PRÁCTICA 4

1. Introduce seguridad criptográfica a tu servidor de ficheros con sockets. Para ello, servidor y cliente se generarán su par de claves, y ambos se mandarán sus respectivas claves públicas. Todo lo que se envíen cliente y servidor deberá ir desde ese momento cifrado y firmado. Haz una versión sin firmar y otra firmando.
2. Modifica el ejercicio anterior para que una vez conocidas las claves públicas del otro extremo de la comunicación, el servidor mande una clave de cifrado simétrico al cliente y lo que se envía (el contenido del fichero) se haga utilizando la clave de cifrado simétrico. Seguirá siendo necesario firmar todo. Implementa una versión firmando y otra sin firma.
3. Toma datos y haz un estudio comparativo de los bytes enviados por el socket y el tiempo empleado en todos los casos que has implementado para la transmisión del fichero. Para ello tendrás que modificar los ejercicios anteriores para que saquen por pantalla información necesaria. Prueba con diferentes tamaños de ficheros y monta una tabla. Los casos a analizar son: sin cifrar, con cifrado asimétrico (prueba con claves de diferentes longitudes) tanto firmando como sin firmar, y con cifrado simétrico tanto firmando como sin firmar.