**第1-2周（本部分的内容量够了，但是要以描述性的口吻去写，写你做了哪些事情，比如查阅了什么资料，研究了什么内容，初步确定采用什么方法解决什么问题）**

我的毕设题目是设计并开发一款安全性高、性能稳定的安全聊天工具。在与导师交流后，我将整个系统分为用户管理、通讯模块、好友管理、系统设置4个功能模块。其中用户管理模块包括用户注册、用户登录、用户信息更新功能。通讯模块包括发送消息（普通模式）、发送消息（阅焚模式）、接受消息，历史消息查看功能。好友管理模块包括添加好友、删除好友、修改好友备注功能。系统设置模块包括设置阅焚消息存在时间的功能、清空历史消息、注销登录。

进一步分析后，我发现系统实现的关键点主要集中在系统界面设计、加密算法设计、网络通信以及通信协议的制定这三个方面。在界面设计方面，我准备以当前主流的网络聊天工具QQ界面设计为参考，再辅以其他一些聊天工具的优点，以简明易用为核心设计系统的操作界面。加密算法方面，我通过互联网了解到，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，所以我准备在本系统上使用C#实现RAS加密算法。在网络通信以及通信协议的制定方面，我根据以往的项目经验，准备使用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，修改数据打包方式，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。

**背景说明**

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。

**主要内容（）**

本系统在功能方面主要包含用户管理、通讯模块、好友管理、系统设置4个功能模块，在信息安全方面主要由三道防护墙保障。

1. 用户管理模块括用户注册和用户登录功能、用户信息更新。用户注册提供给用户注册个人帐号的功能，个人帐号是服务器识别用户身份并且允许用户登录系统的唯一标准。用户登录提供给用户登录系统的功能，通过个人帐号的身份验证，用户才可以登录聊天工具，修改个人信息、增删好友发送消息以及查看历史消息，身份验证是信息安全的第一道防护墙。用户信息更新提供给用户更新个人信息的功能，用户可以修改昵称、登录密码等个人信息。（用户管理模块可以保证吗）
2. 通讯模块包括发送消息（普通模式）、发送消息（阅焚模式）、接受消息，历史消息查看功能。发送消息（普通模式）与接受消息为用户通过基本的通信功能，接发双方都可以自由查看历史消息，无消息显示时间的限制。本系统中的聊天消息的传输使用RSA非对称加密算法，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，这是信息安全的第二道防护墙。如果用户对信息保密性有更高的要求，可以使用本系统的发送消息（阅焚模式）功能，发送消息（阅焚模式）是发送发送的消息在被接受者查看一定的时间后自动销毁并且无法再次查看（显示的时间设置在后面的模块中有介绍）。这是信息安全的第三道防护墙。（加密传输体现在哪里）
3. 好友管理模块包括添加好友、删除好友、修改好友备注功能。用户可以使用被模块的功能对自己账户内的好友进行添加、删除、修改备注信息的管理操作。
4. 系统设置模块包括设置阅焚消息存在时间的功能、清空历史消息、注销登录。设置时间功能可以修改发送消息（阅焚模式）下发送的消息在接收发客户端显示的时间长短。清空历史消息功能可以清空本地历史消息的存储。注销登录功能可以注销当前登录用户。（系统设置是不是内容太少了，应该没有哪个聊天工具系统设置里就一项内容吧）

**方案及进度安排**

第1周-第2周 查阅相关资料，撰写开题报告，完成开题

第3周-第4周 进行需求分析，完成软件系统的概要设计。学习SuperSocket开源框架、学习RSA算法的C#实现，学习其他开发中需要技术知识

第5周-第6周 完成安全聊天工具的UI设计，完成系统数据库设计，完成客户端与服务器通信API设计

第7周-第8周 完成信息传递加密算法的设计与实现，完成系统网络通信协议设计，完成服务器段的模块组合以及其他模块代码的设计与开发

第9周-第10周 完成客户端UI模块、通信模块以及其他模块代码的设计与实现，完成消息阅后即焚功能的设计与实现

第11周-第12周 对系统进行系统测试，完成系统功能，整理资料，准备论文撰写。

第13周-第14周 完成论文撰写，准备毕业论文答辩。

**主要参考资料（格式应参照撰写规范）**

[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,etal.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.

[7] 江振宇.SuperSocket[CP].http://www.supersocket.net,2016-12-21.