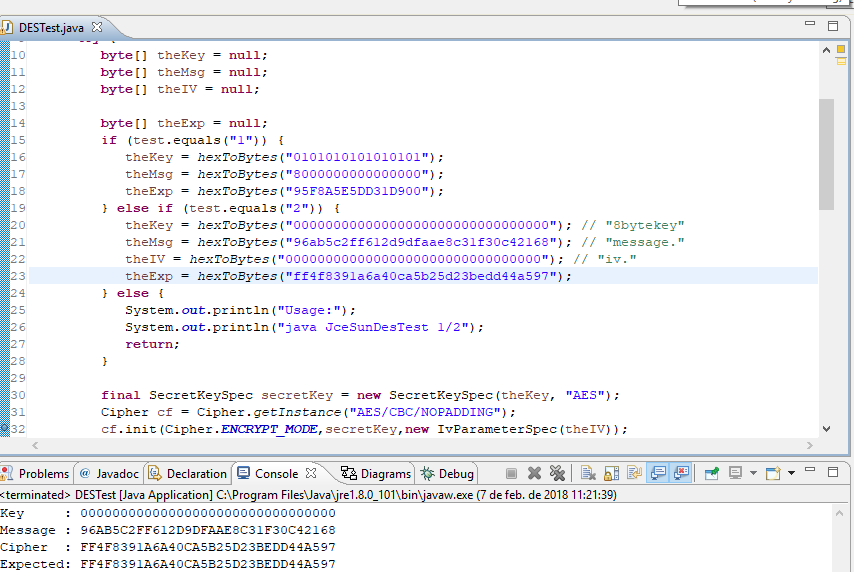


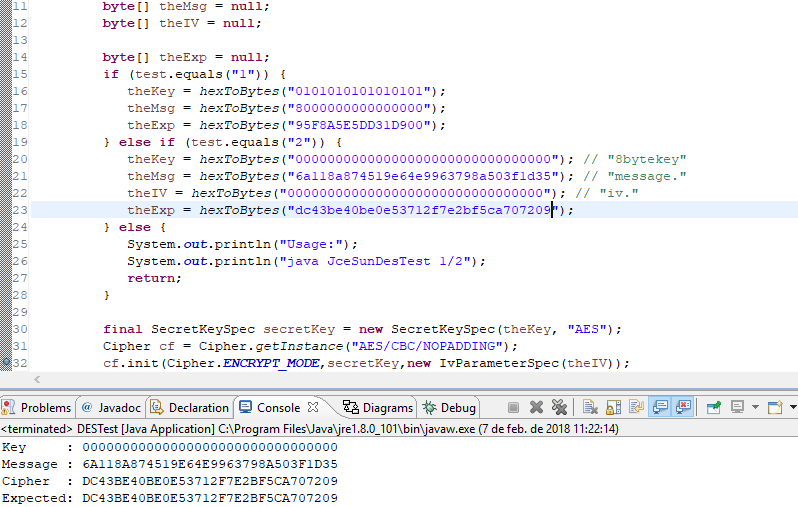
**Parte 3**

Modificación del algoritmo para cifrar en AES. Las líneas modificadas están subrayadas en color rojo.









Algoritmo modificado:

**import** javax.crypto.\*;

**import** javax.crypto.spec.\*;

**class** DESTest {

**public** **static** **void** main(String[] args) {

String test = "2";

**try** {

**byte**[] theKey = **null**;

**byte**[] theMsg = **null**;

**byte**[] theIV = **null**;

**byte**[] theExp = **null**;

**if** (test.equals("1")) {

theKey = *hexToBytes*("0101010101010101");

theMsg = *hexToBytes*("8000000000000000");

theExp = *hexToBytes*("95F8A5E5DD31D900");

} **else** **if** (test.equals("2")) {

theKey = *hexToBytes*("00000000000000000000000000000000"); // "8bytekey"

theMsg = *hexToBytes*("6a118a874519e64e9963798a503f1d35"); // "message."

theIV = *hexToBytes*("00000000000000000000000000000000"); // "iv."

theExp = *hexToBytes*("dc43be40be0e53712f7e2bf5ca707209");

} **else** {

System.***out***.println("Usage:");

System.***out***.println("java JceSunDesTest 1/2");

**return**;

}

**final** SecretKeySpec secretKey = **new** SecretKeySpec(theKey, "AES");

Cipher cf = Cipher.*getInstance*("AES/CBC/NOPADDING");

cf.init(Cipher.***ENCRYPT\_MODE***,secretKey,**new** IvParameterSpec(theIV));

**byte**[] theCph = cf.doFinal(theMsg);

System.***out***.println("Key : "+*bytesToHex*(theKey));

System.***out***.println("Message : "+*bytesToHex*(theMsg));

System.***out***.println("Cipher : "+*bytesToHex*(theCph));

System.***out***.println("Expected: "+*bytesToHex*(theExp));

} **catch** (Exception e) {

e.printStackTrace();

**return**;

}

}

**public** **static** **byte**[] hexToBytes(String str) {

**if** (str==**null**) {

**return** **null**;

} **else** **if** (str.length() < 2) {

**return** **null**;

} **else** {

**int** len = str.length() / 2;

**byte**[] buffer = **new** **byte**[len];

**for** (**int** i=0; i<len; i++) {

buffer[i] = (**byte**) Integer.*parseInt*(

str.substring(i\*2,i\*2+2),16);

}

**return** buffer;

}

}

**public** **static** String bytesToHex(**byte**[] data) {

**if** (data==**null**) {

**return** **null**;

} **else** {

**int** len = data.length;

String str = "";

**for** (**int** i=0; i<len; i++) {

**if** ((data[i]&0xFF)<16) str = str + "0"

+ java.lang.Integer.*toHexString*(data[i]&0xFF);

**else** str = str

+ java.lang.Integer.*toHexString*(data[i]&0xFF);

}

**return** str.toUpperCase();

}

}

}