SERVER

CLIENT1

CLIENT2

请求与2连接

此程序是一个基于秘钥分发的聊天室。

任意一个客户端可以通过向服务器发送连接请求来获得与对应客户端的沟通密钥，从而进行信息交互

SERVER

CLIENT1

CLIENT2

分发密钥

分发密钥

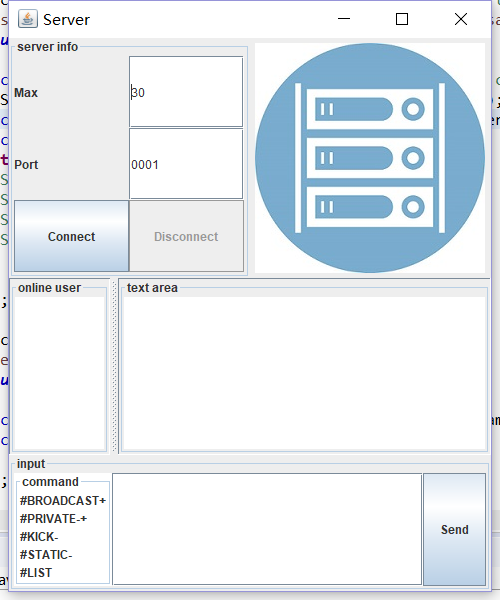
密钥仅限于单次连接。当两个用户中任意一个用户离线或被服务器端剔除时，再次连接需要重新请求密钥

SERVER

CLIENT1

CLIENT2

交换信息

此界面为服务器端。

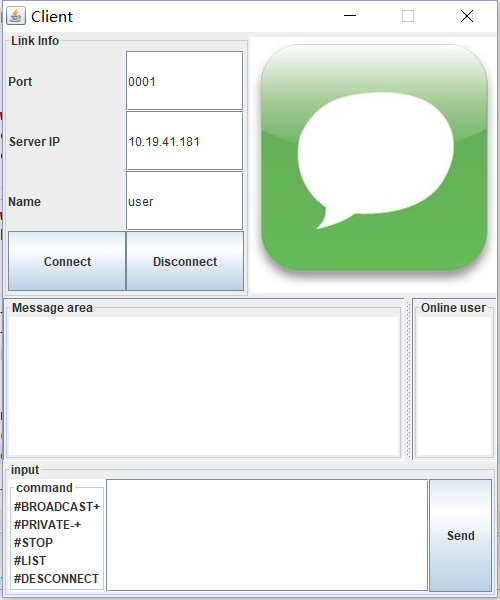
当且仅当服务器启动的时候，客户端才能建立连接

左下为命令区域

其中STATIC命令可以监控每两个用户之间的信息交流（获取被加密的信息）

KICK 命令可以终止某一用户和服务器的连接

BROADCAST 用于群发消息

此界面为客户端。

其中DESCONNECT命令用于请求加密连接

PRIVATE 命令用于发送私密消息

BROADCAST 命令用于发送公共消息

STOP 用于终止连接

程序的基础框架结构（如下）

CLIENT

SERVER

服务器端通过创建客户线程，来管理和确保所有客户端的正常运行和功能实现

客户端之间通过socket来实现消息的交互。所有的被交互信息除去广播消息之外均为加密消息

客户端通过线程监听消息

监听得到的消息经过命令识别之后进行解密，最终转换为文字

发送消息的方式同理。

积极的：

易于实现不同类型的命令

所有聊天都在服务器的控制之下

快速易用

使用方便

添加许多错误报告以避免胎儿错误：例如：如果用户输入了错误的命令并且不存在用户名，程序将首先检查

否定的

所有的消息都应该通过服务器。

同一用户名中的两个用户不能一起访问服务器。（第二个人的程序将被删除）

设计：

对于服务器：

使用ARARYLIST存储客户端。所以很容易获取和查找和删除

客户端和服务器保持活跃，使消息立即出来

所有命令出来的位置都在SeND（）方法中。只是比较字符串很容易修改任何命令

所有命令进来都位于cliththRead（）方法中。只需比较字符串就可以很容易地修改任何类型的命令，使用服务器作为中间程序

一些固定的命令：在UI后面运行一些不可见的命令，使程序更加可靠。

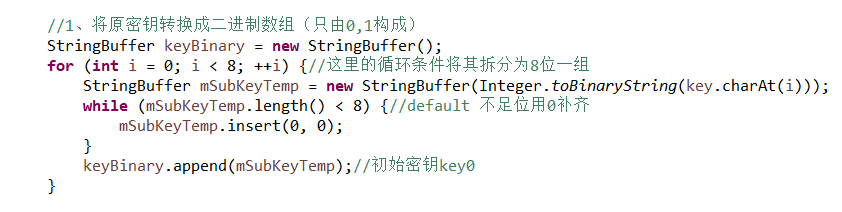
this program uses the DES algorithm to solve the encrypt problem. This is the UI:



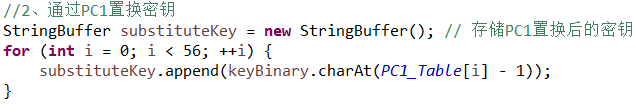
The plaintext and key need to be size 8.

Step1: generate the sub key group.

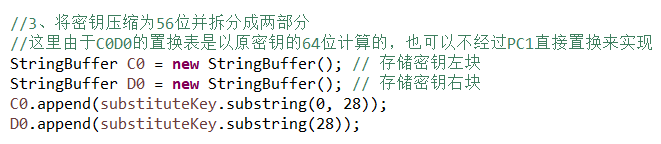
Step 1.1:first we should trans the original keyword into binary type:



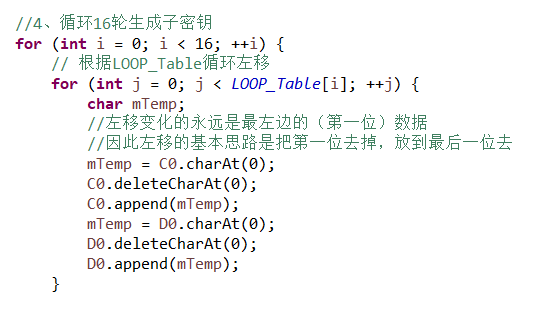
Step 1.2: do the first PC1 replacement:



Step 1.3: zip the key and divided it into two parts:C0&D0

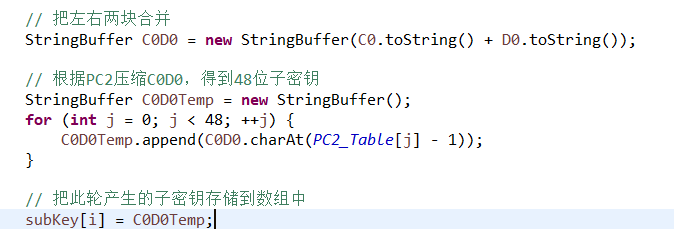


Step 1.4: do the loop, generate the sub key group:

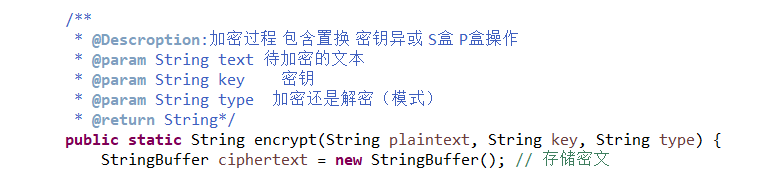


Here we should move horizontally all the numbers with the requirement of LOOP\_Table

Step 1.4.1:we use PC2 to deal with the single key that zip the sub key from 56 to 48



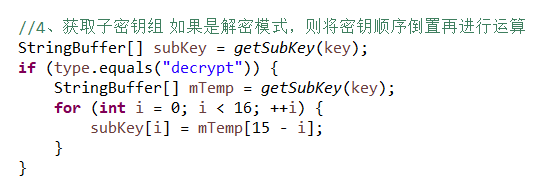
Step2: the encryption operation



Step 2.1 trans the code into binary type and use the IP replacement then divide it into L&R



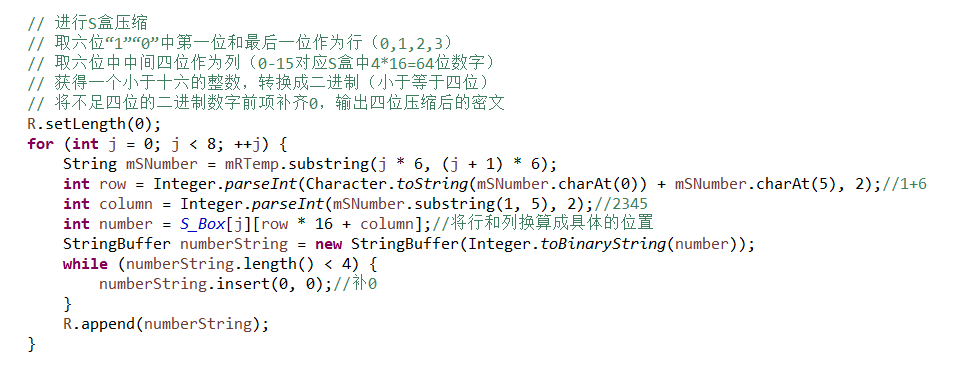
Step 2.2 get the sub key group and decide the type of the algorithm



Step 2.3 16 times loop, with L&R exchange and E expand and not&or operation.



Step 2.4 Sbox operation.



Step 2.5 P\_table replacement



Step 2.6 combine the final result, do the IPR replacement then out put the result.

