

**NAME:** S S JAYAKAR RAJU

**REGNO:** 21BCE5622

**SUBJECT:** Cryptography and network  
security

**FACULTY:** Balasaraswathi V R

**SLOT:** L49+L50

**EXP NO:** 8

# Secure Socket Layer Programming

## SERVER CODE:

```
import javax.net.ssl.SSLServerSocketFactory;
import javax.net.ssl.SSLServerSocket;
import javax.net.ssl.SSLSocket;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.io.PrintWriter;

public class SSL_server {
    public static void main(String[] args) {
        try {
            System.setProperty("javax.net.ssl.keyStore", "keystore.jks");
            System.setProperty("javax.net.ssl.keyStorePassword", "changeit");

            SSLServerSocketFactory ssf = (SSLServerSocketFactory)
SSLServerSocketFactory.getDefault();
            SSLServerSocket serverSocket = (SSLServerSocket)
ssf.createServerSocket(9999);

            System.out.println("SSL ServerSocket started");
            SSLSocket sslSocket = (SSLSocket) serverSocket.accept();
            System.out.println("Server socket accepted");

            PrintWriter out = new PrintWriter(sslSocket.getOutputStream(), true);
            BufferedReader in = new BufferedReader(new
InputStreamReader(sslSocket.getInputStream()));

            String line;
            while ((line = in.readLine()) != null) {
                System.out.println("Received: " + line);
                out.println("Echo: " + line);
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

## Client Code:

```
import javax.net.ssl.SSLSocketFactory;
import javax.net.ssl.SSLSocket;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.io.PrintWriter;

public class SSLClient {
    public static void main(String[] args) {
        try {
            System.setProperty("javax.net.ssl.trustStore", "truststore.jks");
            System.setProperty("javax.net.ssl.trustStorePassword", "changeit");

            SSLSocketFactory ssf = (SSLSocketFactory)
SSLSocketFactory.getDefault();
            SSLSocket sslSocket = (SSLSocket) ssf.createSocket("localhost",
9999);

            PrintWriter out = new PrintWriter(sslSocket.getOutputStream(), true);
            BufferedReader in = new BufferedReader(new
InputStreamReader(sslSocket.getInputStream()));

            out.println("Hello SSL Server");
            String line;
            while ((line = in.readLine()) != null) {
                System.out.println("Received: " + line);
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

## OUTPUTS:

```
PS C:\Users\91738\Desktop\VIT 6th SEM\Crptograpy\DES> keytool -genkey -alias serverkey -keyalg RSA -keystore keystore.jks -keypass changeit -storepass changeit -validity 360 -keyval
id 2048
What is your first and last name?
[Unknown]: Jayakar Raju
What is the name of your organizational unit?
[Unknown]: VIT
What is the name of your organization?
[Unknown]: VIT
What is the name of your city or locality?
[Unknown]: Chennai
What is the name of your State or Province?
[Unknown]: TN
What is the two-letter country code for this unit?
[Unknown]: IN
Is CN=Jayakar Raju, OU=VIT, O=VIT, C=IN correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 360 days
for: CN=Jayakar Raju, OU=VIT, O=VIT, C=IN
PS C:\Users\91738\Desktop\VIT 6th SEM\Crptograpy\DES> keytool -export -alias serverkey -keystore keystore.jks -file server.cer -storepass changeit
Certificate stored in file server.cer
PS C:\Users\91738\Desktop\VIT 6th SEM\Crptograpy\DES> keytool -import -alias serverCert -file server.cer -keystore truststore.jks -storepass changeit
Owner: CN=Jayakar Raju, OU=VIT, O=VIT, C=IN
Issued: CN=Jayakar Raju, OU=VIT, O=VIT, C=IN
Serial number: 6137678280b0d09
Valid from: Wed Apr 17 21:45:45 IST 2024 until: Sat Apr 12 21:45:45 IST 2025
(Certificate fingerprints)
SHA1: E7:F3:35:56:60:C6:F6:96:12:8D:5E:B5:1D:FA:02:B8:69:0C:C2:AC
```

```
Valid from: Wed Apr 17 21:45:45 IST 2024 until: Sat Apr 12 21:45:45 IST 2025
Certificate fingerprints:
    SHA1: E7:F3:35:56:60:C6:F6:96:12:8D:5E:B5:1D:FA:02:B8:69:0C:C2:AC
    SHA256: 12:9A:F4:B5:26:2C:CC:AA:76:0C:9D:53:53:92:94:9A:56:33:F9:94:31:5C:95:C8:FF:31:58:62:0B:1D:96:B7
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key

Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DD BE 06 F1 66 1E 45 67   9D B4 6B 1C 16 2B 2B 4B   ....f.Eg..h...+K
0010: 9E 40 C0 B2                ..@...
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
PS C:\Users\91738\Desktop\VIT 6th SEM\Crptograpy\DES> █
```

```
File Edit Selection View Run Terminal Help 100% SSLServer.java  
1 import java.net.ssl.SSLServerSocketFactory;  
2 import java.net.ssl.SSLServerSocket;  
3 import java.net.ssl.SSLSocket;  
4 import java.io.BufferedReader;  
5 import java.io.InputStreamReader;  
6 import java.io.PrintWriter;  
7  
8 public class SSLServer {  
9     public static void main(String[] args) {  
10         try {  
11             System.setProperty("javax.net.ssl.keyStore", "keystore.jks");  
12             System.setProperty("javax.net.ssl.keyStorePassword", "changeit");  
13  
14             SSLServerSocketFactory sscf = (SSLServerSocketFactory) SSLServerSocketFactory.getDefault();  
15             SSLServerSocket serverSocket = (SSLServerSocket) sscf.createServerSocket(9999);  
16  
17             System.out.println("SSL ServerSocket started");  
18             SSLSocket sslSocket = (SSLSocket) serverSocket.accept();  
19             System.out.println("server socket accepted");  
20  
21             PrintWriter out = new PrintWriter(sslSocket.getOutputStream(), autoFlush=true);  
22             BufferedReader in = new BufferedReader(new InputStreamReader(sslSocket.getInputStream()));  
23  
24             String line;  
25             while ((line = in.readLine()) != null) {  
26                 System.out.println("received: " + line);  
27                 out.println("echo: " + line);  
28             }  
29         } catch (Exception e) {  
30             e.printStackTrace();  
31         }  
32     }  
33 }  
34
```

```
File Edit Selection View Run Terminal Help 100% SSLClient.java  
1 import java.net.ssl.SSLSocketFactory;  
2 import java.net.ssl.SSLSocket;  
3 import java.io.BufferedReader;  
4 import java.io.InputStreamReader;  
5 import java.io.PrintWriter;  
6  
7 public class SSLClient {  
8     public static void main(String[] args) {  
9         try {  
10             System.setProperty("javax.net.ssl.trustStore", "truststore.jks");  
11             System.setProperty("javax.net.ssl.trustStorePassword", "changeit");  
12  
13             SSLSocketFactory sscf = (SSLSocketFactory) SSLSocketFactory.getDefault();  
14             SSLSocket sslSocket = (SSLSocket) sscf.createSocket("localhost", 9999);  
15  
16             PrintWriter out = new PrintWriter(sslSocket.getOutputStream(), autoFlush=true);  
17             BufferedReader in = new BufferedReader(new InputStreamReader(sslSocket.getInputStream()));  
18  
19             out.println("Hello SSL Server");  
20             String line;  
21             while ((line = in.readLine()) != null) {  
22                 System.out.println("received: " + line);  
23             }  
24         } catch (Exception e) {  
25             e.printStackTrace();  
26         }  
27     }  
28 }  
29
```

```
PS C:\Users\91736\Desktop\UIT_6th_Sem\Cryptography\DES> & "C:\Program Files\Java\jdk-10.0.1\bin\java.exe" "-XX:+ShowCodeDetailsInExceptionMessages" "-cp" "C:\Users\91736\AppData\Local\Temp\Code\UIT_6th_Sem\Cryptography\DES\src\main\java\redhat.java;jdt_ws\DES_1d19ic5\bin\" "SSL_server"
SSL ServerSocket started
```

```
PS C:\Users\91736\Desktop\UIT_6th_Sem\Cryptography\DES> & "C:\Program Files\Java\jdk-10.0.1\bin\java.exe" "-XX:+ShowCodeDetailsInExceptionMessages" "-cp" "C:\Users\91736\AppData\Local\Temp\Code\UIT_6th_Sem\Cryptography\DES\src\main\java\redhat.java;jdt_ws\DES_1d19ic5\bin\" "SSL_client"
Received: echo: Hello SSL server
```

```
PS C:\Users\91736\Desktop\UIT_6th_Sem\Cryptography\DES> & "C:\Program Files\Java\jdk-10.0.1\bin\java.exe" "-XX:+ShowCodeDetailsInExceptionMessages" "-cp" "C:\Users\91736\AppData\Local\Temp\Code\UIT_6th_Sem\Cryptography\DES\src\main\java\redhat.java;jdt_ws\DES_1d19ic5\bin\" "SSL_server"
SSL ServerSocket started
server socket accepted
Received: Hello SSL server
```