PSP - DAM FINAL
NOMBRE: FECHA:04/03/24

NOTA ACLARATORIA:

El presente examen corresponde a la evaluación final del módulo de PROGRAMACIÓN DE SERVICIOS Y PROCESOS. Para la corrección del mismo ***se valorarán las buenas prácticas de programación y limpieza a la hora de escribir el código, teniendo en cuenta además, la elegancia e ingenio en la resolución de los problemas propuestos y los COMENTARIOS*** tal como se han ido adquiriendo los conocimientos a lo largo del trimestre. **Deben funcionar OK!!!**

Hay que obtener un 5 (como mínimo) en este examen **para poder aprobar el módulo**

Entregaréis las clases correspondientes a cada ejercicio en carpetas, para posteriormente entregar un fichero comprimido con vuestro nombre en la forma siguiente:

NombreApellidos_Curso → Ejemplo: **AndresChillonSesma_DAM2.zip (rar, 7Z, ...)**

PSP - DAM FINAL
NOMBRE: FECHA:04/03/24

EJERCICIO 1 (5 PUNTOS)

Con el fin de realizar un aprovisionamiento de clientes de confianza, en la empresa ACME han decidido iniciar un proceso de validación y verificación de clientes a través de la información fiel y veraz de los mismos. Para ello tendremos que realizar un programa en el que tengamos un servidor a la escucha de clientes que se quieran conectar (1..N) y cada cliente que se conecte lo hará con un nombre y recibirá del servidor un fichero CIFRADO.txt (que estará cifrado).

El fichero que recibirá cada cliente, se almacenará en su propia ruta. Nosotros, al estar en el mismo PC, vamos a dejarlo en la ruta relativa ./pendFirma/<nombreCliente>/CIFRADO.txt

De este modo podremos tener todos los ficheros en el mismo almacén, simulando diferentes ubicaciones remotas.

Una vez el fichero esté en el cliente:

- Se realice una verificación para comprobar que dicho fichero es el original que envía el servidor (recordad que hay que descifrarlo, obtener el resumen y compararlo con el resumen que también hay que descifrar para saber si son iguales, ya que lo vamos a cifrar todo!!!)

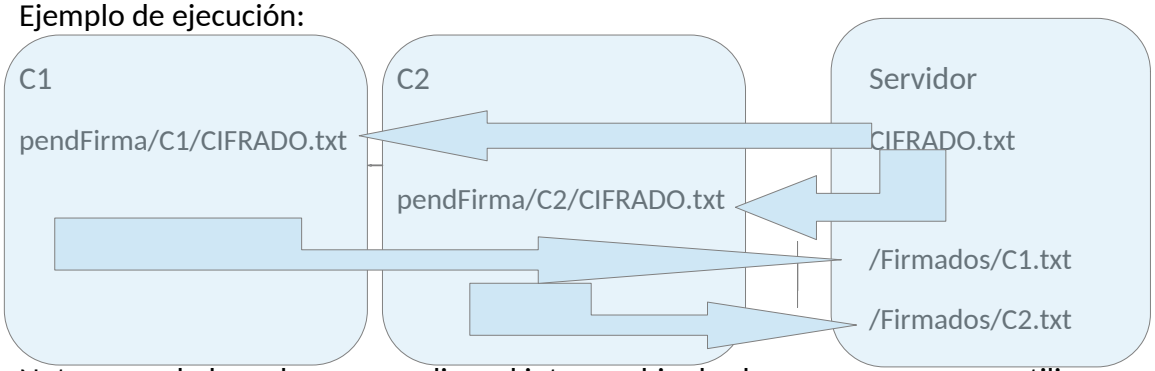
- Modificar el fichero introduciendo las credenciales del cliente nombre y

apellidos al final del fichero recibido, para guardarnos una copia fiel a la original que nos ha enviado el servidor.

- Desde el cliente, vamos a verificar que queremos pertenecer a la corporación cifrando nuevamente dicho fichero y enviándoselo al servidor.

Por último, en el servidor comprobaremos (descifrando el mensaje que el cliente ha retornado con su firma) que el fichero recibido es correcto y lo guardaremos con el nombre del cliente en la carpeta /Firmados.

Ejemplo de ejecución:



Nota: recordad que hay que realizar el intercambio de claves, ya que se va a utilizar un sistema de encriptación de clave pública. (Ejercicios 8 y 9)

1. Firmar los datos de un fichero con la clave privada
2. Verificar la firma de un fichero con la clave pública

PSP - DAM FINAL
NOMBRE: FECHA:04/03/24

EJERCICIO 2 (5 PUNTOS)

Realizar un programa estilo aplicación de mensajería móvil exclusiva por ser solamente pensada para grupos. Con lo cual, habrá un servidor en el que se conectarán uno o varios clientes, de manera que lo que escriba uno, lo vean todos (incluyendo quien lo escribe. Los mensajes irán **con resumen y solamente cifrados con la función que convierte a hexadecimal** al servidor y del servidor al grupo, para preservar algo la seguridad. El servidor almacena una copia en un historial (para facilitar las comprobaciones, **descifrada**) de mensajes de los clientes en un fichero almacenado en la ruta relativa del servidor **/history.txt** de la forma:

fecha: nombre: mensaje

domingo,3 de marzo de 2024, 16:32:42 CET: Pepe: Hola a todos, sabéis a qué hora es el examen de PSP?

domingo,3 de marzo de 2024, 16:33:51 CET: José: Ni idea, pero hay examen? Cuándo?

domingo,3 de marzo de 2024, 16:34:12 CET: Pepe: El lunes, día 4 de Marzo :)

domingo,3 de marzo de 2024, 16:38:57 CET: María: Creo que era después del recreo

domingo,3 de marzo de 2024, 16:39:26 CET: Pepe: Ni de broma! A esa hora no tenemos clase. La duda es, son 2 o 3 horas?

domingo,3 de marzo de 2024, 16:51:02 CET: Juan: No escuchasteis? A las 8:30, las dos clases. Llevo estudiando todo el trimestre para este día. Suerte!

domingo,3 de marzo de 2024, 16:52:04 CET: Pepe: Muchas gracias Juan, nos vemos a las 8:20. Llegaremos antes para estar listos. Suerte a tod@s

domingo,3 de marzo de 2024, 16:52:43 CET: José: Igualmente, A ver si suena la flauta… Descansad!

domingo,3 de marzo de 2024, 16:55:45 CET: María: Gracias compis!. Nos vemos mañana! Suerte igualmente!!!!!

Implementa una solución que de respuesta a esta petición de la manera más elegante.