

Practica 5: Mensajería de última milla II

Parte 3: Aplicar funcionalidad SSL

- 1. A continuación, se muestra la creación del certificado de seguridad para la practica 5

```
C:\WINDOWS\system32>cd C:\Program Files\Java\jdk1.8.0_161\bin

C:\Program Files\Java\jdk1.8.0_161\bin>keytool -genkey -alias practicefive -keyalg RSA -validity 365 -keystore practicefive -
keypass 123456 -storepass 123456
What is your first and last name?
  [Unknown]:  Alvaro Suarez
What is the name of your organizational unit?
  [Unknown]:  axxa
What is the name of your organization?
  [Unknown]:  axxa
What is the name of your City or Locality?
  [Unknown]:  Madrid
What is the name of your State or Province?
  [Unknown]:  Madrid
What is the two-letter country code for this unit?
  [Unknown]:  ES
Is CN=Alvaro Suarez, OU=axxa, O=axxa, L=Madrid, ST=Madrid, C=ES correct?
  [no]:  yes

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool
l -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_161\bin>keytool -list -v -keystore practicefive
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: practicefive
Creation date: 29-nov-2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Alvaro Suarez, OU=axxa, O=axxa, L=Madrid, ST=Madrid, C=ES
Issuer: CN=Alvaro Suarez, OU=axxa, O=axxa, L=Madrid, ST=Madrid, C=ES
Serial number: 2886f6e5
Valid from: Fri Nov 29 14:23:23 CET 2019 until: Sat Nov 28 14:23:23 CET 2020
Certificate fingerprints:
    MD5:  62:EC:58:86:F9:60:EF:94:E1:1D:BB:B1:F1:B2:6C:43
    SHA1: 73:F5:12:CD:4B:75:63:22:1B:A1:30:4A:3F:DC:5C:B5:D6:AE:61:5B
    SHA256: 1B:1C:9E:DD:6D:BD:B7:7D:6F:CA:35:AD:E5:ED:6B:06:8A:03:3C:F6:CF:E0:A6:2D:E0:50:BC:E9:39:CD:27:8E
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 35 4B FB 64 1F 20 E0 5E    6A 4B A5 28 8D 3D 5C DB    5K.d. .^jK.(.=\.
0010: D1 E4 BC B9                ....
]
]

*****
*****

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool
l -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_161\bin>keytool -list -v -keystore practicefive
```

```
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: practicefive
Creation date: 29-nov-2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Alvaro Suarez, OU=axxa, O=axxa, L=Madrid, ST=Madrid, C=ES
Issuer: CN=Alvaro Suarez, OU=axxa, O=axxa, L=Madrid, ST=Madrid, C=ES
Serial number: 2886f6e5
Valid from: Fri Nov 29 14:23:23 CET 2019 until: Sat Nov 28 14:23:23 CET 2020
Certificate fingerprints:
    MD5: 62:EC:58:86:F9:60:EF:94:E1:1D:BB:B1:F1:B2:6C:43
    SHA1: 73:F5:12:CD:4B:75:63:22:1B:A1:30:4A:3F:DC:5C:B5:D6:AE:61:5B
    SHA256: 1B:1C:9E:DD:6D:BD:B7:7D:6F:CA:35:AD:E5:ED:6B:06:8A:03:3C:F6:CF:E0:A6:2D:E0:50:BC:E9:39:CD:27:8E
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 35 4B FB 64 1F 20 E0 5E    6A 4B A5 28 8D 3D 5C DB    5K.d. .^jK.(.=\.
0010: D1 E4 BC B9                ....
]
]

*****
*****







Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_161\bin>keytool -export -alias practicefive -keystore practicefive -rfc -file Certpracticefive.cer
Enter keystore password:
Certificate stored in file <Certpracticefive.cer>

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_161\bin>
```

Y el certificado esta creado en el path de keytool


	AlmacenSR	29/11/2019 13:59	File	3 KB
	appletviewer.exe	01/02/2018 12:48	Application	16 KB
	Certpracticefive.cer	29/11/2019 14:28	Security Certificate	2 KB
	CertSRAutofirma.cer	29/11/2019 14:01	Security Certificate	2 KB
	extcheck.exe	01/02/2018 12:48	Application	17 KB
	idli.exe	01/02/2018 12:48	Application	17 KB

2. Certificado instalado en la aplicación

Error de privacidad

No seguro | localhost:8090

AplicacionesDriveGoogle TravelCalendarAll study program...GASTOS ÁLVARO E...PersonalMis UEducativoPDF ToolsmadridDeportesJuegosServicio de Informá...adAS PWD - Aplica...Drivers | GeForce



La conexión no es privada

Es posible que algunos atacantes intenten robar tu información de **localhost** (p. ej., contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Para ayudar a mejorar la seguridad de Chrome, envía [las URL de algunas páginas que visitas](#), [información limitada sobre el sistema y determinado contenido de páginas](#) a Google. [Política de Privacidad](#)


Configuración avanzada

Volver a seguridad

```
5:03:35.621 [qtp248609774-21] DEBUG o.e.jetty.io.AbstractConnection - onClose HttpConnection@1b4bf459[DecryptedEndPoint@1b23f361{/0:0:0:0:0:0:1:62820<->8090,CLOSED,in,OSHUT,-,-,302
1/30000,HttpConnection)}->SelectChannelEndPoint@2ac3fd4b{/0:0:0:0:0:0:1:62820<->8090,CLOSED,ISHUT,OSHUT,-,-,29/30000,SslConnection){io=1/1,kio=-1,kro=-1}][p=HttpParser{s=CLOSE,0 of
1},g=HttpGenerator@1ff7a4aa{s=START},c=HttpChannelOverHttp@7f709104{r=1,c=false,a=IDLE,uri=null}][b=null]
5:03:35.622 [qtp248609774-27] DEBUG o.e.j.u.t.s.ExecuteProduceConsume - EPR Prod/org.eclipse.jetty.io.ManagedSelector$SelectorProducer@653905a7 produce enter
5:03:35.624 [qtp248609774-21] DEBUG o.e.jetty.io.AbstractConnection - onClose SslConnection@6474fee1{NEED_UNWRAP,eio=-1/-1,di=-1} -> HttpConnection@1b4bf459[DecryptedEndPoint@1b23f36
1{/0:0:0:0:0:0:1:62820<->8090,CLOSED,in,OSHUT,-,-,30204/30000,HttpConnection)}->SelectChannelEndPoint@2ac3fd4b{/0:0:0:0:0:0:1:62820<->8090,CLOSED,ISHUT,OSHUT,-,-,32/30000,SslConnec
tion){io=1/1,kio=-1,kro=-1}][p=HttpParser{s=CLOSE,0 of -1},g=HttpGenerator@1ff7a4aa{s=START},c=HttpChannelOverHttp@7f709104{r=1,c=false,a=IDLE,uri=null}][b=null]
5:03:35.624 [qtp248609774-27] DEBUG o.e.j.u.t.s.ExecuteProduceConsume - EPR Prod/org.eclipse.jetty.io.ManagedSelector$SelectorProducer@653905a7 producing
5:03:35.626 [qtp248609774-21] DEBUG o.eclipse.jetty.io.AbstractEndPoint - onClose SelectChannelEndPoint@2ac3fd4b{/0:0:0:0:0:0:1:62820<->8090,CLOSED,ISHUT,OSHUT,-,-,34/30000,SslConn
ection){io=1/1,kio=-1,kro=-1}
5:03:35.654 [qtp248609774-27] DEBUG org.eclipse.jetty.io.ManagedSelector - Selector loop waiting on select
5:03:35.655 [qtp248609774-21] DEBUG o.e.j.u.t.s.ExecuteProduceConsume - EPR Prod/org.eclipse.jetty.io.ManagedSelector$SelectorProducer@653905a7 ran org.eclipse.jetty.io.ManagedSelect
or$2@6a65dc89
5:03:35.657 [qtp248609774-21] DEBUG o.e.j.u.t.s.ExecuteProduceConsume - EPR Prod/org.eclipse.jetty.io.ManagedSelector$SelectorProducer@653905a7 produce exit
5:03:35.658 [qtp248609774-21] DEBUG o.e.j.util.thread.QueuedThreadPool - ran EPR Prod/org.eclipse.jetty.io.ManagedSelector$SelectorProducer@653905a7
5:03:35.961 [org.eclipse.jetty.server.session.HashSessionManager@6bf256faTimer] DEBUG org.eclipse.jetty.server.session - Scavenging sessions at 1575295415961
5:04:05.963 [org.eclipse.jetty.server.session.HashSessionManager@6bf256faTimer] DEBUG org.eclipse.jetty.server.session - Scavenging sessions at 1575295445963
```

Certificate

GeneralDetailsCertification Path

 **Certificate Information**

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: alvaro suarez


Issued by: alvaro suarez

Valid from 02/12/2019 **to** 01/12/2020

Install Certificate...

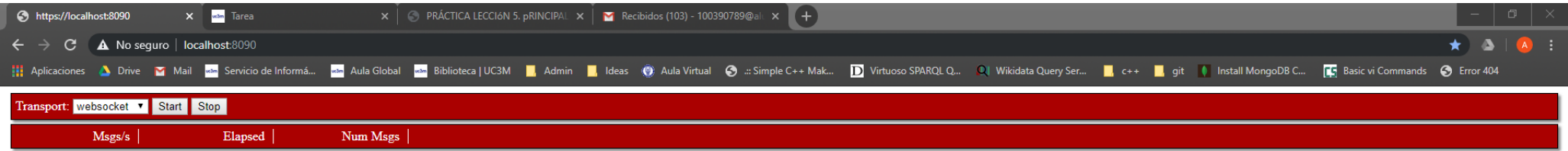
Issuer Statement

Certificate Import Wizard

 The import was successful.

OK

Después de importado el certificado el cliente abre sin problema en el navegador



3. Medición y comparación con tiempos en http

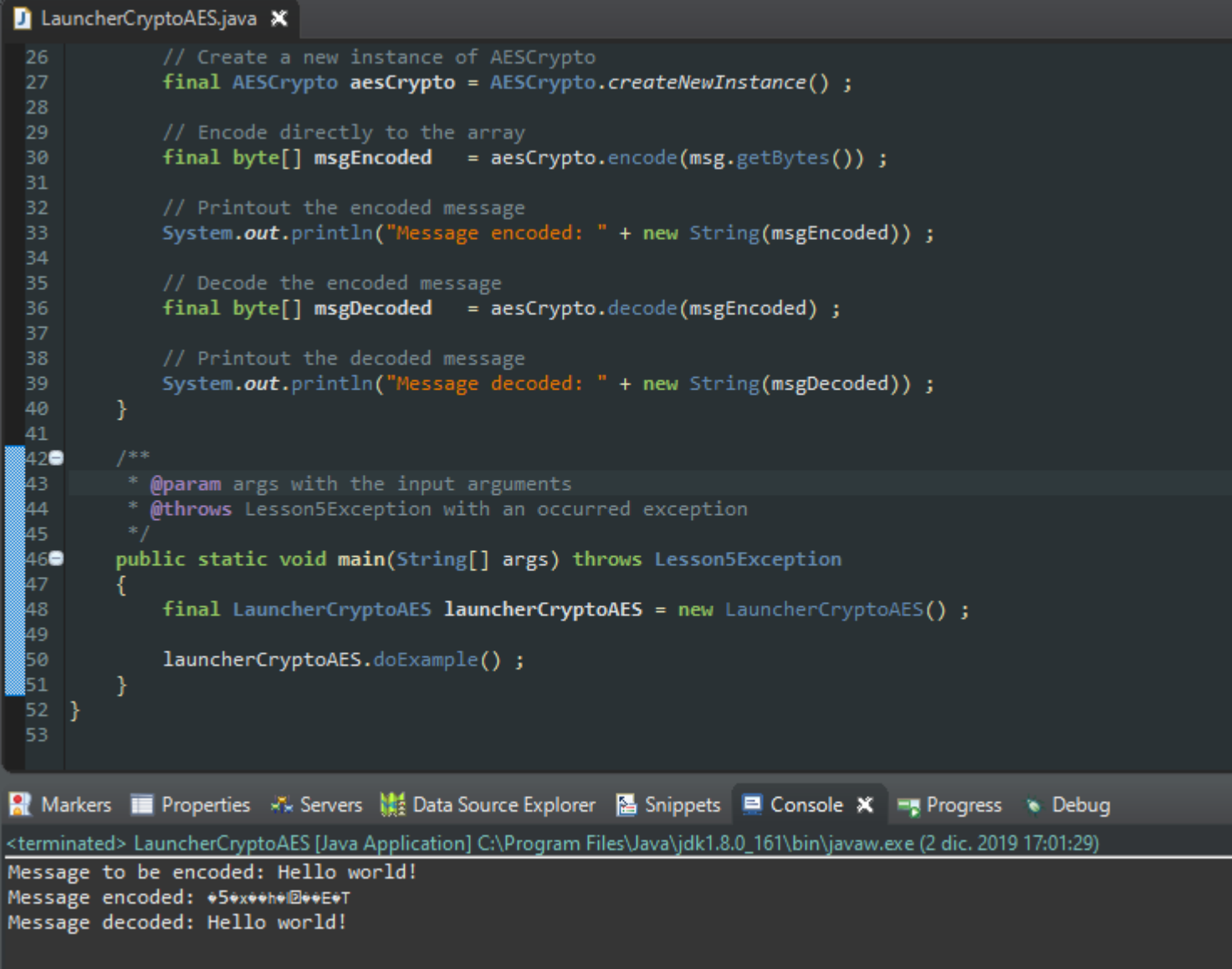
La siguiente es la medición tomada del cliente

SleepTime	Msg/s		Time	Msgs		Transport
	http	https		http	https	
0	130	67	10	1305	667	webSocket
0	18	6	10	176	64	long-polling
1	145	71	10	1447	714	webSocket
1	21	9	10	206	91	long-polling
10	90	72	10	901	723	webSocket
10	17	9	10	174	87	long-polling

Como conclusión el TRADE off de usar una comunicación segura es el rendimiento, tanto con websocket como con long-polling la relación en rendimiento es de 2:1, es decir, si con http puedo enviar dos mensajes, con https puedo enviar un mensaje.

Parte 4: Cifrado y Descifrado simétrico/asimétrico

En modo de cifrado simétrico se envía “Hello world!”:



En modo de cifrado asimétrico se envia “Hello world!”:

LauncherCryptoRSA.java

```
1 package com.cnebrera.uc3.tech.lesson5;
2
3 import com.cnebrera.uc3.tech.lesson5.util.Lesson5Exception;
4
5
6 /**
7  * Launcher class - Crypto - AES
8  * -----
9  * @author Francisco Manuel Benitez Chico
10  * -----
11  */
12 public class LauncherCryptoRSA
13 {
14     /**
15      * @throws Lesson5Exception with an occurred exception
16      *
17      */
18     private void doExample() throws Lesson5Exception
19     {
20         // Message to encode/decode
21         final String msg = "Hello world!" ;
22
23         // Printout the message
24         System.out.println("Message to be encoded: " + msg) ;
25
26         // Create a new instance of RSACrypto
27         final RSACrypto rsaCrypto = new RSACrypto() ;
28
29         final byte[] msgEncoded = rsaCrypto.encodeWithPubKey(msg.getBytes()) ;
30     }
31 }
```

Markers Properties Servers Data Source Explorer Snippets Console Progress Debug

terminated> LauncherCryptoRSA [Java Application] C:\Program Files\Java\jdk1.8.0_161\bin\javaw.exe (2 dic. 2019 17:13:56)

Message to be encoded: Hello world!

Message encoded: yp@#####6###Q####u##@k@b##3#####@S-##Bf. _[##:)*###>'0###@|@P#"##j##\b@o@q##x#_%@>##S+T/@@++]@d e#@q###P#

Message decoded: Hello world!