# 安全的即时通讯系统

1. 需求：
2. 实现客户端和服务器的通讯以及客户端到客户端的通讯
3. 服务器要有登录用户信息验证功能，用数据库存储账号密码
4. 安全性：客户端加密消息后发送，对于本地聊天记录文件，则先加密，再签名。服务器端解密消息后进行操作，发送到客户端的消息也要加密
5. 架构
6. 采用服务器-客户端的架构：服务器负责监听登录请求，解密账号密码数据包之后，到数据库验证身份后发送连接成功消息，然后向所有在线客户端发送广播，告知所有客户端当前在线人的名字和IP；此外，服务器负责转发聊天消息。
7. 客户端，手动输入用户名和密码，加密后发送到服务器端，服务器端解密消息并操作。客户端收到消息后进行解密，然后显示。
8. 服务器和客户端通过UDP协议互联。
9. 加密采用AES加密算法，签名算法为RSA。
10. 使用多线程技术保证客户端和服务器不在某一步无限等待下去，而是可以同时进行多项操作。
11. 具体实现：
12. 套接字：服务器采用两套套接字（分别用同一个本机IP绑定不同的端口，LOG\_PORT和MSG\_PORT分别为登录服务套接字和消息服务套接字），一号线程：LOG\_PORT为登录验证服务套接字，监听用户发来的登录请求，查找数据库验证处理完成后，（此时切换套接字）通过MSG\_PORT广播发送到所有客户端，广播完成后再绑定回LOG\_PORT继续监听登录消息；与此同时，开启二号线程，此线程负责转发聊天消息，绑定MSG\_PORT监听，收到消息后只负责转发，不作任何处理。
13. 客户端也采用双线程，各自绑定一个套接字。在用户输入完账号密码后，一号线程启动，将账号密码加密后发送到服务器的LOG\_PORT套接字，发送完成后，切换到MSG\_PORT接收服务器消息并解密显示出来，并且写日志（加密的）然后对日志签名；二号线程，创建另一个套接字，每当输入聊天文字，向服务器的MSG\_PORT套接字发送聊天消息（只负责发送）,这条线程只负责发送聊天消息；一号线程只负责发送账号密码，然后转入收听消息的状态（收听来自服务器的MSG\_PORT），因为收发消息分离，所以不会出现一直收听消息无限等待的情况，不会卡死。
14. 客户端之间不能直接相连，都要通过服务器转发。
15. 在低并发下，服务器不会出错，高并发（同时连接几十上百个客户端）下会出错误，主要是会出现丢包和发错消息的现象。