

EJERCICIO: 4.4. Firma digital de ficheros JAR e instalador:

AppHotel



4.4.1. Artículo acerca del algoritmo de cifrado MD5


Cada miembro del equipo leerá el artículo

<https://www.redeszone.net/2017/01/20/oracle-bloqueara-todos-los-jar-firmados-md5-partir-abril/> y comentará lo más relevante de la noticia. **Definición de Hecho:** Cada alumno habrá documentado los comentarios acerca de la noticia de Oracle.

El artículo habla sobre las medidas que ha tomado Oracle con firma de seguridad MD5, pues tiene al menos 2 vulnerabilidades conocidas y fácilmente comprobables mediante el comando:

```
jarsigner -verify -J-Djava.security.debug=jar test.jar
```

(Se necesita tener instalado el JDK)



```
C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI>
keytool -genkey -alias AlejandroLopez -keystore almacen -validity 150 -v
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  Alejandro Lopez
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  IES LosMontecillos
¿Cuál es el nombre de su organización?
  [Unknown]:  IES LosMontecillos
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  Coin
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  Malaga
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  ES
¿Es correcto CN=Alejandro Lopez, OU=IES LosMontecillos, O=IES LosMontecil
los, L=Coin, ST=Malaga, C=ES?
  [no]:  si

Generando par de claves DSA de 2.048 bits para certificado autofirmado (SHA
256withDSA) con una validez de 150 días
    para: CN=Alejandro Lopez, OU=IES LosMontecillos, O=IES LosMontecil
los, L=Coin, ST=Malaga, C=ES
Introduzca la contraseña de clave para <AlejandroLopez>
    (INTRO sí es la misma contraseña que la del almacén de claves):
[Almacenando almacen]

Warning:
El almacén de claves JKS utiliza un formato propietario. Se recomienda mig
rar a PKCS12, que es un formato estándar del sector que utiliza "keytool -
importkeystore -srckeystore almacen -destkeystore almacen -deststoretype p
kcs12".

C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI>
```

La contraseña es: contraseña

COMPROBACIÓN DE FIRMA DEL .jar -> DI_T2_AppHotel.jar

```
C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI\Hotel_BD_Cam
biada_FIRMADO\di-t2-apphotel-ermine-Actualizaci-n_desde_proyectoFinal_conWebView\dist>
jarsigner -verify -J-Djava.security.debug=jar DI_T2_AppHotel.jar
jar: beginEntry META-INF/MANIFEST.MF
jar: beginEntry META-INF/ORACLE_J.SF
jar: processEntry: processing block
jar: beginEntry META-INF/ORACLE_J.RSA
jar: processEntry: processing block
jar: Signature Block Certificate: [
[
  Version: V3
  Subject: CN=Oracle Corporation, OU=Java Software Code Signing, O=Sun Microsystems In
c
  Signature Algorithm: SHA1withDSA, OID = 1.2.840.10040.4.3

  Key:  Sun RSA public key, 1024 bits
  modulus: 126736735906127446617017451530770884230135396576195157301080131807546968289
68990562568385879224978158473505814282156579160465306400044345603620997556430080662149
76843292537619832247673117554767101328567384698655873532272434569236988556340455408589
94241905046383116198587381639648842391478764958448225910184331
```

...

```
jar:
jar: beginEntry sun/security/ec/ECPublicKeyImpl.class
jar: Manifest Entry: sun/security/ec/ECPublicKeyImpl.class digest=SHA1
jar:   manifest b4395fb40a7dfc7132ddf899ff1532b99990191e
jar:   computed b4395fb40a7dfc7132ddf899ff1532b99990191e
jar:
jar is unsigned.

C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI\Hotel_BD_Cam
biada_FIRMADO\di-t2-apphotel-ermine-Actualizaci-n_desde_proyectoFinal_conWebView\dist>
```

4.4.2. Distribución aplicación AppHotel

Cada alumno desde NetBeans revisará la aplicación AppHotel de su equipo en última versión y una vez construido el jar se accederá al directorio dist y analizará su contenido:

Verificando que se han incluido todos los recursos de la aplicación, todas las librerías y que el archivo manifest contiene la entradas: Main-Class: paquete.MainClass y Class-Path: lib/Librerias.jar, etc.

```
Directorio de C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI\Hotel_BD_Cambiada_FIRMADO\di-t2-apphotel-ermin-Actualizaci-n_desde_proyectoFinal_conWebView\dist

24/02/2020 17:49 <DIR> .
24/02/2020 17:49 <DIR> ..
24/02/2020 17:48      11.583 DI_T2_AppHotel.html
24/02/2020 17:48    1.971.234 DI_T2_AppHotel.jar
24/02/2020 17:48      3.866 DI_T2_AppHotel.jnlp
24/02/2020 17:49 <DIR> lib
24/02/2020 17:48 <DIR> web-files
                3 archivos      1.986.683 bytes
                4 dirs  50.707.316.736 bytes libres

C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI\Hotel_BD_Cambiada_FIRMADO\di-t2-apphotel-ermin-Actualizaci-n_desde_proyectoFinal_conWebView\dist>
```

El programa DI_T2_AppHotel.jar se ejecuta correctamente con el comando:

Java -jar DI_T2_AppHotel.jar

✓ Firmará el jar de la aplicación sin certificación (autofirma). Revisa para ello el Anexo I del tema.

```
C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI>jarsigner -keystore almacen -signedjar AppHotelFirmada.jar C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI\Hotel_BD_Cambiada_FIRMADO\di-t2-apphotel-ermin-Actualizaci-n_desde_proyectoFinal_conWebView\dist\DI_T2_AppHotel.jar AlejandroLR -verbose

Enter Passphrase for keystore:
updating: META-INF/MANIFEST.MF
  adding: META-INF/ALEJANDR.SF
  adding: META-INF/ALEJANDR.DSA
  adding: di_t2_apphotel/
signing: di_t2_apphotel/Clientes.jasper
signing: di_t2_apphotel/FXMLHabitaciones.fxml
signing: di_t2_apphotel/FXMLHabitacionesController$1.class
signing: di_t2_apphotel/FXMLHabitacionesController.class

...

...

...

...
```

```

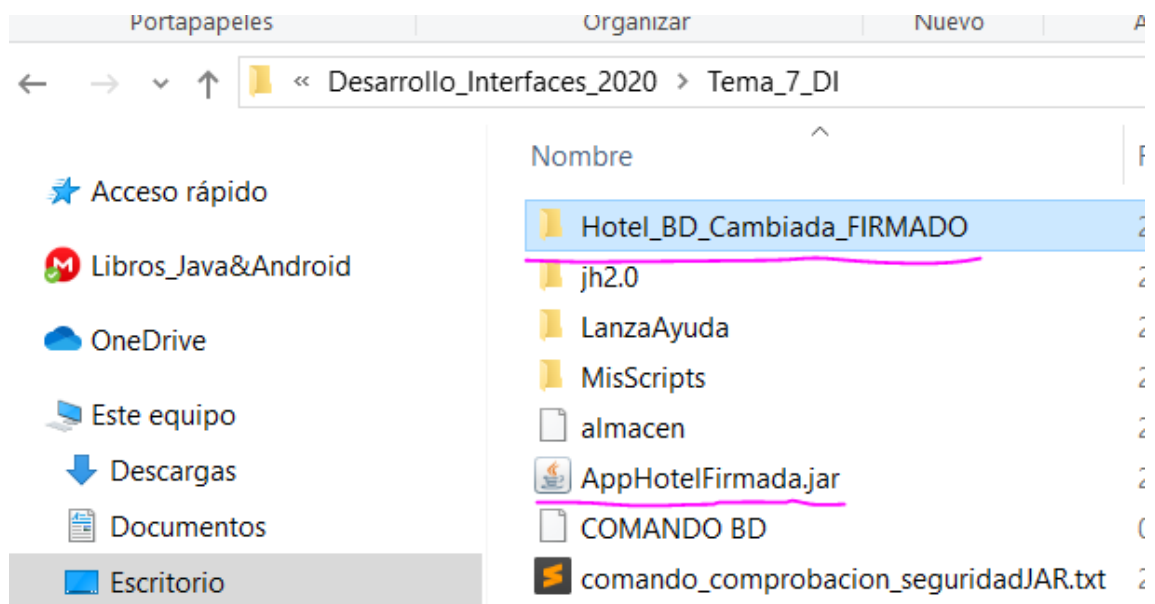
signing: webviewsample/images/reserva_Habitaciones.png
signing: webviewsample/images/reserva_Salon.png
adding: webviewsample/recursosWebview/
signing: webviewsample/recursosWebview/facebook.png
signing: webviewsample/recursosWebview/inicio.png
signing: webviewsample/recursosWebview/sobreapp.png
signing: webviewsample/recursosWebview/twitter.png
>>> Signer
      X.509, CN=AlejandroLR, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=ES
      [trusted certificate]

jar signed.

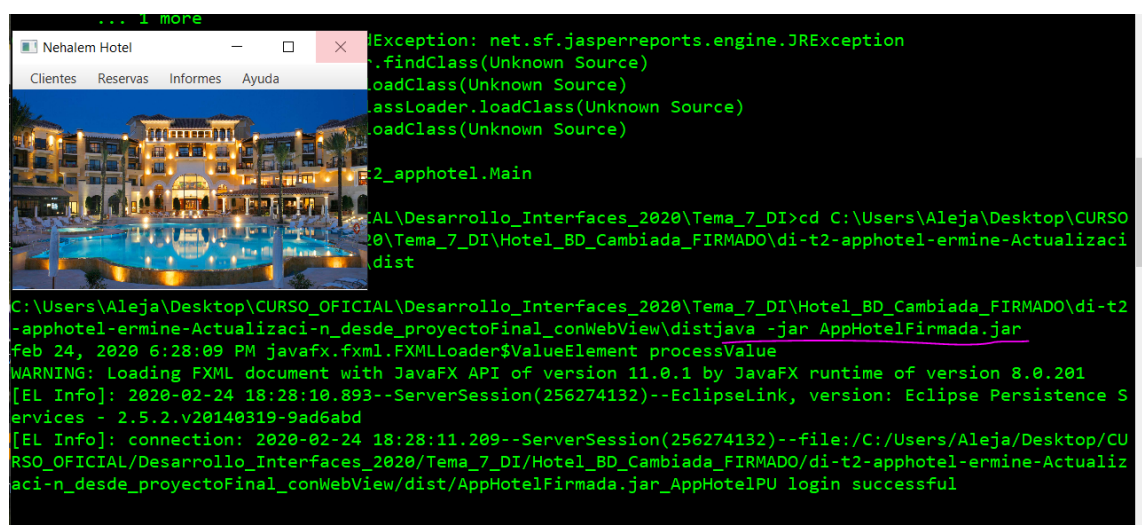
Warning:
The signer's certificate is self-signed.

C:\Users\Aleja\Desktop\CURSO_OFICIAL\Desarrollo_Interfaces_2020\Tema_7_DI>

```

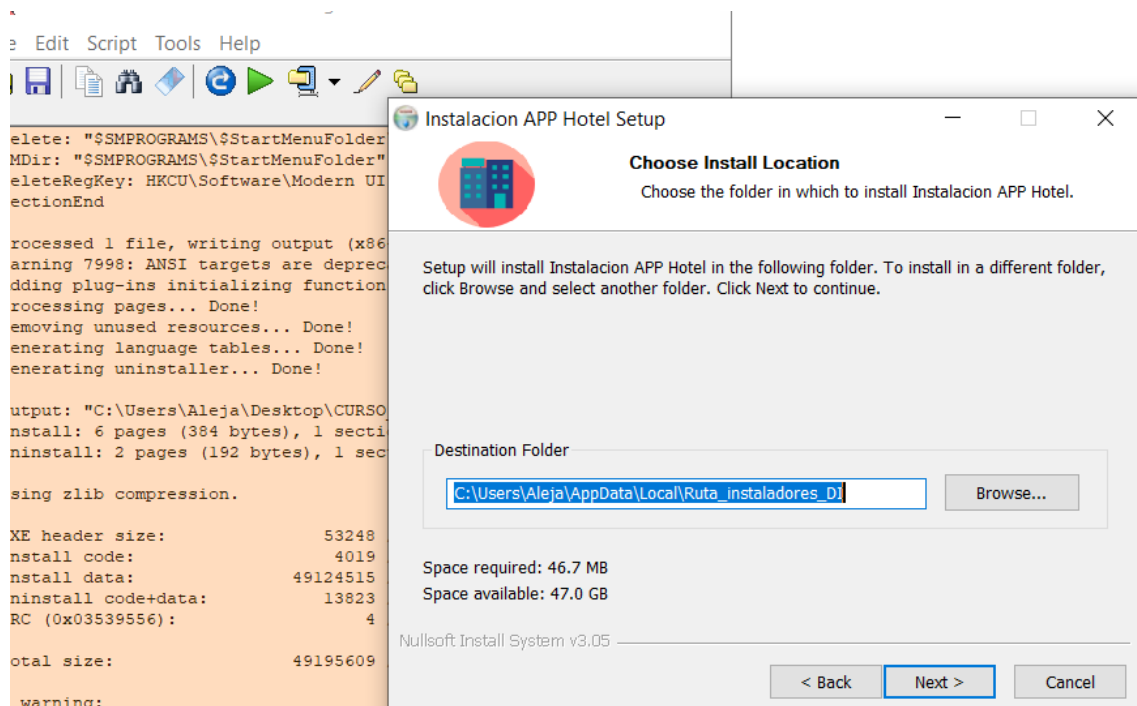
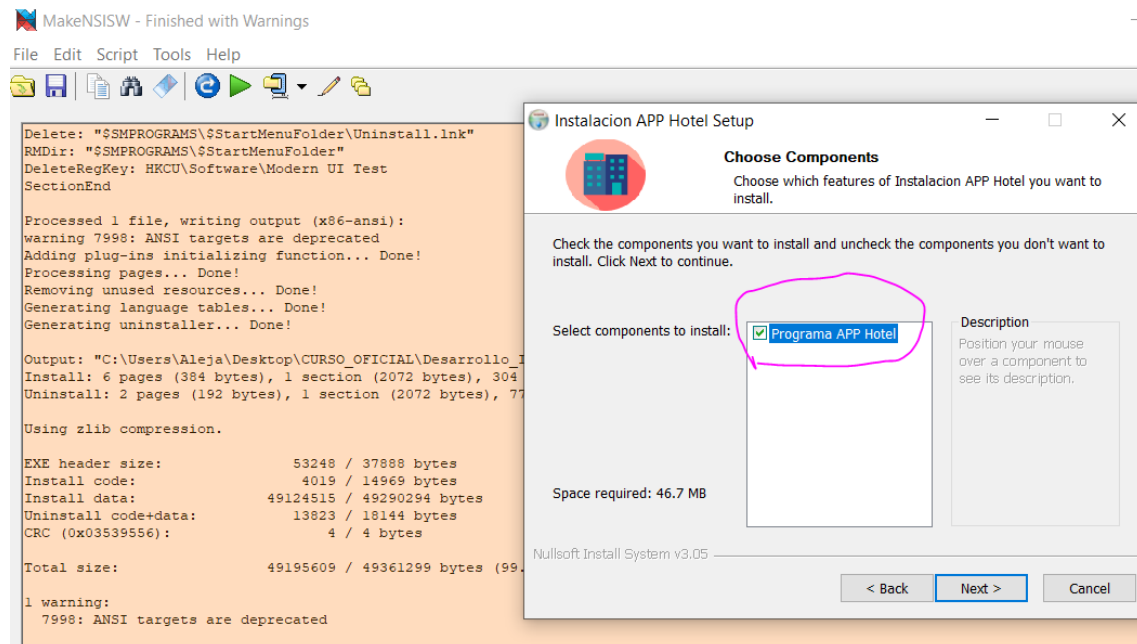


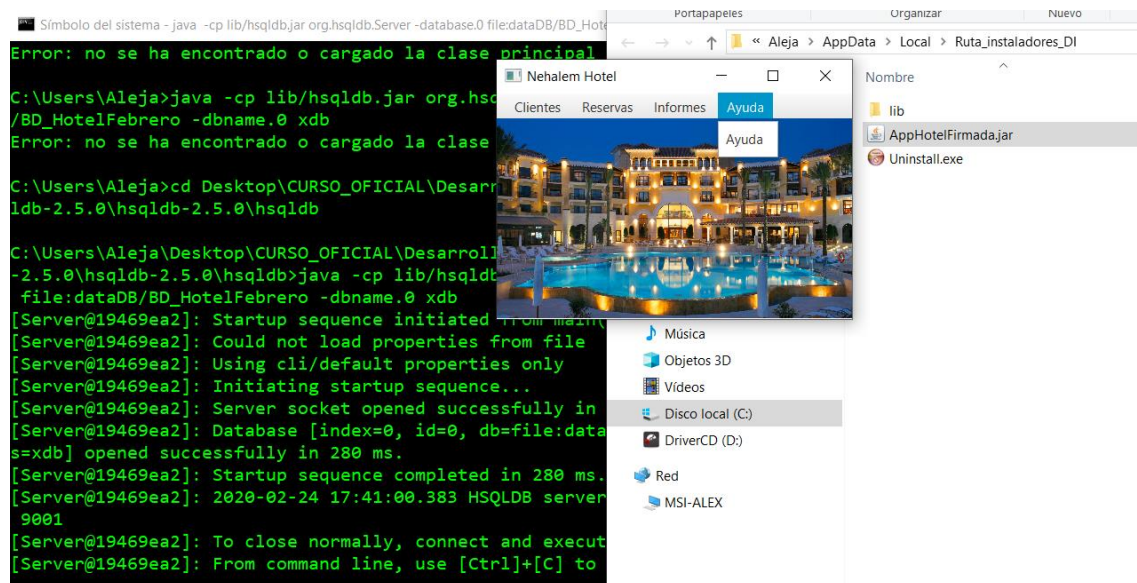
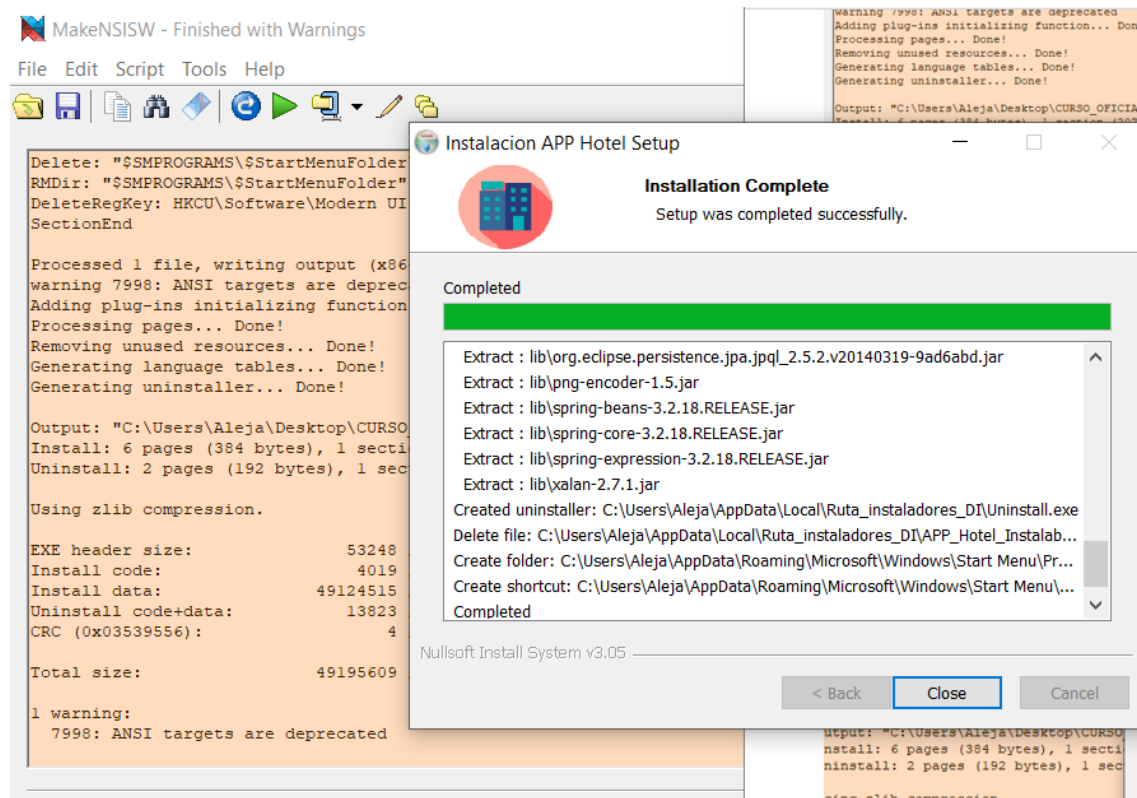
✓ Ejecutando y comprobando que la aplicación se ejecuta fuera de NetBeans.



✓ Creando un instalable con NSIS para instalar y ejecutar la aplicación en Windows.

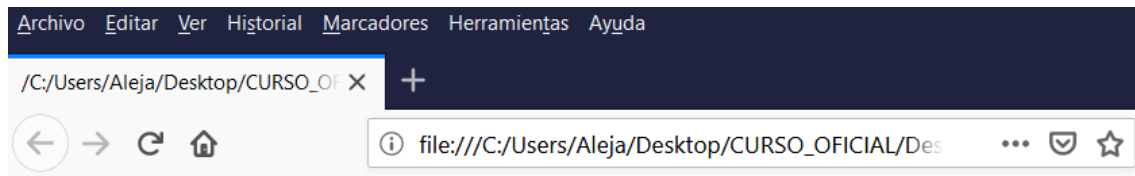
- ✓ Comprobando la instalación y correcta ejecución de la aplicación en Windows.





4.4.3. Distribución aplicación AppHotel (JavaWebStart)

Definición de Hecho: Cada alumno habrá revisado y actualizado los html y jnlp y habrá probado su funcionamiento.



URSO_OFICIAL > Desarrollo_Interfaces_2020 > Tema_7_DI > Hotel_BD_Cambiada_FIRMADO > di-t2-apphotel-err			
Nombre	Fecha de modifica...	Tipo	Tamaño
lib	24/02/2020 17:49	Carpeta de archivos	
web-files	24/02/2020 17:48	Carpeta de archivos	
AppHotelFirmada.jar	24/02/2020 18:24	Executable Jar File	1.933 KB
DI_T2_AppHotel.html	24/02/2020 17:48	Firefox HTML Doc...	12 KB
DI_T2_AppHotel.jar	24/02/2020 17:48	Executable Jar File	1.926 KB
DI_T2_AppHotel.jnlp	24/02/2020 17:48	JNLP File	4 KB

RESPONDES:

RESPONDE 1. ¿Qué paso se realiza en la instalación de un programa?:

a) **Creación de directorios requeridos.**

b) Verificación de la compatibilidad.

c) Compilar el programa.

d) Todas las anteriores

RESPONDE 2. ¿Qué herramienta **no** crea programas de instalación?:

a) IzPack.

b) NSIS.

c) InstallShield.

d) **Synaptic.**

RESPONDE 3. ¿Qué tipo de archivo es el que se utiliza en Ubuntu para distribuir aplicaciones?:

a) Ficheros ejecutables de extensión exe.

b) Fichero ejecutable jar.

c) Script ejecutables sh.

d) **Paquetes deb.**

RESPONDE 4. Para crear un instalador personalizado en Windows deberemos:

a) Crear un paquete de instalación deb.

b) Crear un paquete ejecutable jar.

c) Utilizar algún software específico como NSIS.

RESPONDE 5. Los ficheros JAR:

a) Son paquetes ejecutables que contienen clases Java y otros recursos.

b) Son ficheros con código fuente Java.

c) Son ficheros que deben compilarse para poder ser ejecutados.

RESPONDE 6. En una instalación desatendida:

a) El usuario decide la carpeta de instalación de la aplicación y todas las opciones de instalación.

b) El instalador interactúa continuamente con el usuario final.

c) La aplicación se instala de forma transparente al usuario.

RESPONDE 7. El reconocimiento de la firma digital de una archivo JAR se conoce como:

a) Clave privada.

b) Verificación.

c) Clave pública.

d) Certificación.

RESPONDE 8. En una instalación desde un servidor web:

a) El usuario siempre instala directamente la aplicación sin tener que guardarla antes.

b) La instalación siempre sigue el mismo procedimiento, independientemente del tipo de fichero a descargar.

c) La aplicación se instala automáticamente sólo si se trata de un archivo ejecutable.