**Name: Shaikh Rumman Fardeen**

**Reg No: 21BCE1736**

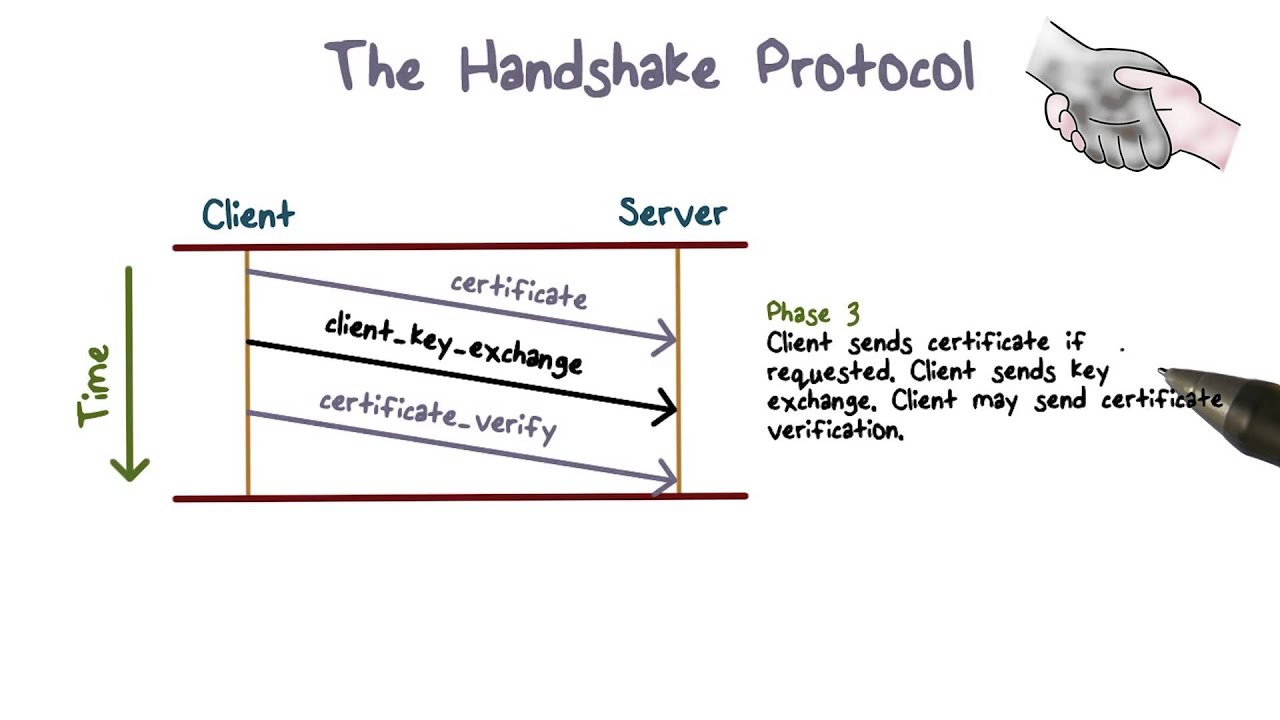
**BCSE309P Cryptography and Network Security Lab**

**Lab 8 : SSL Socket Code**

**Aim:**

Write socket program code to implement SSL using Socket Programming and Handshaking Protocol

**Certificate Creation:The Handshake Protocol**



*Generate a KeyStore*

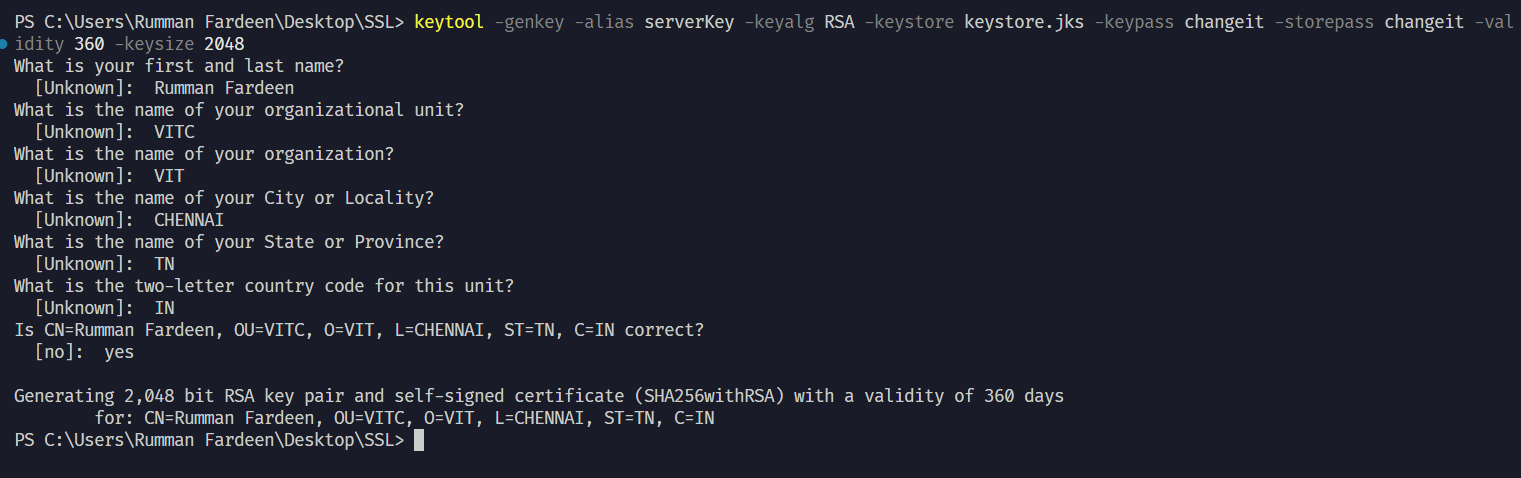
keytool -genkey -alias serverKey -keyalg RSA -keystore keystore.jks -keypass changeit -storepass changeit -validity 360 -keysize 2048

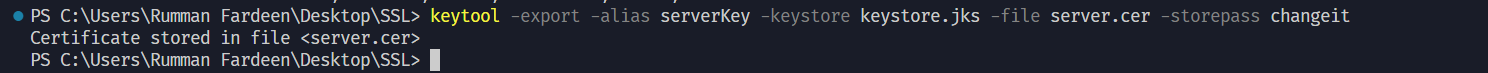
*Export the certificate from the KeyStore*

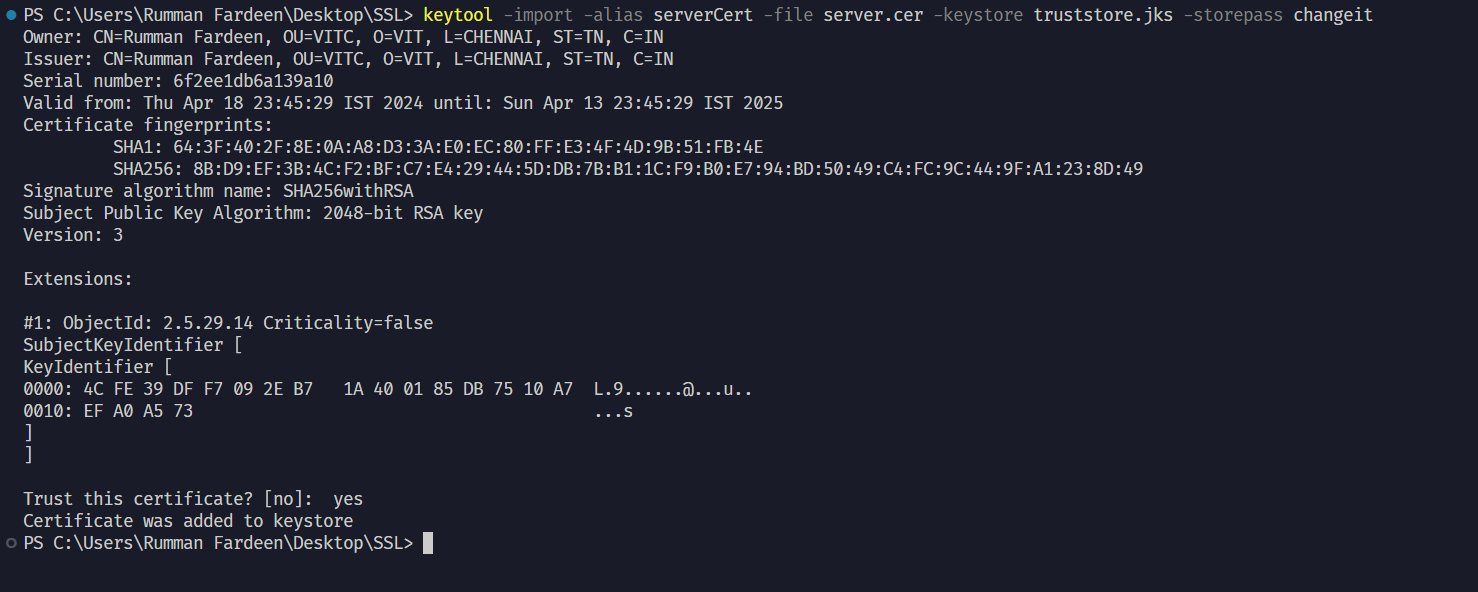
keytool -export -alias serverKey -keystore keystore.jks -file server.cer -storepass changeit

*Create a TrustStore and import the server certificate*

keytool -import -alias serverCert -file server.cer -keystore truststore.jks -storepass changeit

****

****

****

**Code:**

**SERVER CODE**

import java.io.BufferedReader;

import java.io.InputStreamReader;

import java.io.PrintWriter;

import javax.net.ssl.SSLServerSocket;

import javax.net.ssl.SSLServerSocketFactory;

import javax.net.ssl.SSLSocket;

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) {

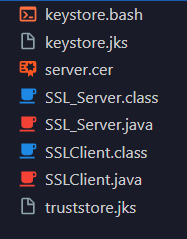
e.printStackTrace();

}

}

}

**Folder Structure:**

****

**Output:**

