开题报告

学院：软件学院

学号：2013201213

姓名：孙雪峰

日期：2016/12/17

1. **背景**

在当今这个信息爆炸的时代中，网络聊天工具已经成为一种必不可少的信息传递工具。而信息的正确传递以及信息的保密性，更是检验一款聊天软件的性能的关键指标。本课题旨在设计开发一款安全性高、性能稳定的安全聊天工具，以用于信息的可靠传递与信息的保密性的保证。

1. **需求分析**
   1. 系统目标分析

设计并实现一套安全性高、性能稳定的聊天工具。该聊天工具可以正确的传递聊天过程中产生的聊天数据，并且通过加密算法加密后按照自定义的通信协议在网络中传输，客户端接受数据后可以正确解析并显示。聊天工具具有阅后即焚的能力，并可在发送端进行时间设置。最终达到聊天信息的可靠传递与信息的保密性的得到保证的效果。

* 1. 系统需求结构图

本系统主要包含用户管理、通讯模块、好友管理、系统设置4个功能模块，各模块之间的关系如图2.1所示。

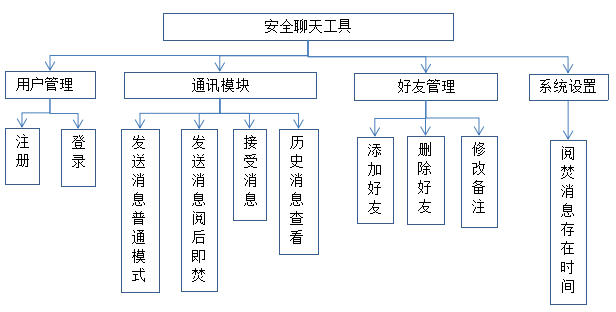


图2.1 系统需求结构图

* 1. 系统功能描述

本系统主要包含用户管理、通讯模块、好友管理、系统设置4个功能模块。其中所有功能模块所包含的具体功能项以及详细说明，如表2.1所示。

表2.1 功能详细描述表

|  |  |  |
| --- | --- | --- |
| **功能模块** | **功能名称** | **功能详细说明** |
| 用户管理 | 注册 | 用户注册个人账号 |
| 登录 | 用户使用个人帐号登录系统 |
| **功能模块** | **功能名称** | **功能详细说明** |
| 通讯模块 | 发送消息-普通模式 | 用户给好友发送消息，消息一直可见 |
| 发送消息-阅焚模式 | 用户给好友发送消息，在好友阅读后，约定时间后自动删除。 |
| 接收消息 | 接收并正确显示好友发送想消息 |
| 历史消息查看 | 查看与好友发送的历史消息 |
| 好友管理 | 添加好友 | 用户添加其他用户为到自己的好友列表中 |
| 删除好友 | 用户将已经添加为好友的用户从自己的账户中删除 |
| 修改好友备注 | 用户在自己的帐号中修改已经添加为好友的用户的备注信息 |
| 系统设置 | 阅焚消息存在时间 | 设置选项，用户设置阅焚消息的存在时间 |

1. **详细设计**
   1. 系统结构图

本系统采用C/S架构设计，通过服务器来中转数据和保存客户数据以及成对的密钥。在客户端使用RSA加密算法加密消息，再通过设计好的通信协议封装数据发送给好友的客户端。具体的系统结构图如图3.1所示。

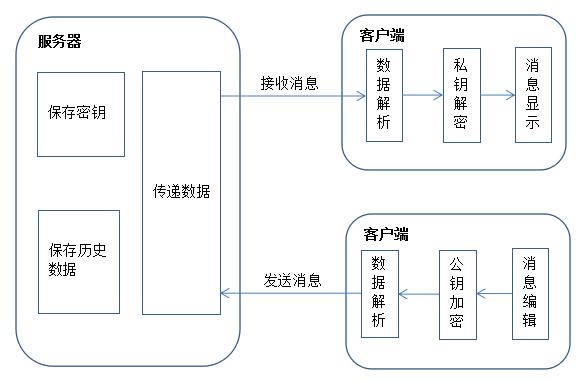


图3.1 系统结构图

* 1. 系统界面设计

本系统的界面主要由登录界面、好友管理界面、通信界面、设置界面四大界面组成。界面风格以简洁明了为主，注意用户体验，方便使用即可，详细的UI设计在后续的工作中有相应体现。

* 1. 加密算法设计

本系统采用非对称密码算法RSA加密算法。RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击。只要其钥匙的长度足够长，用RSA加密的信息实际上是不能被解破的。

用户在注册后会生成一对密钥，在本地保存私钥（公钥和私钥在服务器上都有备份，在本地不存在时，可以在登录时自动从服务器获取私钥）。在发送消息时，用户通过服务器获取到好友的公钥加密数据，发送消息时通过私钥加密消息。服务器只负责转发加密后的数据，即使数据在传递过程中被黑客截获也无法破解。

* 1. 网络通信

本系统使用SuperSocket开源框架搭建服务器，SuperSocket 是一个轻量级, 跨平台而且可扩展的.Net服务器程序框架。通过使用此框架可以方便的更换数据传输的通信协议，控制服务器的客户端连接数目，很方便的使用Socket来实现网络通信。

1. **时间进度安排**

整个系统的时间进度安排情况如表4.1所示。

表4.1 时间进度安排表

|  |  |
| --- | --- |
| **具体进度安排** | **具体时间安排 单位：/周** |
| 客户端UI设计 | 0.5 |
| 数据库设计 | 1 |
| 客户端与服务器通信API设计 | 0.5 |
| 加密算法设计 | 0.5 |
| 通信协议设计 | 0.5 |
| 详细设计说明书的编写 | 0.5 |
| 服务器端开发 | 1 |
| 客户端开发 | 1 |
| 系统测试 | 0.5 |
| 撰写论文 | 2 |

1. **参考文献**

[1]谢希仁. 计算机网络[M].北京：电子工业出版社，1999．

[2]何鹏飞, 王征.　C#实用编程百例[M]．北京：清华大学出版社, 2004．

[3]孙志辉. C#程序设计[M]．北京:人民邮电出版社, 2015．

[4] Charles Petzold.Programming microsoft windows with C#[M]．上海:世界图书出版公司, 2001．

[5] X. Yan, M. Mehan, Y. Huang, et al. A Graph based approach to systematically reconstruct　human transcriptional regulatory modules[J]. Bioinformatics, 2007, 23(13): 577-586.

[6]J. Broeckhove, K. Vanmechelen. An adaptor for C++ callbacks with C and Fortran libraries[J].　Elsevier Journal,2013,184(3):824-832．