Juego de Adivinar el Número utilizando Sockets SSL/TLS en Java

Alejandro Caro Rodríguez
DA2D1A

Explicación detallada

El programa desarrollado es un juego de "Adivinar el Número" que utiliza comunicación segura mediante sockets SSL/TLS, aprovechando la extensión JSSE (Java Secure Socket Extension). El objetivo es implementar un juego interactivo y seguro entre un servidor y un cliente, asegurando que todos los datos enviados y recibidos estén cifrados y protegidos contra posibles interceptaciones.

El servidor actúa como anfitrión del juego. Al iniciar, genera un número aleatorio dentro de un rango predefinido, por ejemplo, entre 1 y 100. Este número será el que el cliente intentará adivinar durante el juego. El servidor utiliza un certificado almacenado en un archivo de tipo keystore.jks, que cual permite establecer conexiones seguras con el cliente mediante el protocolo SSL/TLS. Una vez configurado, el servidor queda a la espera de recibir conexiones.

Por otro lado, el cliente es el participante del juego. Para conectarse al servidor, necesita confiar en el certificado de este, lo cual se logra utilizando un archivo truststore.jks que contiene el certificado del servidor previamente importado. Una vez establecida la conexión, el cliente puede enviar sus intentos al servidor para adivinar el número secreto. Cada intento será evaluado por el servidor, quien responderá: "Mayor" si el número es más grande que el intento, "Menor" si es más pequeño, o "Correcto" cuando el cliente acierta. Este ciclo continúa hasta que el cliente adivina el número.