

(2 Pto) Una empresa de detectives tiene casos en los que trabajan dos detectives, uno por la mañana y otro por la noche. El de por la mañana genera informes que el de por la noche contrasta. La empresa solo tiene un ordenador para todos los empleados y tiene que inventar un mecanismo para que los informes del detective de la mañana solo los pueda ver el de la tarde. Los detectives no se conocen solo saben que uno trabaja por la mañana y otro por la noche. Inventa un mecanismo para que los informes solo los puedan ver ellos, y el de por la noche este completamente seguro de que el informe lo ha hecho el de la mañana.

(2 Pto) Un casino ilegal quiere mantener seguras las apuestas de sus clientes, para no levantar sospechas en la policia no dispone de HTTPS y las peticiones se hacen por http.
El registro en el casino ilegal se hace de manera presencial, los usuarios van al casino, y el casino entre otras posibles cosas les apunta el nombre de usuario y el numero de cuenta y les da toda la información necesaria para que las apuestas solo las pueda ver el casino y el resto de participantes. El unico juego del casino es la ruleta y todos los participantes registrados pueden ver las apuestas de los demás. Lo que no se quiere es que alguien de fuera pueda ver las apuestas viendo la comunicación o entrando en BD sin permiso.
El casino se fia de que todos los clientes por el simple hecho de registrarse.
El objeto apuesta tiene el nombre del usuario, el numero y la cantidad.
Haz el mecanismo para que un cliente haga un apuesta, un POST. No hace falta que el servidor guarde la apuesta en ningun sitio, solo que la saque a la consola.

(2 Pto) Entre un usuario y un servidor hay que hacer una comunicación segura punto a punto, es necesario un rest para añadir Datos y un get para devolverlos.
El usuario ya está registrado y tendrá en su carpeta local todas las claves necesarias y el servidor tb.
Haz la comunicación mandando el objeto Dato de manera segura.

3 (3.5 Pto) se quiere hacer un servidor para envios de mensajes de amor, estos mensajes se guardan en un buzón en el servidor, y cuando el usuario entra podrá consultarlo. Los mensajes tienen un remitente un destino y el mensaje. Los mensajes no tienen que ser leidos por nadie salvo su destinatario, que tendrá que poder asegurar que el mensaje es del remitente.
Habrá dos peticiones, dejar mensaje para alguien, y ver mis mensajes.
Al dejar el mensaje para alguien, guarda el mensaje en una lista estatica en servidor.
Al ver mis mensajes, el servidor tiene que poder verificar que el usuario es quien dice ser.
Si hace falta un registro de usuario por parte del servidor hazlo si no, no.
Un login con usuario y contraseña sí que no hace falta.

1) (4Pto) En un pueblo perdido del amazonas llega el "The man of Tallahassee" (guiño a serie famosa), (info para curiosos, tallahassee está a unas 490 millas de nashville).
Este tio quiero venderles un ordenador, les dice que para guardar secretos entre grupos de aldeanos. El caso es que consigue venderse, pero antes tiene que encargar el programa para hacerlo.
Teniendo en cuenta un par de cosas:
Solo hay un ordenador en el pueblo, no tienen conexión a internet.
En el pueblo hay muchos grupos que se reúnen habitualmente para hablar de sus cosas.
Han decidido que la fecha en la que quedan es lo que van a guardar para que solo los del grupo puedan verla y nadie les moleste.

Tienen que evitar que graciosos pongan fechas que no son, así que cualquiera que vaya al ordenador para ver la fecha de su siguiente reunión tiene que poder salir pensando que la fecha es correcta sin lugar a dudas.

Las fechas se van poniendo por cada miembro del grupo en orden para que todos puedan elegir las horas que más les convengan.

No se fían unos grupos de otros, solo se fían del jefe de la aldea, que conoce a todos los del grupo y puede verificar que son de ese grupo pero no se fían tanto como para que pueda ver la fecha.

El jefe de la aldea tiene que estar presente cuando metan la fecha, pero no hace falta que esté cuando el resto de personas la vea.

Haz el programa lo más sencillo posible.