



Universidad
Carlos III de Madrid

Universidad Carlos III de Madrid

Practica 2. Cifrado en Java.

GUIA DE USO.

Criptografía y Seguridad Informática

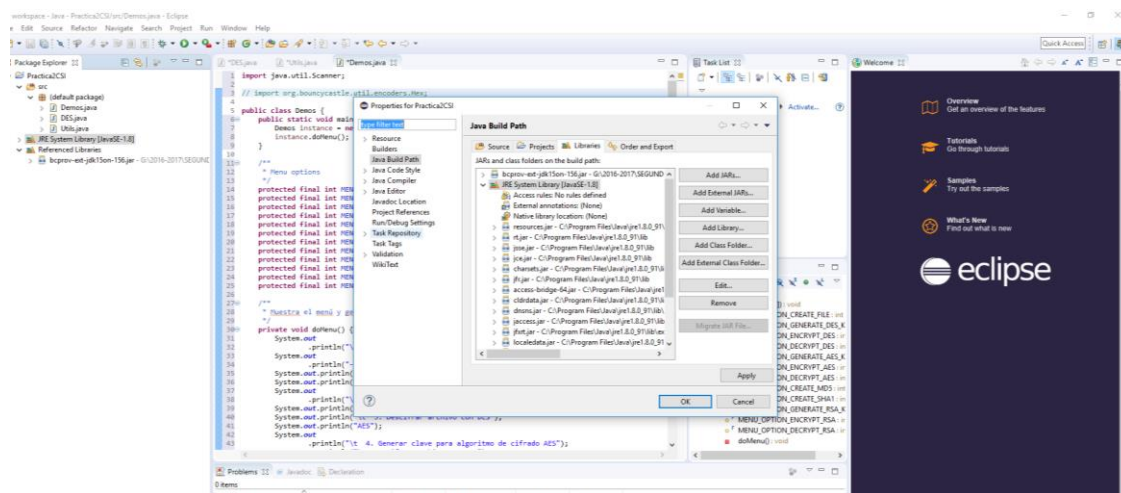
Curso 2016/2017

Federico Banda Sierra.

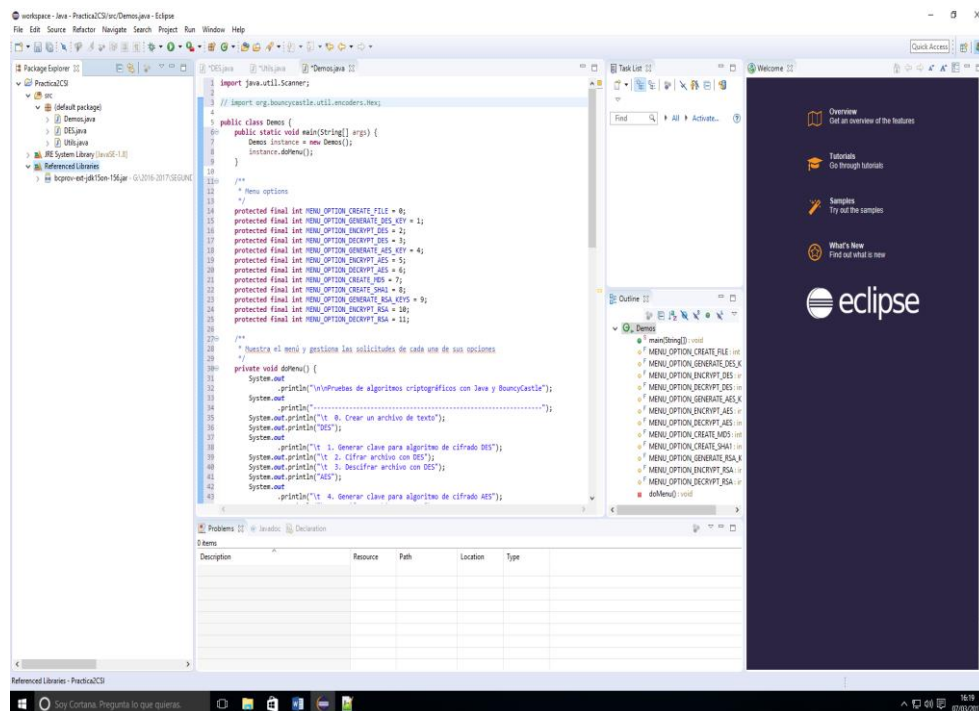
Iván Vicente León Fernández.

1.- Cómo integrar el código fuente de los algoritmos DES, AES, HASH, RSA y DEMOS en el IDE (entorno integrado de desarrollo) Eclipse.

1. Incluir las librerías (JRE SYSTEM LIBRARY/ADD EXTERNAL JAIR)

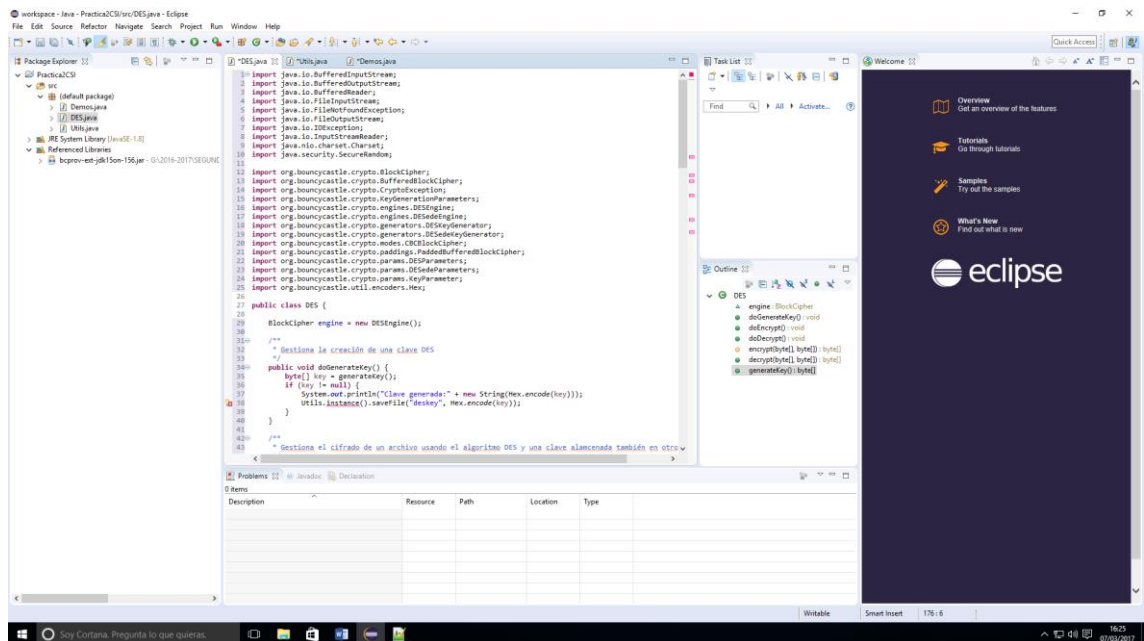


Añadir la librería bcprov-ext-jdk15on-156.jar

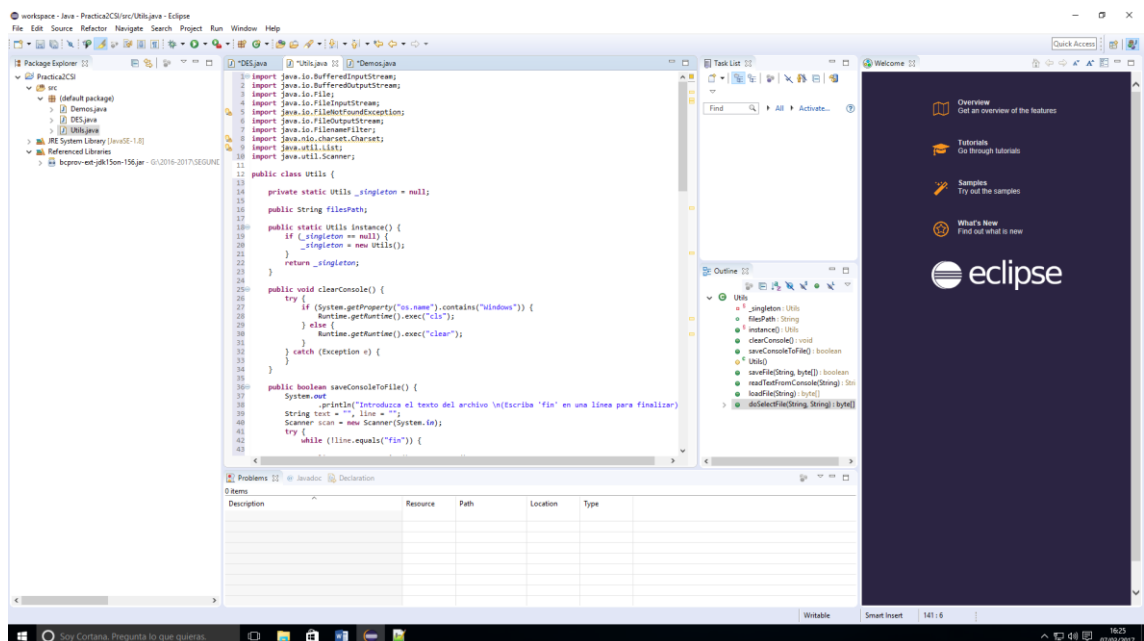


2. Vamos a probar la clase DES.java (para lo cual necesitamos introducir la clase Utils.java así como la clase principal genérica Demos.java)

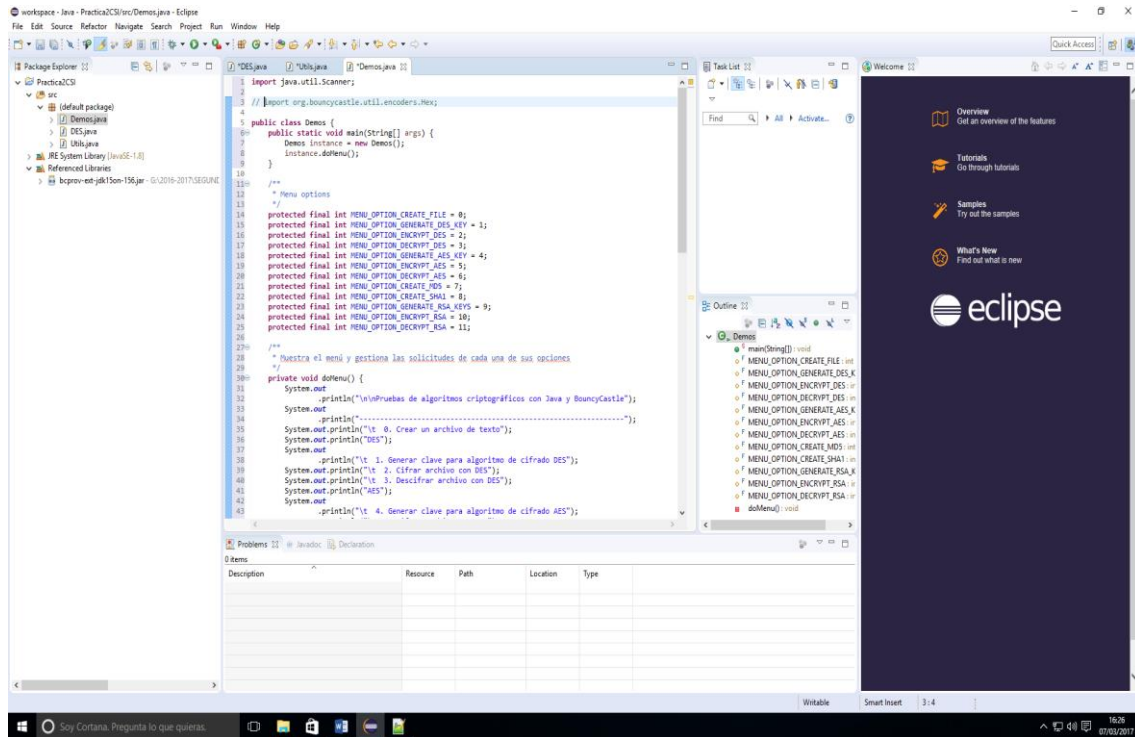
1. Introducimos la clase DES.java



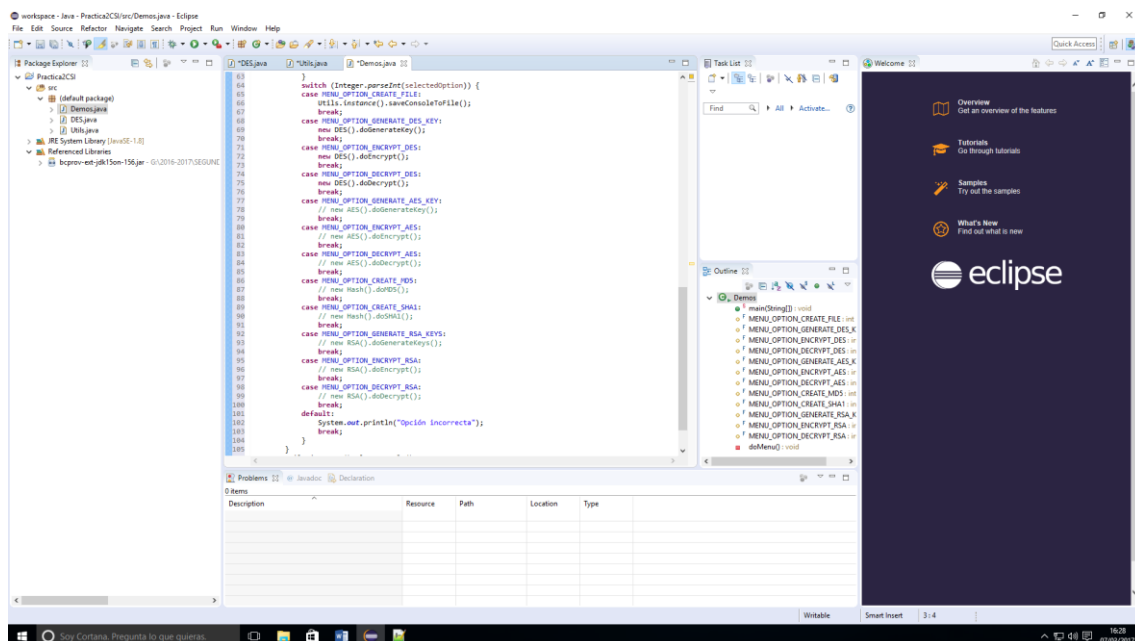
2. Introducimos la clase Utils.java



3. Introducimos la clase Demos.java (asteriscando todas las opciones que no son las del ALGORITMO DES, para solo probar el DES).



Asteriscando quedaría así:



3. Así para cada una de las clases siguientes (AES.java, Hash.java y RSA.java).

4. A continuación seguimos el enunciado de la práctica 2 propuesta de modo que lo primero que tenemos que hacer es

a. CREAR UN ARCHIVO DE TEXTO.

Esta opción es importante para ir viendo las distintas ejecuciones de los distintos algoritmos.

b. GENERAR UNA CLAVE PARA EL ALGORITMO DE CIFRADO DE DES.

c. CIFRAR EL ARCHIVO CON DES.

d. DESCRIFRAR EL ARCHIVO CON DES.

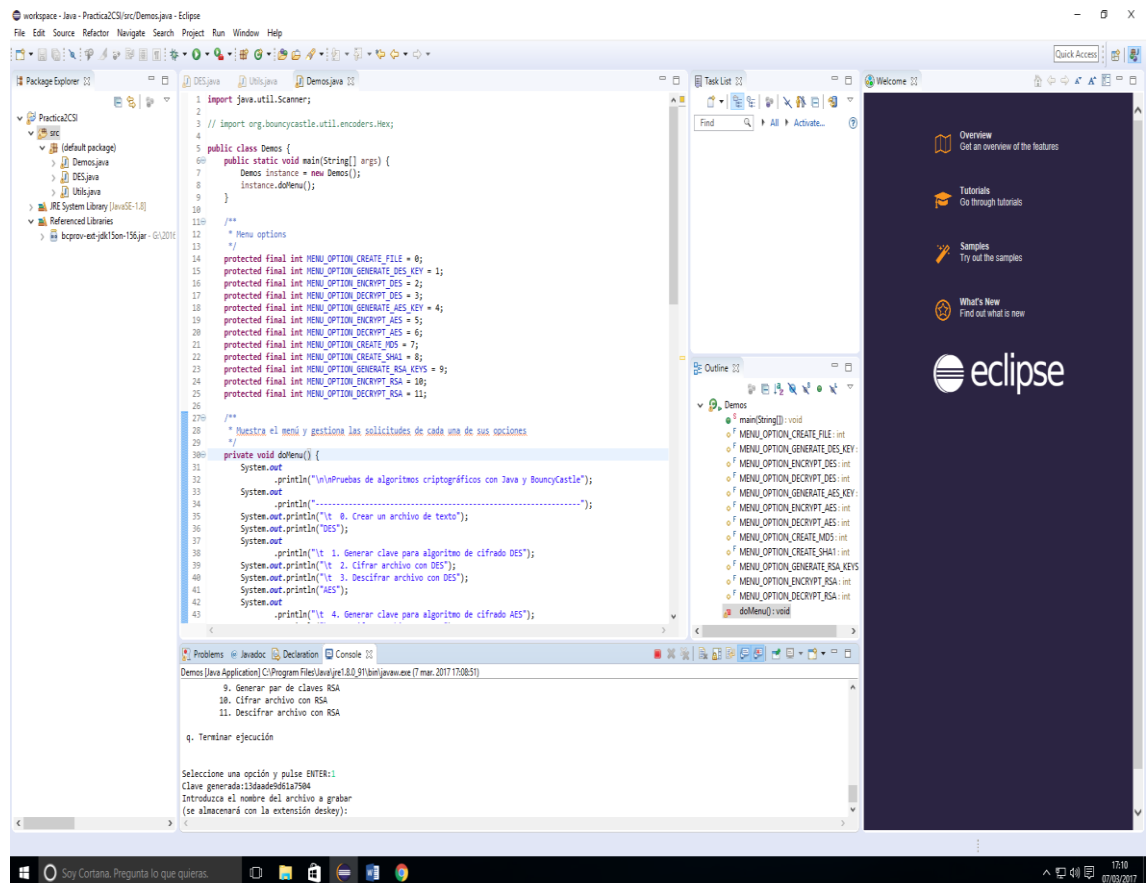
2.- Ejemplo de Ejecución del Algoritmo DES.

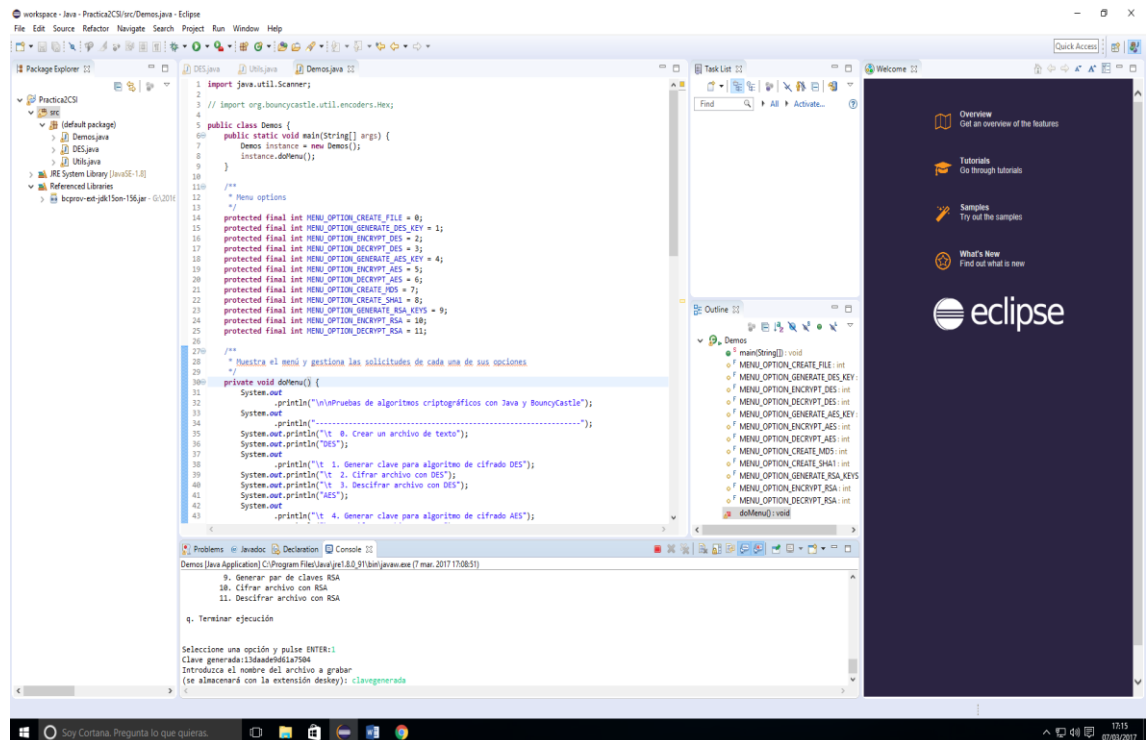
1. Creamos el fichero con el texto (por ejemplo),

CIFRADO DES, AES, RSA Y HASH

Lo guardamos con el nombre CIFRADOJAVA.TXT

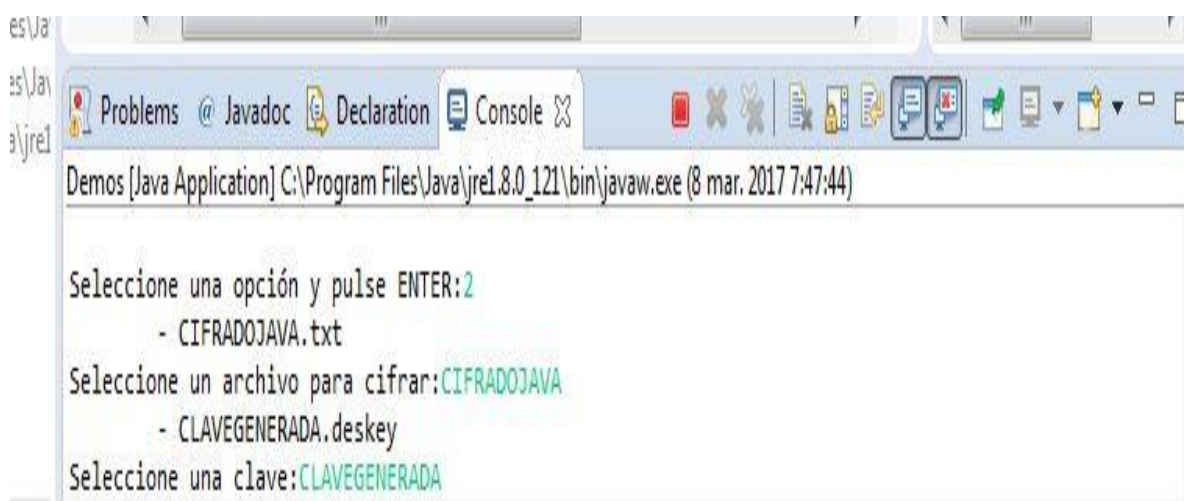
2. Generamos la clave para el algoritmo DES.





Guardamos con el nombre (por ejemplo)
CLAVEGENERADA.DESKEY

3. Ciframos el archivo con DES (OPCIÓN 2)



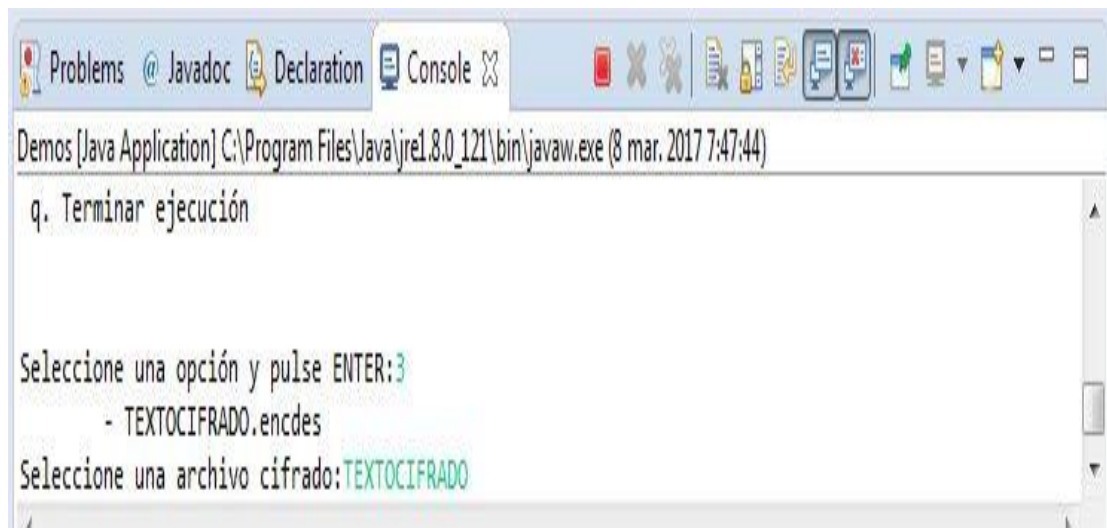

```
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 7:47:44)
Seleccione un archivo para cifrar: CIFRADOJAVA
- CLAVEGENERADA.deskey
Seleccione una clave: CLAVEGENERADA
Texto cifrado (en hexadecimal): 73d0a7f7a3f61834e9eea48ac2f7e965493f6d5371a3efb5d5acb408afa364a0
Introduzca el nombre del archivo a grabar
(se almacenará con la extensión encdes):
```

```
Problems Javadoc Declaration Console
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 7:47:44)
Seleccione un archivo para cifrar: CIFRADOJAVA
- CLAVEGENERADA.deskey
Seleccione una clave: CLAVEGENERADA
Texto cifrado (en hexadecimal): 73d0a7f7a3f61834e9eea48ac2f7e965493f6d5371a3efb5d5acb408afa364a0
Introduzca el nombre del archivo a grabar
(se almacenará con la extensión encdes): TEXTOCIFRADO
```

4. Desciframos el archivo con DES (OPCION 3) .

```
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 7:47:44)
q. Terminar ejecución

Seleccione una opción y pulse ENTER: 3
- TEXTOCIFRADO.encdes
Seleccione una archivo cifrado:
```

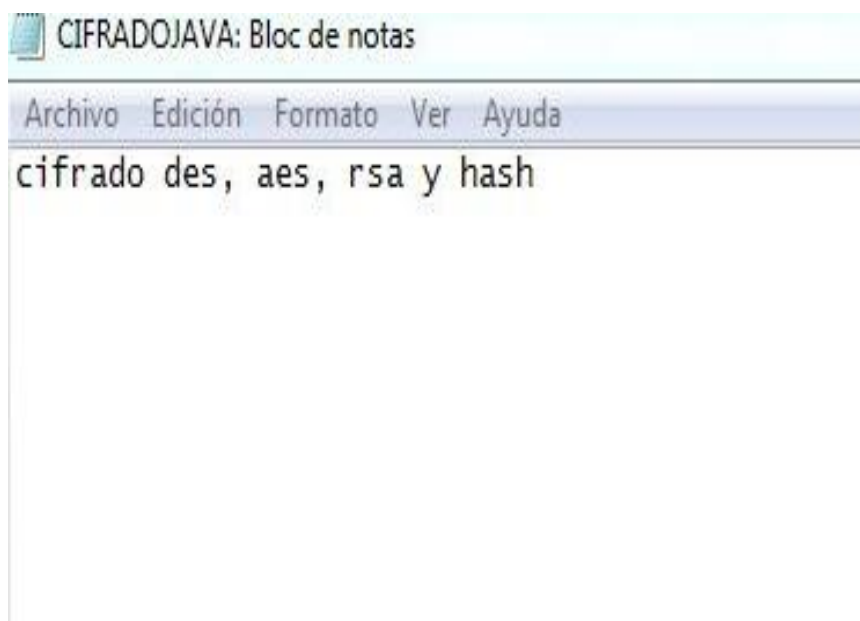
```
Problems @ Javadoc Declaration Console X
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 7:47:44)
q. Terminar ejecución

Seleccione una opción y pulse ENTER:3
- TEXTOCIFRADO.encdes
Seleccione una archivo cifrado:TEXTOCIFRADO
```



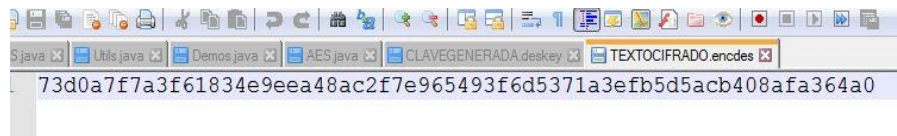
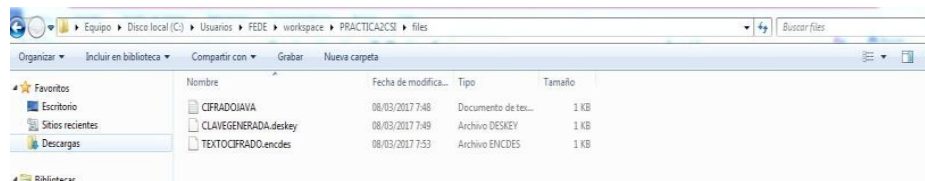
```
Problems @ Javadoc Declaration Console X
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 7:47:44)
Seleccione una opción y pulse ENTER:3
- TEXTOCIFRADO.encdes
Seleccione una archivo cifrado:TEXTOCIFRADO
- CLAVEGENERADA.deskey
Seleccione una clave:CLAVEGENERADA
```

COMPROBAMOS TODO



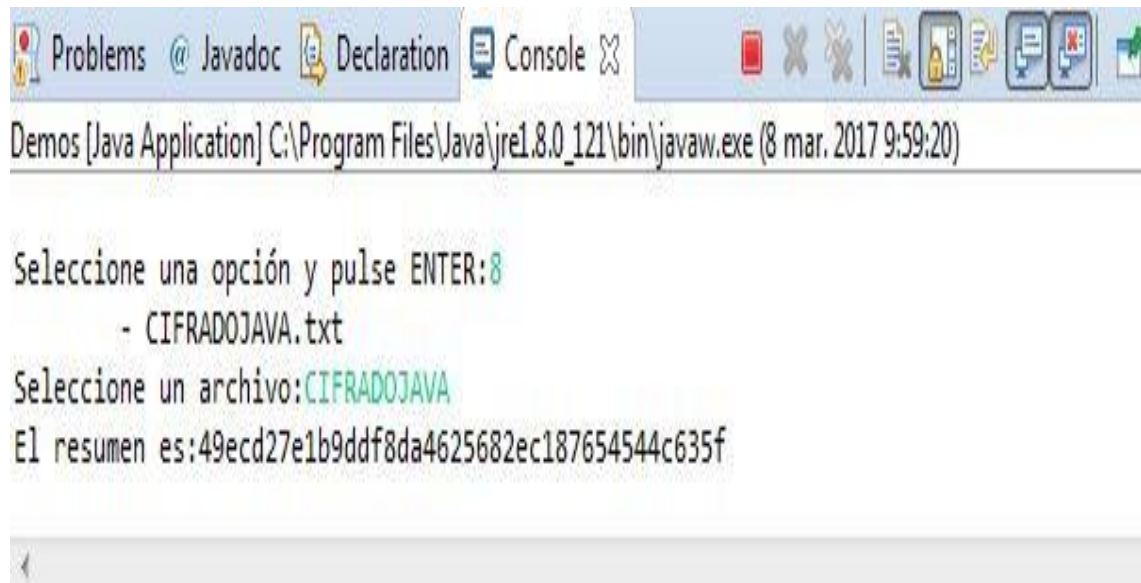
```
CIFRADOJAVA: Bloc de notas
Archivo Edición Formato Ver Ayuda
cifrado des, aes, rsa y hash
```

Y VEMOS TODOS LOS FICHEROS GENERADOS



5. Generar clave para algoritmo de cifrado AES (opción 4)
6. Cifrar archivo con AES (opción 5)
7. Descifrar archivo con AES (opción 6)
8. Generar resumen MD5 de un archivo (opción 7)
9. Generar resumen SHA1 de un archivo (opción 8)
10. Generar par de claves RSA (opción 9)
11. Cifrar archivo con RSA (opción 10)
12. Descifrar archivo con RSA (opción 11)








**AL FINAL DE LA EJECUCIÓN DE LAS OPCIONES 4 A LA 12
TENEMOS QUE TENER GENERADO LOS FICHEROS DE DES, AES,
MD5, SHA1 Y RSA SIGUIENTES:**



```
Problems @ Javadoc Declaration Console X
Demos [Java Application] C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe (8 mar. 2017 9:59:20)

Seleccione una opción y pulse ENTER:8
- CIFRADOJAVA.txt
Seleccione un archivo:CIFRADOJAVA
El resumen es:49ecd27e1b9ddf8da4625682ec187654544c635f
```

Compartir con ▾ Grabar Nueva carpeta

Nombre	Fecha de modifica...	Tipo	Tamaño
 CIFRADOJAVA	08/03/2017 7:48	Documento de tex...	1 KB
 CLAVEGENERADA.deskey	08/03/2017 7:49	Archivo DESKEY	1 KB
 clavegeneradaaes.aeskeyiv	08/03/2017 10:07	Archivo AESKEYIV	1 KB
 CLAVEGENERADAAES	08/03/2017 10:09	Archivo ENCAES	1 KB
 CLAVERSA1.priv	08/03/2017 10:17	Archivo PRIV	1 KB
 CLAVERSA1	08/03/2017 10:17	Documento de Mi...	1 KB
 TEXTOCIFRADO.encdes	08/03/2017 7:53	Archivo ENCDDES	1 KB