**Ejercicios de resumen (MD5 y SHA).**

**1º** Vamos a generar un programa cliente que le enviará a otro servidor una cadena y un resumen (con “SHA1” o “MD5”). El servidor deberá comprobar si la cadena es correcta.

**Nota:** serializa la cadena y el resumen. El servidor deberá leer ambos y calcular su propio resumen para ver si la cadena es correcta.

**2º** Modifica el bloc de notas que hicimos en temas anteriores. Le vamos a añadir tres botones: ***Guardar***, ***Enviar*** y ***Comprobar***. Cuando pulsemos ***Guardar*** se guarda el texto y el resumen en archivos diferentes. Cuando pulsemos ***Enviar*** se genera el resumen y se guarda el texto para enviarlo todo a un servidor que se encargar de guardar esa información y comprobar por su cuenta que la información enviada es correcta. El botón ***Comprobar*** lo podremos pulsar al abrir el documento y comprobara que el texto cargado corresponde con la última versión.

**Ejercicios de firmas digitales.**

**3º** Repite el ejercicio 1 usando la firma digital. El cliente generará un par de claves (pública y privada) pasará al servidor la pública y luego le transmitirá texto firmado. El servidor deberá comprobar que el texto es correcto.

**4º** Amplia el ejercicio anterior para que el cliente pueda enviar todos los textos que quiera (usar una aplicación gráfica); todos irán firmados.

**5º** Generaliza el ejercicio anterior para que el servidor admita varios clientes. Creará un hilo para cada cliente que se encargará de verificar lo recibido.

Amplia un poco más este ejercicio de manera que el servidor y el cliente guarden sus claves en ficheros y no haga falta generarlas cada vez. Es decir, si el cliente es la primera vez que se ejecuta genera el par de claves. Guarda la privada en un fichero (“*clave.pri*”) y le pasa la clave al servidor que la guardará en un fichero llamado: “*DNI\_clave.pub*”. Lógicamente el cliente preguntará el DNI al usuario y se lo transmitirá al servidor. Si los ficheros existen es que la comunicación ya se había realizado y, por lo tanto, se recuperan las claves de los ficheros.

**Ejercicios de encriptación.**

**6º** Crearemos un servidor que recibirá un DNI y le asignará una clave simétrica. Dicha clave se pasará al cliente. El cliente tendrá dos áreas de texto una donde escribirá el texto plano y otra donde aparecerá el texto cifrado según la clave proporcionada por el servidor. Al pulsar enviar se enviará al servidor el texto cifrado que mostrará el texto plano en otra área de texto.

**7º** Repetimos el ejercicio anterior pero en este caso la clave será la asimétrica. El servidor mediante sockets no seguros proporcionará la clave pública al cliente. El cliente cifrará el texto con la clave pública proporcionada y se la enviará al servidor. El servidor la descifrará y la almacenará en alguna colección asociada al cliente.

**8º** Añadir a los ejercicios 6 y 7 la opción de que la clave se guarde en un fichero y sea recuperada en cada comunicación.

**Ejercicios de SSLSocket.**

**9º** Cambiar los sockets utilizados en los ejercicios anteriores por sockets seguros.