# Proyecto SDS: GoChat

**Autores**: César González Mora y Pedro Rafael Tarancón Baeza

## Descripción del proyecto

El proyecto GoChat consiste en un chat cifrado en el que dos usuarios o más se pueden comunicar. De esta forma, un usuario se registra en la aplicación de terminal GoChat, accede con su nombre de usuario y tiene la opción de entrar en una sala de chat pública, o chatear con un usuario en concreto buscando su nombre de usuario. En el caso de que ambos usuarios estén conectados, podrán comunicarse entre ellos a partir de este chat.

## Tecnologías y metodologías utilizadas

Para el trabajo en equipo entre los dos miembros del grupo, se ha utilizado github para un control de versiones distribuido, con 1 rama de trabajo para cada miembro y una rama común donde juntar todo el trabajo realizado.

## Diseño e implementación

El diseño que hemos planteado para este proyecto es el siguiente. Contamos con dos roles, el cliente y el servidor, los cuales se comunican entre sí, cliente con servidor y servidor con cliente.

El servidor se encarga de establecer la conexión con cada cliente, gestionar el registro y login de cada cliente, recibir los mensajes que este quiere enviar y enviar al cliente los mensajes que reciba. El servidor no tiene acceso a los datos enviados por el usuario ya que están cifrados.

El cliente se encarga de enviar todas las acciones al servidor y los mensajes que quiera mandar a otros clientes. Todos los mensajes que escriba el cliente (además de la contraseña), estarán cifrados en ChaChá (la contraseña en hash), de forma que cuando el cliente los reciba tendrá que descifrarlos.

Para su implementación hemos utilizado Go con las respectivas librerías para la comunicación entre cliente-servidor, trabajo en el terminal, cifrado, etc.

## Principales funciones implementadas

* Funcionalidad
  + Login/Registro: sí que se almacenan en la base de datos.
  + Chats (público y privado): sólo con usuarios que estén logueados, no hay persistencia de los mensajes.
  + Ver y buscar perfiles usuario: de todos los usuarios almacenados en la base de datos.
* Seguridad
  + Autenticación seguro: está hecho con hash. Si tenemos tiempo miraremos de hacerlo con Hash+Sal o PBKDF+Sal.

## Principales funciones por hacer

* Funcionalidad
  + Sincronización de mensajes entre usuarios: si tenemos tiempo miraremos si utilizar el mutex para la sincronización entre usuarios.
* Seguridad
  + Cifrado en tiempo real: tenemos pensado hacerlo con ChaCha.
  + Optimización de privacidad: tenemos pensado hacerlo cifrando y descifrando los mensajes de chat el cliente. Los datos que tendría en claro el servidor serían los mensajes de login, registro, ver y buscar perfiles.
  + Transporte de red seguro: tenemos pensado hacerlo con TLS.