

A dark blue vertical bar is on the left. A blue arrow points right from it, containing the date.

1/6/2023

IS2109

Information Systems Security

Practical 03

Several thin, curved lines in dark blue and light grey originate from the bottom left and curve upwards and to the right.

Name: Gunaratne B.S.

INDEX NO: 20020422

Q1.

Code: `keytool -genkeypair -keystore keystore.jks -storetype JKS -keyalg RSA -keysize 2048 -validity 365 -alias mykey`

```
sachintha@sachintha-VirtualBox:~$ keytool -genkeypair -keystore keystore.jks -storetype JKS -keyalg RSA -keysize 2048 -validity 365 -alias mykey
Enter keystore password:
What is your first and last name?
[Unknown]: Sachintha Gunaratne
What is the name of your organizational unit?
[Unknown]: Information Systems
What is the name of your organization?
[Unknown]: UCSC
What is the name of your City or Locality?
[Unknown]: Kalutara
What is the name of your State or Province?
[Unknown]: Western Province
What is the two-letter country code for this unit?
[Unknown]: LK
Is CN=Sachintha Gunaratne, OU=Information Systems, O=UCSC, L=Kalutara, ST=Western Province, C=LK correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 365 days
for: CN=Sachintha Gunaratne, OU=Information Systems, O=UCSC, L=Kalutara, ST=Western Province, C=LK
Enter key password for <mykey>
(RETURN if same as keystore password):
```

Q2.

Code: `sudo nano /opt/tomcat/conf/server.xml`

```
GNU nano 6.2
    type="org.apache.catalina.UserDatabase"
    description="User database that can be updated and saved"
    factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
    pathname="conf/tomcat-users.xml" />
</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share
a single "Container" Note: A "Service" is not itself a "Container",
so you may not define subcomponents such as "Valves" at this level.
Documentation at /docs/config/service.html
-->
<Service name="Catalina">

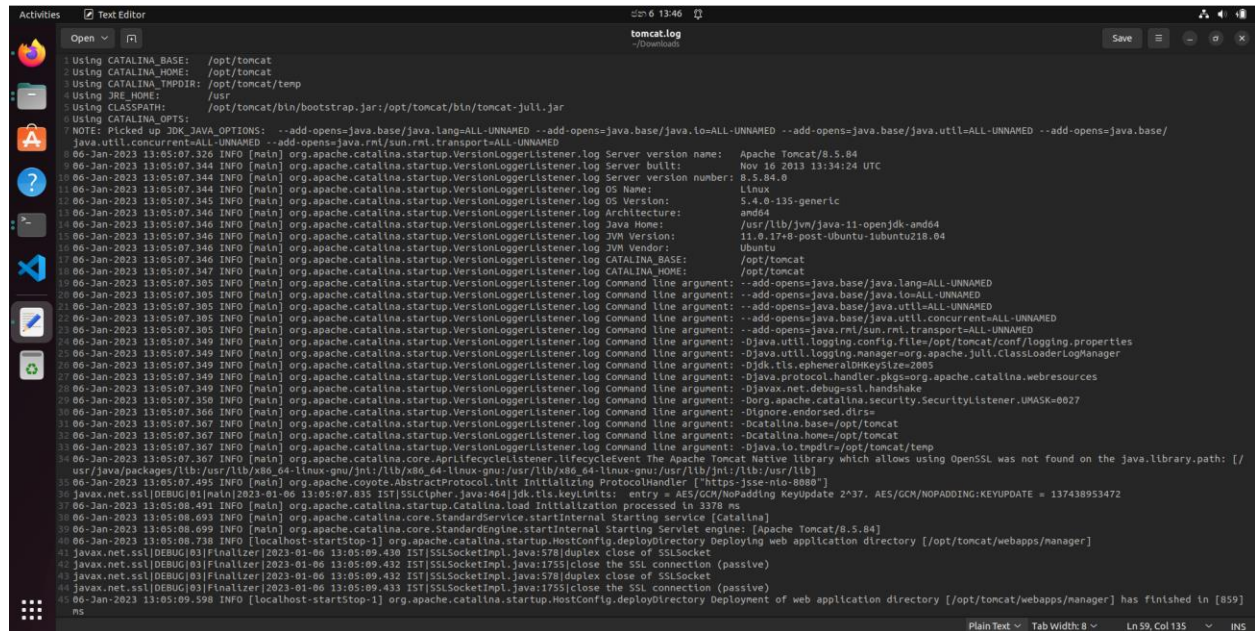
    <!--The connectors can use a shared executor, you can define one or more named thread
    <!--
    <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
        maxThreads="150" minSpareThreads="4"/>
    -->

    <!-- A "Connector" represents an endpoint by which requests are received
    and responses are returned. Documentation at :
    Java HTTP Connector: /docs/config/http.html
    Java AJP Connector: /docs/config/ajp.html
    APR (HTTP/AJP) Connector: /docs/apr.html
    Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443"
        SSLEnabled="true"
        sslProtocol="TLS"
        keystoreFile="/home/sachintha/keystore.jks"
        keystorePass="123456"
        keystoreType="JKS"
        keyAlias="mykey"
        clientAuth="false"
        scheme="https"
    />

    <!-- A "Connector" using the shared thread pool-->
    <!--
    <Connector executor="tomcatThreadPool"
        port="8080" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" />
```

Q3.

Code: `sudo sh /opt/tomcat/bin/catalina.sh run > tomcat.log 2>&1`



```
1 Using CATALINA_BASE:   /opt/tomcat
2 Using CATALINA_HOME:   /opt/tomcat
3 Using CATALINA_TMPDIR:  /opt/tomcat/temp
4 Using JRE_HOME:        /usr
5 Using CLASSPATH:        /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
6 Using CATALINA_OPTS:
7 NOTE: Picked up _JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
8 06-Jan-2023 13:05:07.326 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name:   Apache Tomcat/8.5.84
9 06-Jan-2023 13:05:07.344 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built:      Nov 16 2013 13:34:24 UTC
10 06-Jan-2023 13:05:07.344 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version number: 8.5.84.0
11 06-Jan-2023 13:05:07.344 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:          Linux
12 06-Jan-2023 13:05:07.345 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:       5.4.0-135-generic
13 06-Jan-2023 13:05:07.346 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:    amd64
14 06-Jan-2023 13:05:07.346 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:        /usr/lib/jvm/java-11-openjdk-amd64
15 06-Jan-2023 13:05:07.346 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:      11.0.17-b0-post-Ubuntu-1ubuntu218.04
16 06-Jan-2023 13:05:07.346 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:       Ubuntu
17 06-Jan-2023 13:05:07.347 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:    /opt/tomcat
18 06-Jan-2023 13:05:07.347 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:    /opt/tomcat
19 06-Jan-2023 13:05:07.305 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.lang=ALL-UNNAMED
20 06-Jan-2023 13:05:07.305 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.io=ALL-UNNAMED
21 06-Jan-2023 13:05:07.305 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.util=ALL-UNNAMED
22 06-Jan-2023 13:05:07.305 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.util.concurrent=ALL-UNNAMED
23 06-Jan-2023 13:05:07.305 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
24 06-Jan-2023 13:05:07.349 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties
25 06-Jan-2023 13:05:07.349 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
26 06-Jan-2023 13:05:07.349 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djdk.tls.ephemeralDHKeySize=2048
27 06-Jan-2023 13:05:07.349 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.protocol.handler.pkgs=org.apache.catalina.webresources
28 06-Jan-2023 13:05:07.349 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djavax.net.debug=ssl.handshake
29 06-Jan-2023 13:05:07.350 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dorg.apache.catalina.security.SecurityListener.UNASK=0027
30 06-Jan-2023 13:05:07.366 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dignore.endorsed.dirs=
31 06-Jan-2023 13:05:07.367 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=/opt/tomcat
32 06-Jan-2023 13:05:07.367 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=/opt/tomcat
33 06-Jan-2023 13:05:07.367 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=/opt/tomcat/temp
34 06-Jan-2023 13:05:07.367 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent The Apache Tomcat Native library which allows using OpenSSL was not found on the java.library.path: [/usr/java/packages/lib:/usr/lib/x86_64-linux-gnu:/usr/lib/x86_64-linux-gnu:/usr/lib/x86_64-linux-gnu:/usr/lib/jni:/usr/lib]
35 06-Jan-2023 13:05:07.405 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["https-jse-nio-8080"]
36 javax.net.ssl[DEBUG][main]2023-01-06 13:05:07.835 IST[SSLCipher: java:464]jdk.tls.keyInit: entry = AES/GCM/NoPadding KeyUpdate 2^37, AES/GCM/NoPadding KeyUpdate = 13743B953472
37 06-Jan-2023 13:05:08.491 INFO [main] org.apache.catalina.startup.Catalina.load Initialization processed in 3376 ms
38 06-Jan-2023 13:05:08.693 INFO [main] org.apache.catalina.core.StandardService.startInternal Starting service [Catalina]
39 06-Jan-2023 13:05:08.699 INFO [main] org.apache.catalina.core.StandardEngine.startInternal Starting Servlet engine: [Apache Tomcat/8.5.84]
40 06-Jan-2023 13:05:08.738 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [/opt/tomcat/webapps/manager]
41 javax.net.ssl[DEBUG][3]Finalizer:2023-01-06 13:05:09.430 IST[SSLSocketImpl: java:578]duplex close of SSLSocket
42 javax.net.ssl[DEBUG][3]Finalizer:2023-01-06 13:05:09.432 IST[SSLSocketImpl: java:1755]close the SSL connection (passive)
43 javax.net.ssl[DEBUG][3]Finalizer:2023-01-06 13:05:09.432 IST[SSLSocketImpl: java:578]duplex close of SSLSocket
44 javax.net.ssl[DEBUG][3]Finalizer:2023-01-06 13:05:09.433 IST[SSLSocketImpl: java:1755]close the SSL connection (passive)
45 06-Jan-2023 13:05:09.598 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [/opt/tomcat/webapps/manager] has finished in [859] ms
```