

**UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA**

**MANUAL DE USUARIO – LABORATORIO 1
CRIPTOGRAFIA Y PROTOCOLOS DE SEGURIDAD**

Integrante: Matías Quinteros
Ayudante: Pedro Rojas
Profesora: Rosa Muñoz
Carrera: Ingeniería Civil Informática
Fecha: 7 de marzo del 2016
Periodo: Semestre II, 2015

ÍNDICE DE CONTENIDOS

1 PRESENTACIÓN	1
2 INSTALACIÓN	1
2.1 REQUISTOS.....	1
2.2 ARCHIVOS	1
2.3 INICIANDO EL PROGRAMA	2
3 UTILIZACIÓN	4
3.1 SERVIDOR	4
3.1.1 Vista Servidor	4
3.1.2 Administración de Usuarios.....	5
3.2 CLIENTE.....	6
3.3 EJECUTANDO EL PROTOCOLO NEEDHAM-SCHROEDER	8

1 PRESENTACIÓN

El presente documento corresponde a una guía para la utilización del programa creado para el primer laboratorio del ramo Criptografía y Protocolos de Seguridad de la Universidad de Santiago de Chile que tiene por objetivo simular el funcionamiento del protocolo de seguridad Needham – Schroeder en su versión de clave simétrica.

En esta guía se detalla las funcionalidades del programa creado utilizando el lenguaje de programación Java y SQL (mysql para las bases de datos), por lo que antes de iniciar su ejecución es necesario instalar algunos programas necesarios para la correcta ejecución de este programa y esto se detalla en la sección de instalación (sección 2).

La sección 3 indica cómo utilizar el programa luego de tener instalados todos los programas indicados en la sección 2, además en la sección de utilización se detalla cuáles son los pasos a seguir para que el programa creado ejecute de forma correcta el protocolo Needham – Schroeder.

Finalmente, la realización de esta guía es compatible con versiones de Windows 7/8 y 10.

2 INSTALACIÓN

2.1 REQUISITOS

Para la utilización del programa es necesario que se tengan instalados previamente los siguientes programas:

- JAVA SE 8u73/8u74
(<http://www.oracle.com/technetwork/articles/javase/index-jsp-138363.html>)
- Winrar(<https://www.winrar.es/descargas>)
- XAMPP (<https://www.apachefriends.org/es/index.html>)

Con respecto a XAMPP, es necesario que se instale el módulo de mysql y de Apache, además de tener por defecto la clave nombre de usuario por defecto para mysql, (usuario = root y pass = "").

2.2 ARCHIVOS

Luego de tener instalados los programas detallados en la sección anterior, es necesario descomprimir el archivo "*Quinteros_Lab.rar*" para acceder al programa.

Al descomprimir el archivo, se encuentra el directorio "*Codigo_Fuente*", el cual contiene el proyecto para Netbeans. Este directorio contiene los dos proyectos:

- LabNeedhamSchroeder_Protocol
- LabServidorJavaRMI

Además, la carpeta "*ejecutables*" contiene ya los archivos .jar para ser ejecutados y la carpeta "*base_de_datos*" contiene el archivo "*dataserver_rmi.sql*" correspondiente al archivo necesario para la base de datos.

Un punto importante es que la carpeta "*ejecutables*" también contiene los directorios "*images*" y "*lib*", los cuales no pueden ser modificados y son necesarios para la ejecución del programa.

2.3 INICIANDO EL PROGRAMA

Previo a iniciar el programa, es necesario que se inicie mysql, para ello inicie el programa XAMPP y en el panel de control inicie los módulos de mysql y Apache. En el módulo mysql presione “Admin” para iniciar phpmyadmin, esto se muestra en la Figura 2.1:

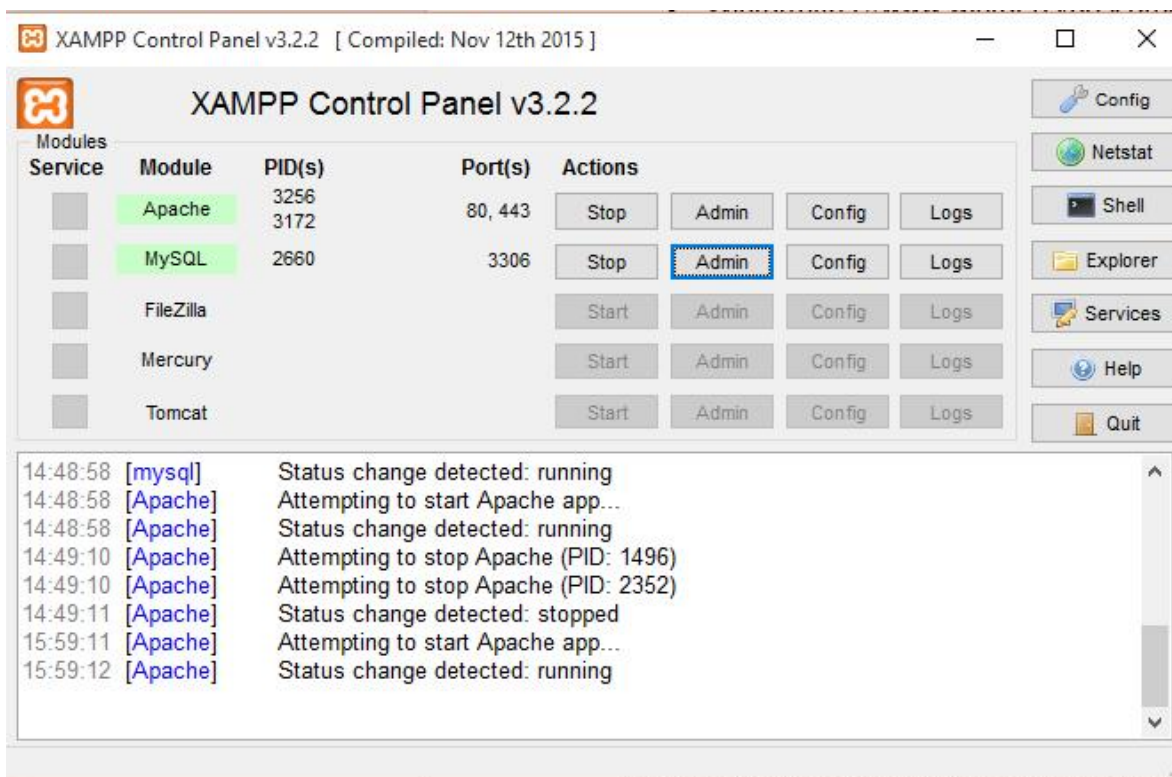


Figura 2.1: Panel de Control XAMPP

Ya iniciado phpMyadmin, presione en la barra lateral Nueva para crear una nueva base de datos y como nombre de la base de datos es necesario el nombre de “dataserver_rmi”, esto se detalla en la Figura 2.2:

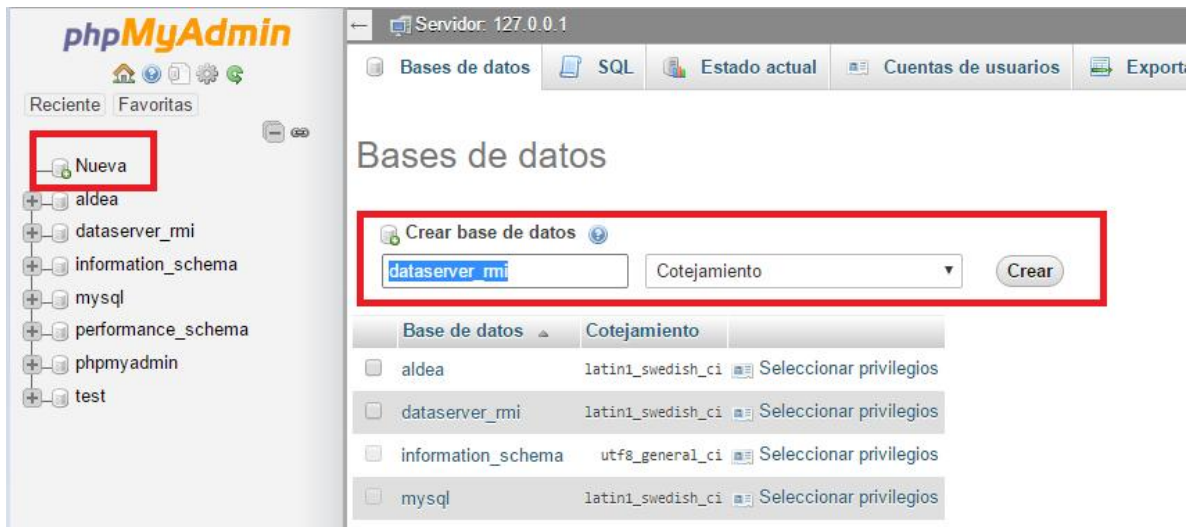


Figura 2.2: Creando la base de datos en PHPMYAdmin

Luego seleccione la base de datos “dataserver_rmi” y presione la pestaña importar para poder seleccionar el archivo “dataserver_rmi.sql” de la carpeta “base_de_datos”, realizado este paso, es posible iniciar el programa. Además, es importante mencionar que para cada uso del programa es necesario iniciar el módulo de mysql en XAMPP. La Figura 2.3 muestra lo explicado:



Figura 2.3: Creando la base de datos dataserver_rmi

3 UTILIZACIÓN

Como se mencionó en la sección 2, antes de utilizar el programa es necesario que el módulo de mysql este iniciado en el programa XAMPP. Considerando que se iniciaron estos pasos, para comenzar a utilizar el programa es necesario primero iniciar el programa: “ServidorJavaRMI.jar”. Los detalles del programa y su utilización se explican a continuación.

3.1 SERVIDOR

3.1.1 Vista Servidor

Para iniciar el servidor es necesario presionar el botón “Iniciar Servidor”, de este modo, otros clientes se podrán conectar al servidor. Además, en la sección Log del servidor se muestran todas las interacciones que tienen otros clientes con el servidor o si se realizó algún cambio en la base de datos, mostrando además el timestamp asociado a cuando ocurrió el evento. La Figura 3.1 muestra la vista servidor:

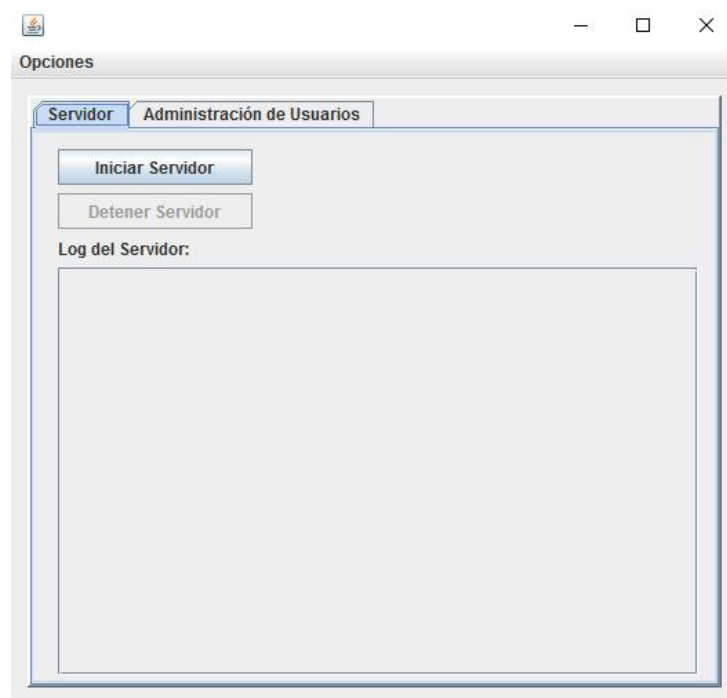


Figura 3.1: Vista Iniciar Servidor

También si se presiona el botón “Detener Servidor” luego de iniciarlo, cualquier cliente no podrá establecer algún tipo de comunicación.

3.1.2 Administración de Usuarios

La pestaña administración de usuarios permite crear y eliminar usuarios. Por defecto la base de datos contiene dos usuarios de prueba, pero si se quieren crear más usuarios, se deben llenar los campos de nombre de usuario y contraseña con un largo mínimo de 6 caracteres y presionar el botón guardar, además automáticamente la tabla “*ver usuarios*” se actualizará. La Figura 3.2 muestra la pestaña de Administración de Usuarios.

Opciones

Servidor Administración de Usuarios

Ingresar Usuario

Nombre de Usuario:

Contraseña:

Guardar

Ver Usuarios

Id	Nombre Usuario	Contraseña
32	matias	123456
33	laboratorio	987654

Seleccionar fila, luego click derecho para modificar/eliminar

Figura 3.2: Administración de usuarios

Si se quiere eliminar un usuario, entonces se debe pinchar sobre el usuario y luego se debe presionar el botón secundario del mouse. Luego de realizar esto aparecerá en pantalla un “pop up” pequeño que al presionarlo ejecutará la acción de eliminar un usuario de la base de datos. Esta acción se muestra en la Figura 3.3.

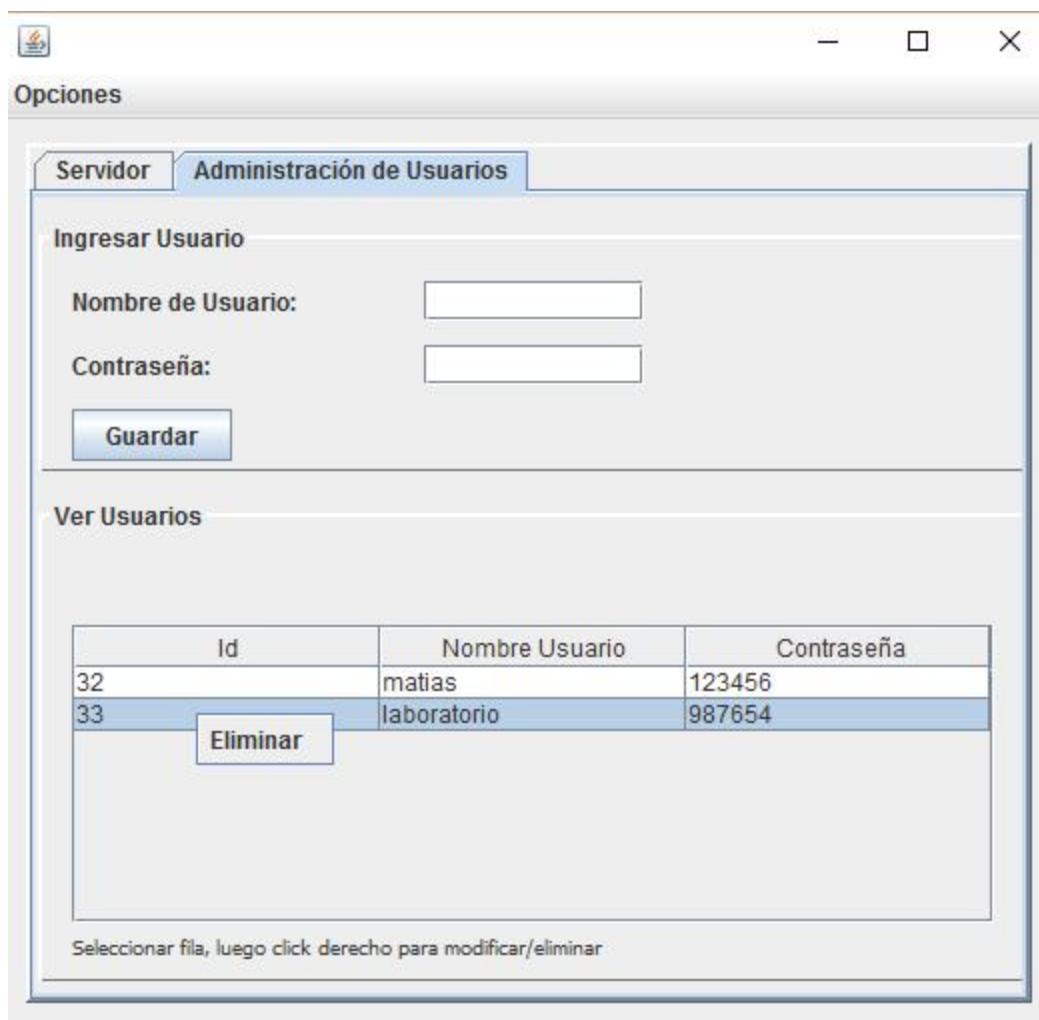


Figura 3.3: Eliminar usuario

3.2 CLIENTE

Al ejecutar el archivo: "NeedhamSchroeder_Protocol.jar" se ejecutará el programa para los usuarios. La figura 3.4 muestra la ventana principal al iniciar este programa.

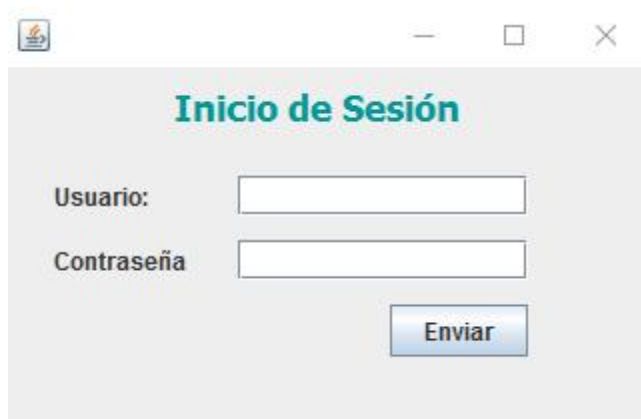


Figura 3.4: Inicio de Sesión

En esta ventana se deben ingresar un nombre de usuario y contraseña válido, el cual debe ser creado en el servidor. Al pulsar enviar, se le muestra al usuario la siguiente ventana para ejecutar el protocolo.




Figura 3.5: Ventana para el protocolo

Es válido mencionar que como pre requisitos es necesarios que, en la instancia del servidor, este se encuentre iniciado además de tener el módulo de mysql ejecutándose en XAMPP.

3.3 EJECUTANDO EL PROTOCOLO NEEDHAM-SCHROEDER

Para utilizar el programa y que este utilice de forma correcta el protocolo es necesario que primero se establezca el servidor de javaRMI, para ello es necesario seguir las indicaciones de la sección 3.1. Luego de iniciar el servidor es necesario que se ejecuten dos instancias del programa "NeedhamSchroeder_Protocol.jar". Además, como se ha mencionado anteriormente, es necesario que el módulo de mysql en XAMPP este iniciado.

Como modo de prueba, la base de datos contiene dos usuarios de prueba para efectuar el protocolo, estos usuarios y sus contraseñas son las siguientes:

- Usuario: matias, password: 123456
- Usuario: laboratorio, password: 987654

Con estos datos inicie sesión tal como muestra la Figura 3.6 muestra un ejemplo de estos datos ingresados correctamente:

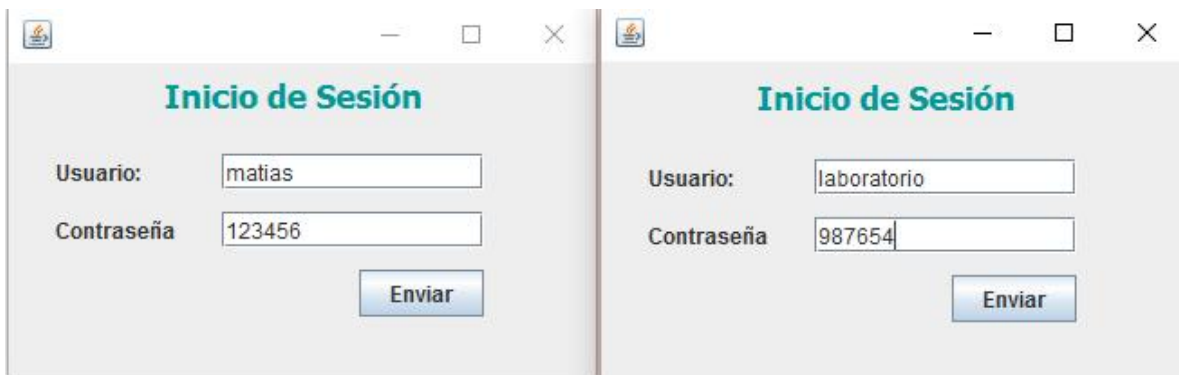


Figura 3.6: Inicio de sesión para los dos usuarios

El paso siguiente luego de iniciar sesión es ejecutar el protocolo. Si tuvo problemas para iniciar sesión, siga los pasos para crear nuevos usuarios desde el servidor en la sección 3.1.2 o bien, vea las contraseñas guardadas en el servidor. Para ejecutar el protocolo es necesario que en cualquiera de las dos instancias del programa para los usuarios, primero se seleccione con cuál de los usuarios conectados se quiere establecer la comunicación, para ello en la Figura 3.7 se muestra en que parte del programa se selecciona un usuario. Si no hay usuarios conectados, presione el botón "Refrescar lista".

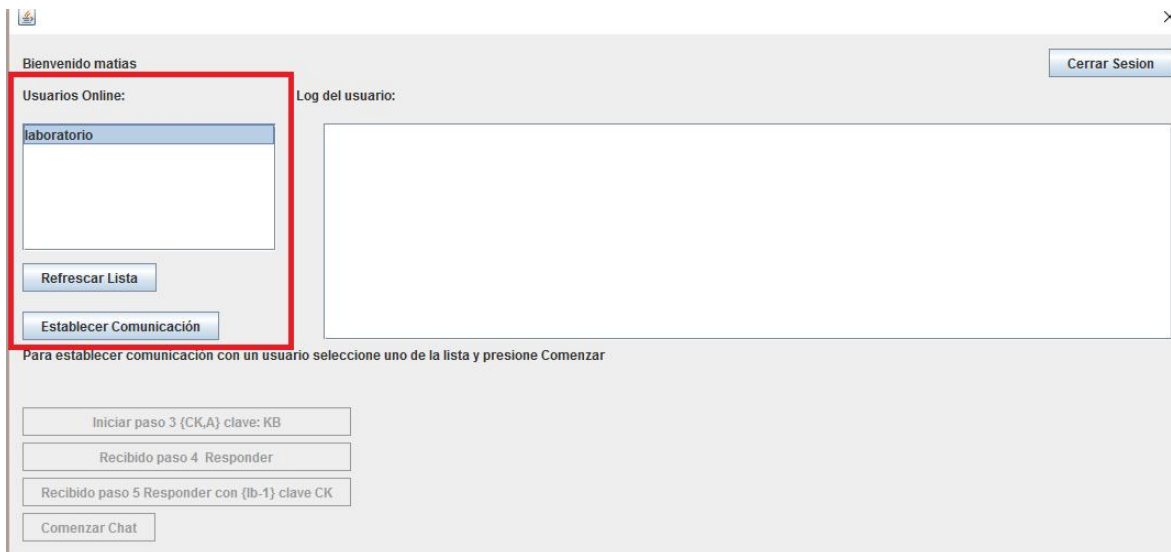


Figura 3.7: Usuarios conectados

Para esta guía, el usuario A será la instancia que inició sesión “matias” y el usuario B será la instancia que inició sesión “laboratorio”. Por lo que, con “A” presione el botón “Establecer comunicación” seleccionando dentro de la lista de usuarios conectados “laboratorio” (usuario B), tal como lo muestra la Figura 3.7. Con esta acción se iniciará el primer paso del protocolo, el paso 1 y 2, en donde ese usuario “A” le enviará al servidor la información y el servidor le responderá el mensaje encriptado con la clave del usuario “A”. Si se realizó este procedimiento correctamente, el programa debería mostrar lo que aparece en la Figura 3.8.

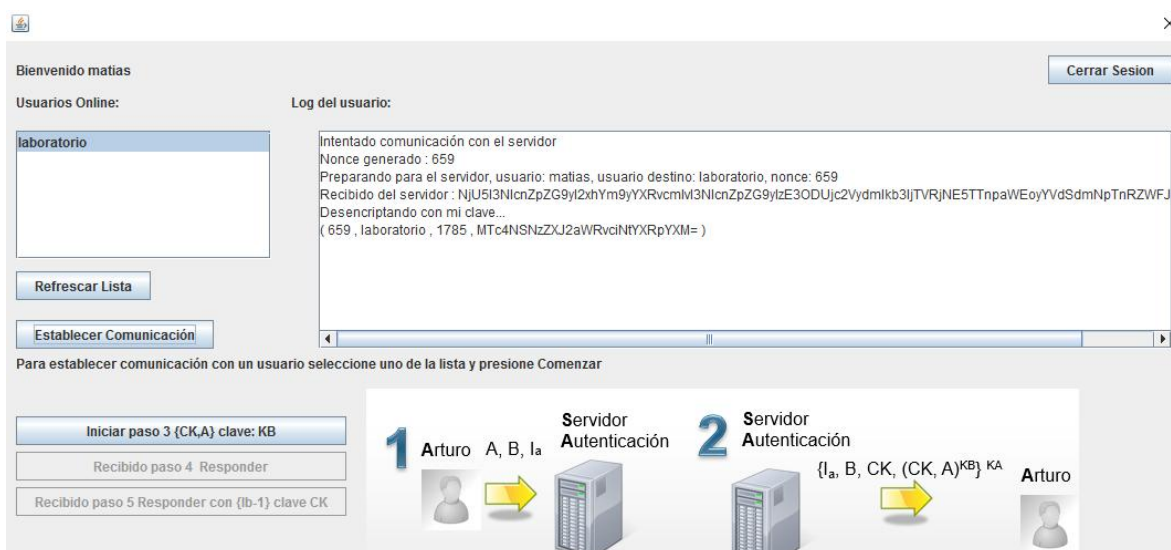


Figura 3.8: Iniciando pasos 1 y 2.

Tanto el servidor, como la instancia de “A” mostrarán en el log lo que sucedió, principalmente indicando el mensaje encriptado y los valores que se enviaron. Si el paso se realizó correctamente entonces en la misma instancia de “A” presione el botón Iniciar paso 3, el cual se desbloqueó luego de que se realizara correctamente el paso 1 y 2 del protocolo. La Figura 3.9 muestra el cambio en la instancia de “A” al presionar el botón mencionado. En este paso, el mensaje será enviado a la instancia “B” el cual recibe el mensaje y verifica si su contenido es correcto. La Figura 3.10 muestra el programa de la instancia “B” luego de recibir el mensaje del paso 3. Además, si se quiere más detalle de lo ocurrido, para todos los pasos se muestran los resultados en el Log del servidor.

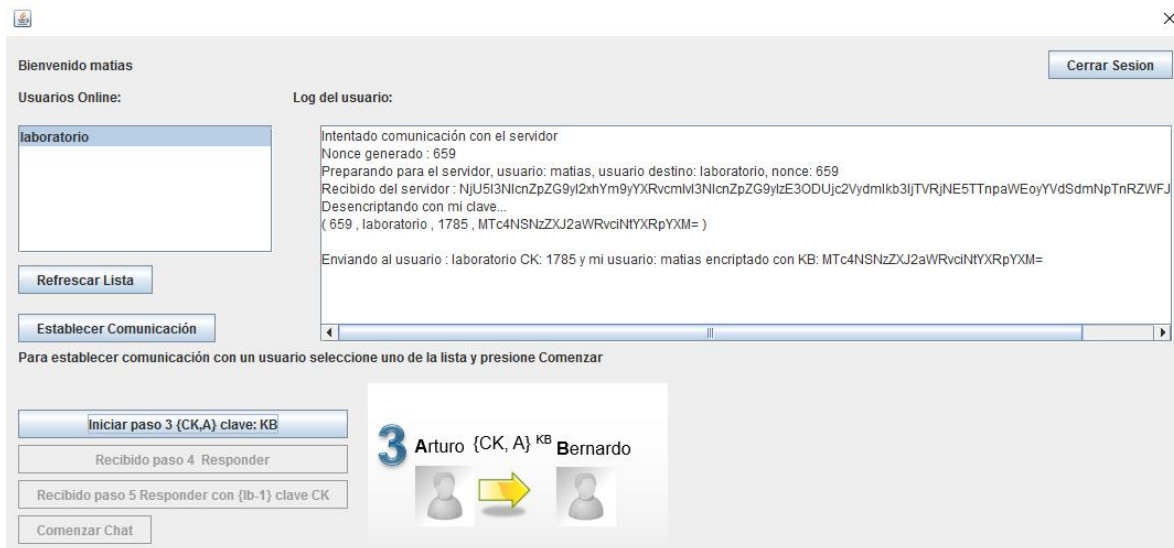


Figura 3.9: Paso 3 en instancia “A”

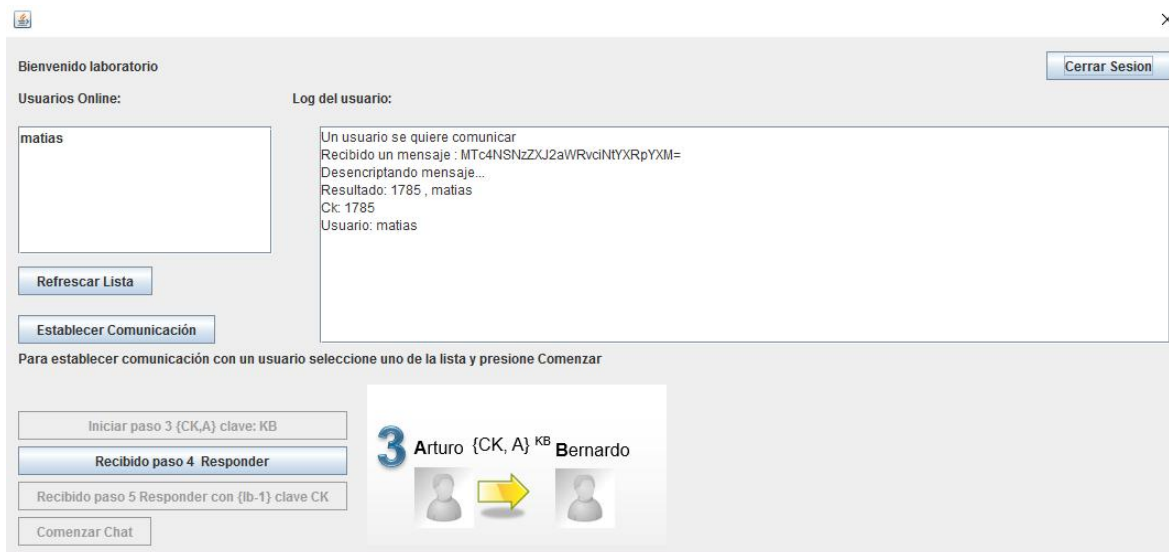


Figura 3.10: Paso 3 recibido en instancia "B"

Luego de ejecutar el paso 3, "A" queda en espera a que "B" le responda, para ello en "B" presione el botón "Recibido paso 4 Responder", con esto "B" quedará a la espera de que A realice el paso 5. La Figura 3.11 muestra a "B" enviando el paso 4 y la Figura 3.12 muestra a "A" luego de recibir correctamente y efectuar las comprobaciones luego de que "B" realice el paso 4.

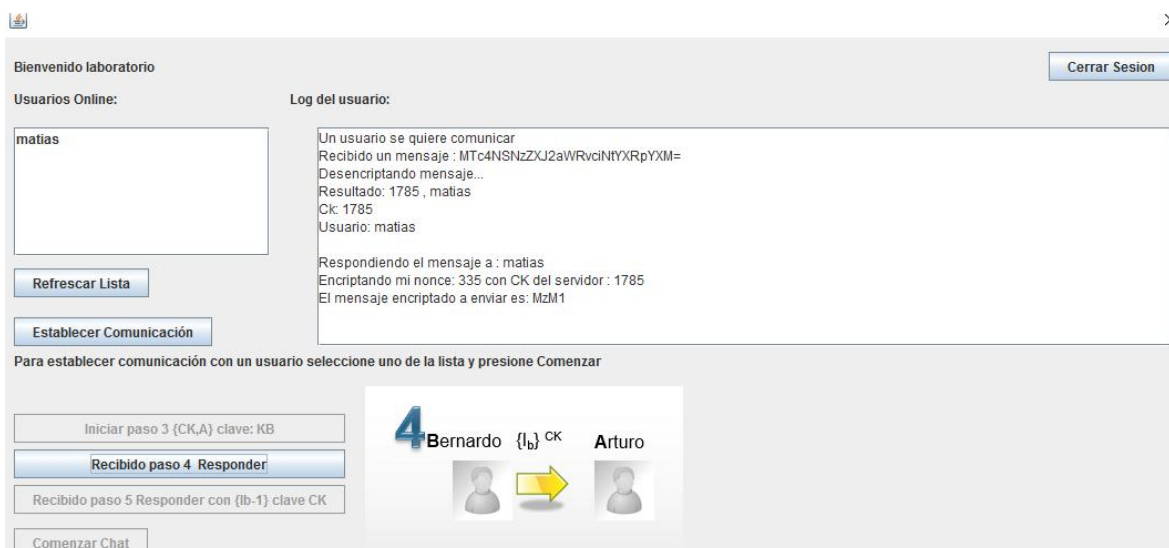


Figura 3.11: B luego de efectuar paso 4



Figura 3.12: A luego de recibir el mensaje de B del paso 4

La Figura 3.12 muestra que “A” recibió correctamente desde “B” el mensaje y las comprobaciones fueron las correctas, al ocurrir esto, se habilitó el botón del paso 5, por lo que para efectuar el paso5, “A” debe presionar el botón “Recibido paso 5 Responder con {lb -1}”. Al presionar este botón, “A” le envía el mensaje a “B”, “B” por su parte comprueba el mensaje y si las comprobaciones son correctas, habilita el botón “Comenzar chat” y le envía el mensaje a “A” para indicar que es segura la comunicación, por lo que en “A” también se muestra el botón “Comenzar chat”. La Figura 3.13 muestra a “A” luego de efectuar el paso 5 correctamente y la Figura 3.14 muestra a “B” luego de recibir el paso 5 correctamente.



Figura 3.14: A luego de realizar el paso 5 correctamente

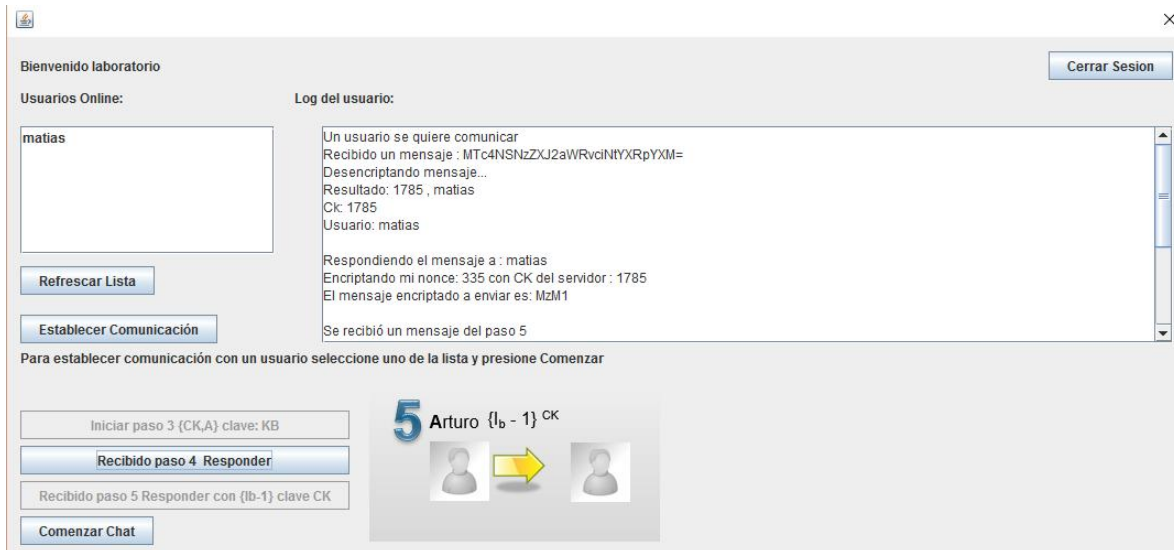


Figura 3.15: B luego de recibir el mensaje de A del paso 5

Teóricamente, si los pasos están correctamente realizados “A” y “B” podrían efectuar la comunicación. Si se realizó todo correctamente, al presionar el botón “Comenzar Chat” se muestra un mensaje el cual se puede ver en la Figura 3.16.

Que los usuarios se comuniquen a través de un chat no está implementado en el programa, pero teóricamente, estos podrían tener una comunicación confiable debido a que el protocolo Needham-Schroeder fue realizado correctamente.

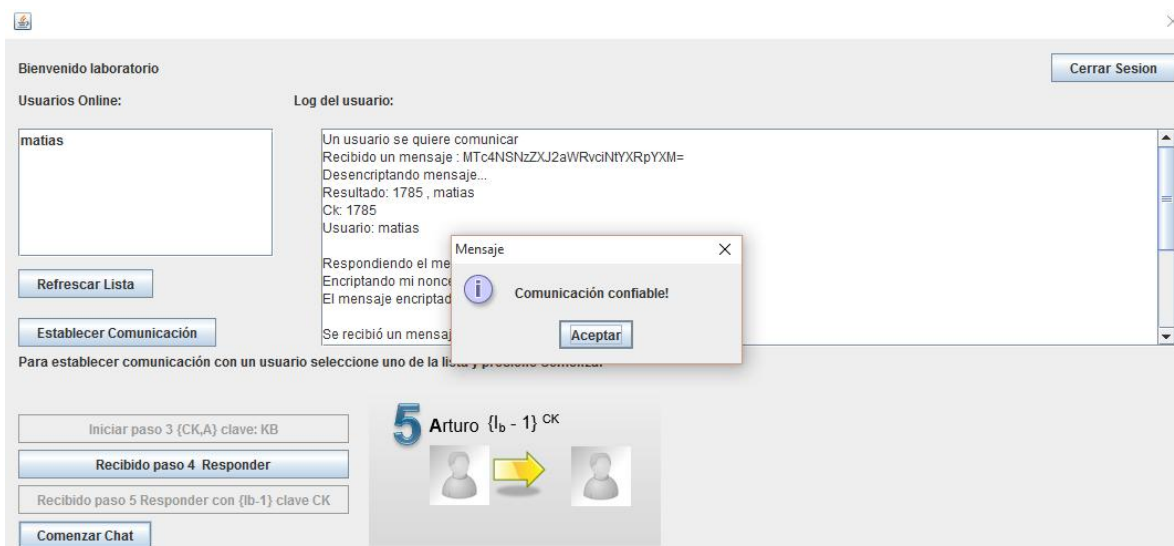


Figura 3.17: Mensaje para comenzar chat