存档编号_____

华北水利水电大学

North China University of Water Resources and Electric Power

毕 业 设 计

题目 电子邮件加密技术及应用

学　　院　信息工程学院

专　　业　计算机科学与技术

姓　　名　尚聪聪

学　　号　201215019

指导教师　王天芹

完成时间　2016.05.24

教务处制

独立完成与诚信声明

本人郑重声明：所提交的毕业设计（论文）是本人在指导教师的指导下，独立工作所取得的成果并撰写完成的，郑重确认没有剽窃、抄袭等违反学术道德、学术规范的侵权行为。文中除已经标注引用的内容外，不包含其他人或集体已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示了谢意。本人完全意识到本声明的法律后果由本人承担。

毕业设计（论文）作者签名：　　指导导师签名：

签字日期：　　签字日期：

毕业设计（论文）版权使用授权书

本人完全了解华北水利水电大学有关保管、使用毕业设计（论文）的规定。特授权华北水利水电大学可以将毕业设计（论文）的全部或部分内容公开和编入有关数据库提供检索，并采用影印、缩印或扫描等复制手段复制、保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交毕业设计（论文）原件或复印件和电子文档（涉密的成果在解密后应遵守此规定）。

毕业设计（论文）作者签名：　　导师签名：

签字日期：　　签字日期：

目 录

电子邮件加密技术及应用

摘 要

随着信息产业的蓬勃发展，信息安全在人们生活中变得越来越重要。电子邮件（E-mail）作为 Internet 中最广泛的应用之一，它的安全性一直备受重视。随着电子邮件依赖性的爆炸式增长，认证性和保密性服务需求也在日益增长。PEM、MOSS、S/MIME、PGP、GPG 是相继出现的一些有关安全电子邮件的协议和标准，本文主要针对 PGP 方法的原理、使用方法以及应用做详细的阐释，并根据 PGP 的加解密原理介绍一个具体应用的小系统。

PGP 是保障电子邮件安全性的开源软件包。它通过使用数字签名提供认证，通过对称分组加密提供保密性，用 ZIP 算法做压缩，并使用基数 64 编码模式提供电子邮件兼容性。PGP 的实际操作有四类服务组成：认证（数字签名）、保密（消息加密）、压缩和电子邮件兼容性。而这四种服务具体使用什么方法实现 PGP 并不要求绝对的统一，也就是说你可以用 DSS/SHA 或 RSA/SHA 做数字签名都可以，使用 CAST 或 IDEA 或 3DES 或 AES 做都可以在 PGP 中做数据加密。所以 PGP 是加密方法，也是加密模型。

通过对 PGP 模型的学习和研究，发现 PGP 加密的思想方法可以运用到希望加密的任何地方。本文的小系统就是简单地模拟演示 PGP 加密运用到字符串、本地文件及网络信息的安全之中。字符串模块主要演示 PGP 加解密的详细过程；文件加密模块运用 PGP 技术保护本地文件安全；安全聊天模块采用 P2P 技术实现一个简单网络聊天，并把 PGP 技术运用到消息传递过程中，保证双方通信的信息的安全性。

关键词：电子邮件；PGP；数字签名；信息安全

E-mail encryption technology and its application

Abstract

With the rapid development of information industry, information security is becoming more and more important in people's life. As one of the most widely used applications in Internet, E-mail's security has been highly valued. With the explosive growth of E-mail dependence, certification and confidentiality services demand is also growing. PEM, MOSS, S / MIME, PGP and GPG have appeared in some of the secure E-mail protocols and standards.This paper is mainly for PGP's principle, method and application. And introduces a specific application of a small system based on the principle of PGP's encryption and decryption.

PGP is an open source software package to ensure the security of E-mail. It provides authentication through the use of digital signatures, and provides confidentiality by symmetric block encryption, using ZIP algorithm to do compression, and the base 64 encoding mode to provide e-mail compatibility. The actual operation of PGP consists of four types of services: authentication (digital signature), confidentiality (message encryption), compression, and email compatibility. As for what method to be used to implement PGP does not require absolute unity. That is to say you can do digital signature through RSA/SHA or DSS/SHA, and CAST, IDEA, 3DES or AES can be done in PGP in data encryption. So PGP is the encryption method, and also the encryption model.

Through the study and research of PGP model, I found that PGP encryption method can be applied to any place you want to encrypt. The small system I do is a simple simulation that demonstrates the use of PGP encryption to the strings, the local files, the security of network informations. String module demo PGP encryption and decryption process in detail;file encryption module use PGP technology to protect local file security; secure chat module uses P2P technology to achieve a simple network chat, and use PGP technology to messaging process, to ensure the parties information security.

Key words: E-mail; PGP; digital signature; information security

第 1 章 绪论

1.1 研究背景

现今计算机技术已经涉及到各行各业的方方面面，已经成为我们生活中最重要的部分之一。然而网络系统作为计算机技术的核心，在最开始设计的时候并未考虑到安全性的问题。随着计算机网络的发展，网络中的安全问题也日趋严重。最近 20 年计算机应用技术和通信技术的快速发展，使得大量的敏感和重要的信息通过互联网进行信息传递，例如：银行账户、支付宝账户、个人电子档案信息、电子作品等。并且针对网络的攻击方式可谓是层出不穷，只有你想不到的没有攻击者办不到的。常见的攻击方式有口令入侵、特洛伊木马、WWW 欺骗、电子邮件攻击、节点攻击、网络监听、黑客软件、安全漏洞、端口扫描等。这些行为的增加，给信息安全提出了极大的挑战[1]。

在今天，信息量剧增，信息安全已经成为一个国家，一个企业团体保持领先优势的重要因素。当我们想要把我们重要的信息资源通过网络传递共享，或者去换取交易，又或者仅仅是需要保密通信，这个时候密码学理论与技术是你最有力的“武器”。当网络中的用户来自社会的各个阶层与部门时，大量在网络中存储和传输的数据就需要保护。怎样保护信息，不让有用信息被窃取、篡改和破坏成为信息安全领域普遍关注的问题，使用密码学的方法处理这个问题就是最主要的途径[2]。

密码学是研究编制密码和破译密码的技术科学。我们来定义一些术语。原始的消息为明文，而加密后的消息为密文。从明文到密文的变换过程被称为加密；从密文到明文的变换过程被称为解密。研究各种加密方案的领域被称为密码编码学。这样的加密方案被称为密码体制或密码。不知道任何加密细节的条件下解密消息的技术属于密码分析学的范畴。密码分析学即外行所说的“破译”。密码编码学和密码分析学统称密码学。密码编码学具有三个主要的特征：转换明文为密文的运算类型（代替和置换）；所用的密钥数（一个对称密码，两个非对称密码）；处理明文的方法（分组密码和流密码）。密码分析学：密码分析学攻击依赖于算法的性质、明文的一般特征或某些明密文对。这种形式的攻击企图利用算法的特征来推导出特定的明文或使用的密钥。穷举攻击：攻击者对一条密文尝试所有可能的密钥，直到把它转化为可读的有意义的明文。平均而言，获得成功至少要尝试所有可能密钥的一半[3]。

20 世纪 70 年代公钥密码产生之前，当时学术界主要主要局限于设计和分析密码体制（一般称为密码系统）。公钥密码密码体制提出后，人们开始研究考虑数字签名和抵抗攻击的因素，开始构造不能伪造的数字签名系统和能够抵抗欺骗的协议[4]。PGP 正是基于这样的想法研发出来的加密模型，其结合了对称和非对称加密算法的优点，通过对称加密算法对压缩后的消息内容进行加密，然后用非对称加密对其会话密钥进行加密，形成加密数字信封，发送到接收方。接收方接收到加密的信封后先利用非对称密钥对其会话密钥解密，然后再利用解密后的密钥解密消息内容的本身，获取消息原文[5]。

计算机信息网络化发展给社会的发展繁荣带来了很大的促进作用，计算机网络日益影响社会和人们生活的各个方面，已经不单只是起初单纯的在军事上的应用和在学术研究的应用，现如今网络更多的应用在政府信息门户，办公政务、海关联网信息沟通，信息管理、商业领域的电子商务、利用网络点歌，商务连锁管等方面[6]。网络信息化得思潮也在向其他行业和领域不断渗透，有些领域的，例如传统的制造领域，他们生产的产品需要一般有生产、分配、流通、消费四个基本的环节，他们的信息系统管理也要根据实际生产配套设计四个系统相对应，在四个系统进行信息沟通和交互的时候就存在信息的保密和认证的过程，因此要是没有一个安全的基础网络通信设施加以保证的话，用户获得的信息可用性将会大打折扣；再加上我们现在使用的互联网是一个开放的，互联的网络系统，给某些不怀好意的人，可能为了个人的一己私利做出损人利己的事；正因为如此，将导致网络受到人为攻击，他们会出于各种不同的目的信息窃取、攻击正常用户的网络和破坏别人的正常的网络办公和网络生活的事时有发生[7]。用户被黑客攻击事故频频发生，给用户带来的经济损失数额越来越大，因为经济利益攻击用户的事发生的频率越来越高；并且，计算机网络化的应用已经深入渗透到关乎一个国家的发展体制的金融系统、商务活动、国防工业等等核心领域，它的安全性越来越更一个国家、政府、企业以及我们每一个人的切身利益息息相关。

1998 年 3 月，第一个由中国人自己开发的免费邮件系统在丁磊和陈磊华的努力下诞生。这第一套免费邮件系统很快被丁磊挂在 163.net 上供中国当时的网民免费使用，并在当年年底就拥有了 40 万用户。电子邮件的应用除个人外，包括在中小型企业、大型集团公司，以及政府、军工等这些国家级事业单位，都有广泛的应用，也就是我们熟知的企业邮箱，它大大的提高了办公效率与协同工作的效率，包括使用统一的域名作为邮件地址的后缀域名，不仅提升了自身的形象，而且也有利于管理者的监督，起着必不可少的作用[8]。

随着电子邮件的发展，人们渐渐发现了一些致命的问题。有调查显示，有 70%的企业担忧电子邮件沦为泄密管道，致使机密资料误入他人之手[9]。此外，更有半数的员工承认曾经在工作时不慎将不雅或机密的电子邮件错送给他人。然而在政府、军工等国家高级机关也存在同样的安全隐患。

在过去五年当中，电子邮件用户和公司所面临的安全风险变得日益严重。病毒、蠕虫、垃圾邮件、网页仿冒欺诈、间谍软件和一系列更新、更复杂的攻击方法，使得电子邮件通信和电子邮件基础结构的管理成为了一种更加具有风险的行为。可能发生许多身份被窃的事件，结果将导致知识产权受到侵害和个人信息（如信用卡号和社会安全号）丢失。这些问题以及电子通信的成功促使了电子邮件安全协议的研究与发展。

1.2 国内外研究现状

我国互联网发展迅速，电子邮件作为常用的信息交流工具，其发展也十分迅速，我国的电子邮件安全的现状表现为：

电子邮件安全技术的重点主要集中于军事、科研、金融等传统的保密要求较高的部门，一般的企业、机构、政府机关单位和个人用户相对弱一些；在安全性建设上，对硬件的安全性投入较高，而对互联网安全策略、操作安全等建设的力度要欠缺一些；在安全发展方向上，侧重于技术的研发，而对邮件用户的安全意识的培养还没有足够地形成；在安全意识方面，对病毒入侵、邮件丢失、信息泄密等安全问题研究很深入，但对垃圾邮件的危害宣传还不足[10]。

在选择邮件安全技术产品时主要侧重于产品的安全技术指标，即主要参考其性能、价格、工作效率和带宽等因素，而对于产品与用户的融合度考虑得很少，对于适用性、个性化需求方面的要求较低。相关的信息安全法律法规还有待完善，用户的法律意识还有待进一步地培养。

为保证电子邮件的安全，必须加强电子邮件的安全防范。事实上，国内外计算机专家对电子邮件的安全性都给予了广泛的关注，开展了大量工作，也取得了丰硕的成果，提出了各种安全电子邮件解决方案，如在电子邮件系统中引入数字证书，建立各种加密邮件协议和标准，研究邮件防病毒技术，垃圾邮件过滤技术等[11]。同时不少国家都出台了电子邮件应用相关的法律法规，如电子签名法、反垃圾邮件法等，对其进行约束和规范。

在理想状态下，电子邮件因该遵循统一的标准，所有的邮件开发者和厂商都应该严格执行它。目前 Internet 上有两套成型的安全邮件标准：PGP 和 S/MIME[12]。

PGP（Pretty Good Privacy）是 Phillip Zimmerman 在 1991 年提出来的，它既是一种规范也是一种应用，已经成为全球范围内流行的安全邮件系统之一。

PGP 的特点是通过单向散列算法对邮件体进行签名，以保证邮件无法修改，使用对称和非对称密码相结合的技术保证邮件体保密且不可否认，可以支持 1024 位的公开密钥与 128 位的传统密钥加密，达到军事级别的标准，完全能够满足电子邮件对于安全性的要求。通信双方的公钥发布在公开的地方，如 FTP 站点，而公钥本身的权威性则可由第三方（特别是收信方信任的第三方）进行签名认证。在 PGP 系统中，信任是双方之间的直接关系，或通过第三者、第四者的间接关系，但任意双方之间都是对等的，整个信任模型构成网状结构[13]。最近，基于 PGP 的模式又发展出了另一种类似的安全电子邮件标准，称为 GPG（Gnu Privacy Guard）。

S/MIME（Secure/Multipurpose Internet Mail Extension）同 PGP 一样，S/MIME 也是利用单向散列算法和公钥与私钥相结合的技术保证邮件保密且不可否认。与 PGP 不同的主要有两点：S/MIME 的认证机制依赖于层次结构的证书认证机构，所有下一级组织和个人证书均有上一级组织负责认证，根证书相互认证，整个信任关系是树状的；S/MIME 将信任的加密签名后作为特殊的附件传输[14]。

1.3 研究内容与成果

本文首先介绍了信息安全的现状与密码学的基本概念，并简要介绍了电子邮件安全的现状以及常用的安全解决办法，还阐明了研究电子邮件加密的意义。其次，针对 PGP 中用到的密码学基础知识，AES 加密算法的加解密原理，RSA 的算法原理，安全 Hash 函数 SHA，以及数字签名的概念。之后详细描述 PGP 模型的原理细节。最后用一个简单的模拟程序实现上述原理的在字符串、本地文件以及网络中的应用。通过该应用来显示 PGP 的保密性和认证性，以及如何在具体的实用中保护自己的信息安全。

第 2 章 密码学基础知识

PGP 模型运用了多种密码学的基本方法，如 AES、DES、RSA、SHA 等，所以本章将 PGP 实验用到的基础知识做一个简单的介绍。

2.1 对称加密算法 AES

AES 是一种分组密码，其分组长度为 128 位，密钥长度为 128 位、192 位或 256 位。AES 进行了多轮的变换和置换操作，其中每轮由 4 个单独的运算组成：字节代替变换，行移位变换，列混淆变换，轮密钥加变换。该算法输入分组、输出分组与状态长度均为 128 位[15]。

AES 的总体过程如图 2-1：

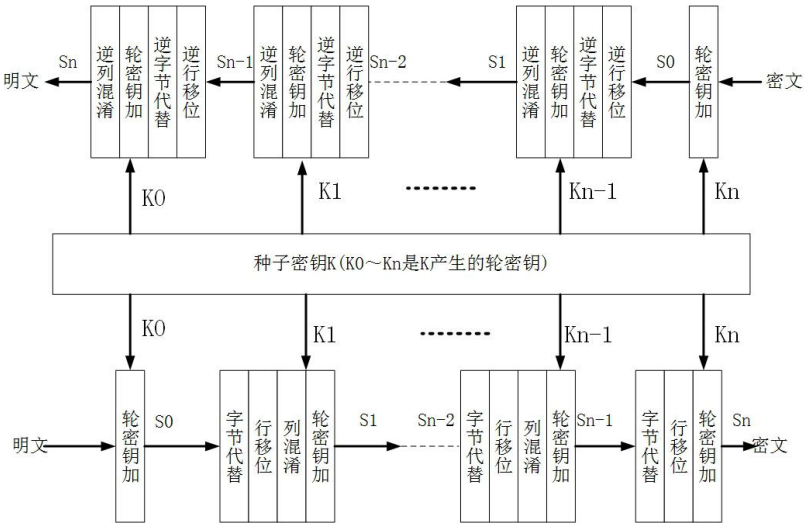

图 2-1 AES 总体变换

其中的轮数是根据密钥长度设定的（密钥长度 128 位，轮数 N=10；密钥长度 192 位，轮数 N=12；密钥长度 256 位，轮数 N=14）

字节代替变换:是一个基于 S 盒的非线性置换，它用于输入或中间态的每一个字节通过一个简单的查表操作，将其映射为另一个字节。映射方法是：把输入字节的高 4 位作为 S 盒的行值，低 4 位作为列值，然后取出 S 盒中对应行和列的元素作为输出。例如，输入为“89”(十六进制)的值所对应的 S 盒的行值为“8”，列值为“9”，S 盒中相应位置的值为“a7”，就说明“89”被映射为“87”。

行移位变换：移位变换完成基于行的循环移位操作，即行移位变换的作用在中间态的行上，第 0 行不动，第 1 行循环左移 1 个字节，第 2 行循环左移 2 个字节，第 3 行循环左移 3 个字节。

列混淆变换：列混淆变换实现逐列混淆，其方法是：

$$s'(x) = c(x) \cdot s(x) \bmod (x^4 + 1) \tag{2-1}$$

其中，$c(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\}$，$\{x\}$内的数表示是字节。

用矩阵表示为

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \tag{2-2}$$

轮密钥加变换：轮密钥加变换用于将输入或中间态 S 的每一列与一个密钥字 W[i] 进行按位异或，其中，$W[i](i = 0,1,\cdots,4(N_r + 1) - 1)$ 由原始密钥通过密钥扩展算法产生[16]。

2.2 公钥密码算法 RSA

RSA 是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。当时他们三人都在麻省理工学院工作。RSA 就是他们三人姓氏开头字母拼在一起组成的[17]。

RSA 是被研究得最广泛的公钥算法，也是目前最优秀的公钥算法之一。这种算法是第一个能同时用于加密和数字签名的算法，理解与操作起来也简易。RSA 的安全性依赖于大数的因子分解，但并没有从理论上证明破译 RSA 的难度与大数分解难度等价。

RSA 的缺点主要有：分组长度太大，为保证安全性，n 至少也要 600 bits 以上，使运算代价很高，尤其是速度较慢，较对称密码算法慢几个数量级；且随着大数分解技术的发展，这个长度还在增加，不利于数据格式的标准化。产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。

RSA 算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对密钥，使用其中一个加密，则需要用另一个才能解密。

RSA 算法涉及三个参数，n、e1、e2。

其中，n 是两个大质数 p、q 的积，n 的二进制表示时所占用的位数，就是密钥长度。e1 和 e2 是一对相关的值，e1 可以任意取值，但是要求 e1 与*(p-1)*(q-1)*互质；再选择 e2，要求*(e2*e1)mod((p-1)(q-1))=1*。

（n 及 e1），（n 及 e2）就是密钥对。

RSA 加解密的算法完全相同，设 A 为明文，为密文，则：*A = B^e1 mod n；B=A^e2 mod n* ；

e1 和 e2 可以互换使用，即 *B = A^e1 mod n* ； *A = B^e2 mod n* ；

RSA 的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 就一定需要作大数分解。假设存在一种无需分解大数的算法，那它肯定可以修改成为大数分解算法。

一般来讲，不管是从软件还是硬件上实现。RSA 最快的情况也比 DES 慢上好几倍，其主要原因是 RSA 算法进行的都是大数计算。因此，速度成为 RSA 的主要缺陷。少量的数据加密比较适合使用 RSA。

到目前为止，由于 RSA 的可靠的安全性，以及它可以方便的实现等优势，RSA 已被用作 PGP 加密的一部分[18]。

2.3 密码学 Hash 函数

Hash 函数将可变长度的消息映射为固定长度的 Hash 值或消息摘要。Hash 函数具有这样的特点：对于大的输入集合使用该函数，产生的结果均匀地分布且看起来随机。

在安全应用中使用的 Hash 函数称为密码学 Hash 函数。密码学 Hash 函数要求如下两种情况在计算上不可行（即没有攻击方法比穷举攻击更有效）：（a）对预先指定的 Hash 值找到对应的数据块(单向性)；（b）找到两个不同的数据块对应相同的 Hash 值（抗碰撞性）。由于这样的特点密码学 Hash 函数的常见应用有：消息认证（验证消息完整性的一种机制或服务）、数字签名、产生单向口令文件、入侵检测和病毒检测等。

近年来，安全 Hash 算法（SHA）是使用最广泛的 Hash 函数。事实上，由于其余的被广泛应用的 Hash 函数被发现存在安全性缺陷，从 2005 年以来 SHA 或许是这几年中仅存的 Hash 算法标准。SHA-1 产生 160 位的 Hash 值。2002 年，NIST 发布了修订版的 FIPS 180-2，其中给出了三种新的 SHA 版本，Hash 值长度依次为 256、384 和 512 位，分别称为 SHA-256、SHA-384 和 SHA-512。这些算法被称为 SHA-2[19]。

SHA-512 是 SHA-2 中安全性较高的算法，主要由附加填充位、附加长度、初始化 Hash 缓冲区和单位处理消息等部分组成，初始值和中间运算结果由 8 个 64 位移位寄存器组成 。SHA-512 输入长度任意位 X,(X 不大于 2^128 位)，输出是 512 位的消息摘要，输入的消息以 1024 位的分组为单位进行处理。

消息填充：填充消息使其长度模 1024 与 896 同余（即长度=896（mod 1024)），即使消息已经满足上述长度要求，仍然需要进行填充，因此填充位数在 1——1024 之间，填充由一个 1 和后续的 0 组成。

附加长度：在消息后附加一个 128 位的块，将其视为 128 位的无符号整数（最高有效字节在前），它包含填充前消息的长度。

初始化 Hash 缓冲区：Hash 函数的中间结果和最终结果保存于 512 位的缓冲区中，缓冲区用 8 个 64 位的寄存器表示，并将这些寄存器初始化为：前八个素数取平方根，取小数部分的前 64 位。

单位处理消息：算法的核心是具有 80 轮运算的模块。每一轮都把 512 位缓冲区的值作为输入，并更新缓冲区的值。每一轮有一个基于置换的轮函数和一个附加的常数。轮常数的获得是由对前 80 个素数开立方根，取小数部分的前 64 位。

2.4 PGP 加密技术介绍

2.4.1 PGP 描述

PGP（Pretty Good Privacy）是目前最流行的一种加密软件，它是一个基于 RSA 公钥加密体系的邮件加密软件。我们可以利用它对邮件保密以防止非授权者读取邮件内容，它还能对用户的邮件加上数字签名，使得邮件具有明确的个人身份信息。因为它采用了非对称的“公钥”和“私钥”加密体系，即使从未见过的人通信，之前也并不需要任何保密措施的来传递蜜钥[20]。

PGP 是个混合加密算法，它是由一个对称加密算法（IDEA）、一个非对称加密算法（RSA）、一个单向散列算法（MD5）以及一个随机数产生器（从用户击键频率产生伪随机数序列的种子）组成的，多种算法在 PGP 实现的过程中组合使用，都是 PGP 不可分割的组成部分，因此 PGP 不是一种完全的非对称加密体系。它集中的集中加密算法的优点，使它们彼此得到互补，这也是 PGP 算法得到大家认可，并且非常流行的原因。

2.4.2 PGP 加密的工作流程

PGP 加密的工作流程如图 2-2 所示。首先，PGP 采用 MD5 单向分解函数生成明文的单向分解值，并用 RSA 数字签名，发方密钥也进行 RSA 数字签名，把它们和明文信息合并后，再进行 ZIP 压缩。然后用户的击键序列产生随机密钥，一方面使用 IDEA 算法加密 ZIP 压缩的结果；另一方面，随机密钥和发方公钥也进行 RSA 加密，把两个加密结果合并后进行编码，即生成最终的密文。接收方收到消息后，先用自己的私钥解开密文得加密信息和加密的随机密码，再利用 RSA 解密得随机密钥，用此密钥解密 IDEA 加密信息得到的压缩结果，解压后，就可以得到签名和明文消息。此时，用 MD5 单向分解函数生成明文得单向分解值，用 RSA 算法和发方公钥对签名解密把解密结果与明文单向分解值对比，如果两者无差异，则表明发方签名和消息都是真实的[21]。

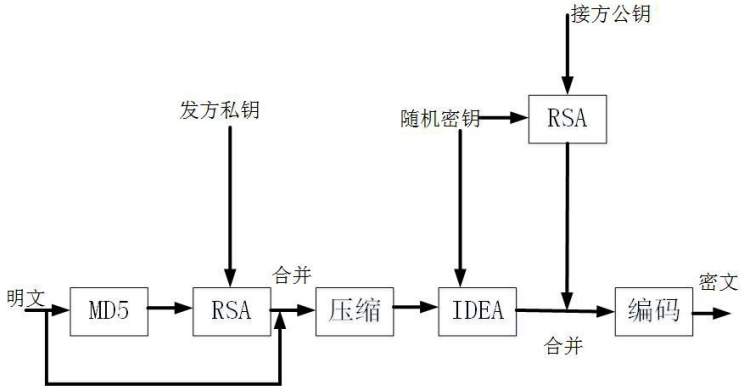

图 2-2 PGP 加密流程

2.4.3 用于加密电子邮件

PGP 发送加密信件的内部过程如图 2-3：

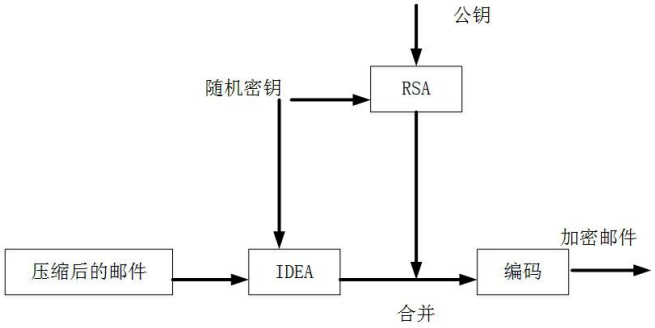

图 2-3 PGP 加密内部过程

首先，钥匙管理模块根据用户输入的收信人标示信息，找到收件人的公开密钥。随机数发生器产生只使用一次的 128 位会话密钥。IDEA 算法用这个 128 位的会话密钥对明文信件进行加密，生成密文信件。另一方面，RSA 算法用收件人的公钥对随机数发生器产生的 128 位的会话密钥进行 RSA 加密。最后，PGP 把 RSA 加密后的会话密钥和 IDEA 加密后的明文信件合并在一起，形成一个新的文件。需要说明的是，PGP 每次加密都使用一个随机的会话密钥。每一次使用不同的会话密钥大大加强了 PGP 系统的安全性。它可以抵抗已知明文和选取明文的攻击。

收件人进行解密处理恢复出信件明文的过程如图 2-4 所示。

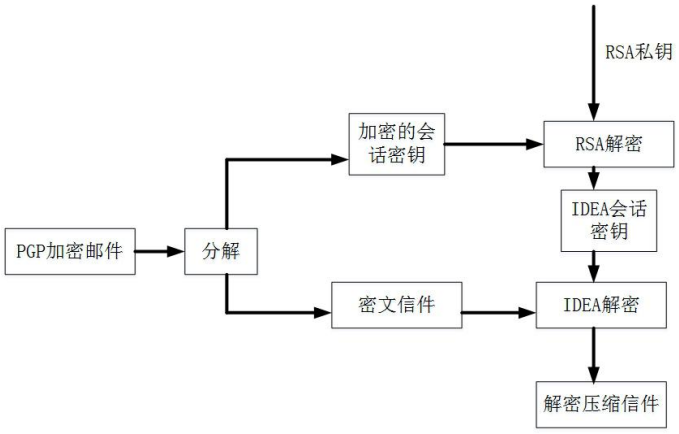

图 2-4 收件人解密流程

2.5 本章小结

本章首先介绍了常用的加密算法，然后有说明了 PGP 的加密原理。为接下来的加解密算法的使用奠定好了基础。

第 3 章 PGP 应用系统设计

3.1 系统需求分析

电子邮件是人们最常用的应用之一。网络环境存在诸多的不安全因素，使得人们强烈的希望深入了解，如何保护我们数据不被别人窃取，如何保护我们的虚拟身份不被冒充，如何去相信我们聊天的对话方确实是本人。不用焦虑和心急，本设计将尝试以最强悍的加密算法来构造电子邮件加密算法 PGP 模型，保证您在网络中的“人身安全”，“财产安全”，“隐私安全”。任何的加解密算法都不能保障绝对的数据安全，但是我们可以在我们能力的范围内做到尽可能的安全。PGP 是电子邮件加密方法，但同时 PGP 也可用于文件加密，以及其他任何你想加密的地方。

虽然社会上的安全产品很多，但我们并不知道实现的原理，也不可能知道软件本身的安全性，主要是加密软件产品要保护自己的知识产权以及软件的安全性。本系统将主要面向大众，希望将这种加密的具体实现方法传递给每个人，使用户明白自己到底是如何实现自己数据的安全的，以及如何利用加解密算法实现自己想要的安全。

本系统的主要目的有：

一、显示电子邮件加密算法 PGP 模型的流程，使用户了解数据是如何加密、认证以及验证身份的，模拟邮件的文本加密；

二、使用电子邮件加密算法 PGP 加密办法实现对本地文件的加密保护，让用户的本地文件安全性上升到 PGP 的高度，模拟邮件的附件加密；

三、给本地文件夹加锁，简单的运用 PGP 来保证文件夹访问的安全；

四、采用 P2P 技术实现一个简单的网络会话聊天，并将 PGP 算法运用到聊天消息的传输中，保证双方会话的机密性，模拟邮件网络通信安全传输。

由于本系统采用的是 SHA-512 安全 Hash 函数，AES 高级加密算法，RSA 非对称加密，这些目前一直是安全性较高的也是使用最广泛的密码学算法，所以技术上的可行性较高，并且安全的保证性也好。

3.2 概要设计

3.2.1 任务概述

设计目标是：保证用户登录注册信息的安全；用户能通过字符串加解密看到加密过程和解密过程的中间数据；用户对本地电脑中的文件（文本、图片、视频等）加密后只有用户加密账户才能解密；对文件夹加锁要保护存储的文件夹密码的安全性；会话聊天过程中要尽可能地减少明文数据的沟通，尽量传送加密后的消息。

开发语言：C#

程序定义：Windows 窗体应用程序

开发工具：Visual Studio 2013 , SQL Server 2008

软件运行要求：本系统要求运行在装有.NET Framework 4.5 及其以上版本的 Windows 7 或 Windows 8 环境中。

3.2.2 总体设计

系统总体运行流程：如图 3-1 所示，用户登录模块用户可以注册、改密、登录；字符串加解密模块可以给用户输入的任意字符串运用电子邮件加密算法 PGP 实现加解密；文件加解密模块，可以提供用户选择任意文件，实现加密成密文文件存储到用户指定的位置；文件夹加锁模块可以让用户自设文件夹锁的密码，实现文件夹加锁解锁功能；安全聊天模块，实现基于 P2P 的安全聊天。以上模块除登陆模块，均有电子邮件加密算法 PGP 提供安全支持。

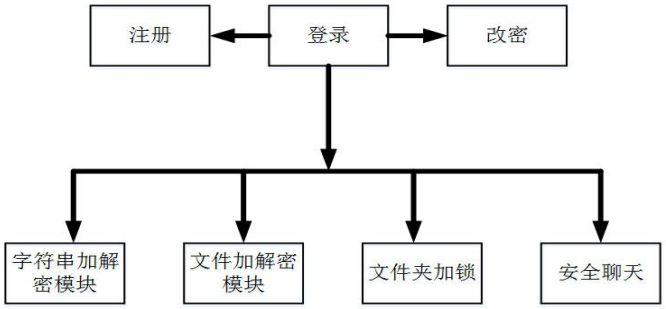

图 3-1 模块分布

系统核心技术：

（1）加解密算法结构。加解密算法采用电子邮件加密算法 PGP 模型，但对加解密的实现略作调整。对称加密算法采用安全强度较高的 AES 加密，本系统所使用的 AES 密钥长度为 32 字节（即 256 位哦）。非对称加密算法 RSA 采用的是 1024 位密钥的，即短消息（二进制值小于 RSA 的 n 值）加密后的密文长度为 1024 位（128 字节）。这

点很重要，因为这样固定长度，在解密时很容易分离出会话密钥。Hash 函数采用了 SHA-512，因为 SHA-1 虽未被完全攻破，但安全性已经降低。

电子邮件加密算法 PGP 加密流程如图 3-2 所示，明文消息 M 经过 Hash 函数 SHA-512 产生消息摘要，用发信人私钥做签名，之后和消息合并一起做一次性会话密钥的 AES 加密，并用收信人公钥加密会话密钥，之后会话密钥的密文和消息密文合并成一个串做基数 64 转换发出消息。（注：基数 64 转换可将任意字节流转变成 64 个可显示字符组成的序列，方便传输和显示，但是缺点是消息长度增加了原来的 1/3）

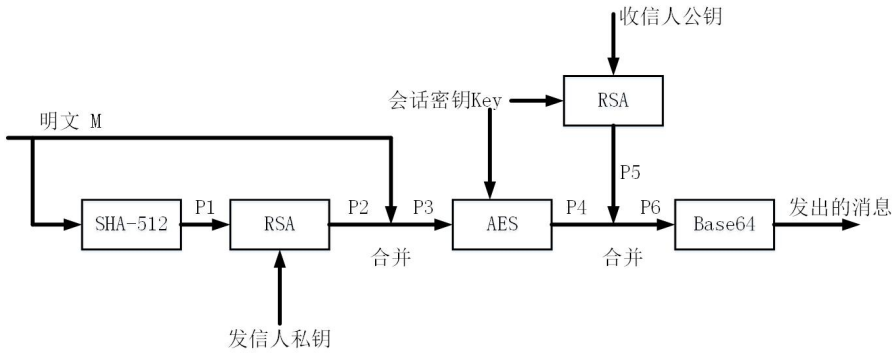

图 3-2 PGP 加密流程

电子邮件加密算法 PGP 解密流程如图 3-3 所示，这个是加密过程的逆过程。首先对收到的消息做基数 64 转换，然后就用到了固定密钥长度的非对称加密，直接取出消息中的前固定位（图中 P5）就是会话密钥加密后的内容。利用会话密钥对密文消息解密后生成(图中 P3)明文的消息和消息签名。消息签名利用对方的私钥加密，所以也很容易分离出，再利用发信人的公钥解密。同时对消息明文再次使用 SHA-512 生成消息摘要，和解密出的摘要比较验证消息的完整性。并且通过公钥的身份认证出对方的真实身份，这个身份保证了消息来源的可靠性。

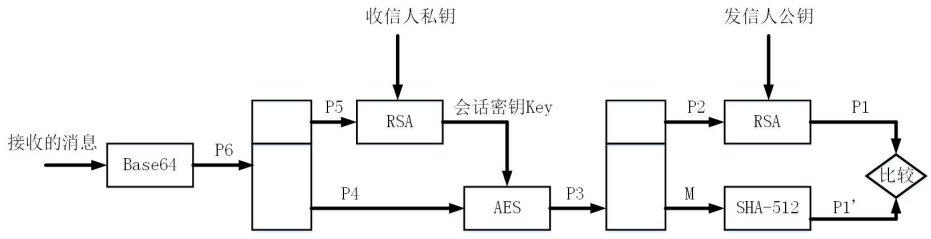

图 3-3 PGP 解密流程

对本系统使用的 RSA 密钥做简单的说明。由于系统要求对本地文件加解密（即发信方与收信方均为本用户），故本系统每个用户拥有两对 RSA 公私钥对，一个做解密一个做加密。

（2）用户账户安全的分析。不论是字符串、文件、文件夹还是聊天，所有的安全性都在于用户账户的安全。如果攻击者拿到了用户的 RSA 公私钥对，那么所有的安全性都将不复存在。或者拿不到公私钥对，而是想办法弄到了账户的密码（如穷举、攻击数据库、读取运行时内存信息、监控用户键盘等）。那么，用户的秘密也将公之于众。也许还有其他更加强劲的手段，我们这里暂时不做讨论。

针对这些问题，本系统的数据是这样保护的如图 3-4 所示。图中的矩形为用户注册时入的数据，中间过程数据或函数操作，椭圆形为数据库中存放的数据。当用户点击注册，用户 ID 和用户密码分别通过 Hash 函数产生两个 AES 对象的 Key 和 IV（初始化值）。然后利用用户 ID 产生的 AES 对象加密用户输入的信息，包括密码，加密之后将密文存放在数据库。即使攻击者攻击数据库也很难找出用户的密码，因为攻击者不知道系统使用的是什么 Hash 函数以及如何安排的 Key 和 IV 的取值。这个过程瞬间进行，用户密码加密后就用密文把原密码覆盖进一步保证安全。用户的两对私钥则通过用户密码产生的 AES 对象做加密，进一步保证安全。用户在数据库中存放的信息，除了用户 ID 和公钥之外，其他数据信息均是密文存放，以此来保障账户的安全性。

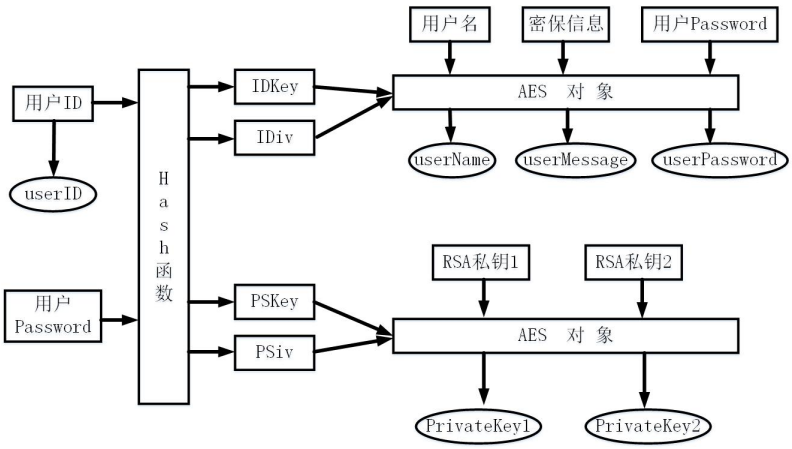

图 3-4 用户注册流程

（3）P2P 技术简介。P2P 技术名叫对等网络，顾名思义通信双方是平等的，“你有的我也有”。当用户量不断增加时，服务器愈来愈吃力，以至于最后崩溃。所以研究人员开始考虑对等网络，让用户机之间共享文件。这种想法遇到非常多的后顾之忧，如：安全，这样的系统中如何保护信息安全？如何抵抗病毒攻击？如何鉴定用户身份？当

然，也有技术方面的问题，如：怎样发现其他客户端的存在？如何定位其他客户端包含的文件块？

这不是本文研究的重点，这里只简单介绍 P2P 体系结构。本系统采用 PNRP 协议解决部分上述问题。PNRP 是由微软公司设计的基于 IPv4 和 IPv6 的点对点协议。它提供了安全灵活的动态名称注册和名称解析协议。和传统的 DNS 协议不同，它不需要一台域名服务器存储域名列表和对应的 IP 地址，而是利用了 IPv6 近乎无限的公网 IP 地址，采用点到点的方式解析域名，可以为任何一台电脑提供一个单独的域名，使你在任何地点都可以轻松访问你的电脑。

3.3 本章小结

本章讨论了电子邮件加密算法 PGP 应用系统的需求分析，并根据需求分析列出了实现的工具以及运行环境等。并介绍了总体的设计思路，使用电子邮件加密算法 PGP 对字符串进行加密模拟邮件文本加密，使用电子邮件加密算法 PGP 对本地文件进行加密模拟邮件附件加密，使用电子邮件加密算法 PGP 保护 p2p 聊天的安全模拟邮件传输安全。以及对用到的关键技术做了详细的解释。

第 4 章 PGP 应用系统实现

根据上一章的设计目标以及提供的技术支持，本章将针对数据库设计，总体结构设计，模块详细设计，以及测试与分析做更为详细的阐释。

4.1 详细设计

4.1.1 数据库设计

根据设计构想，数据库的设计共需三张表分别是：

用户表：User，表中存放用户的个人信息，如用户名，密保信息，密码，登录标志

公钥环：PuKeyRing，保存公钥环提供多用户共享彼此间的公钥

私钥环：PrKeyRing，保存用户自身的私钥同公钥环区分，保护帐户安全

数据库设计的详细如下表 4-1、表 4-2、表 4-3：

表格 4-1 用户信息

列名	数据类型	可否为空	默认值	说明
UserID	Varchar(50)	Not null	无	用户 ID
UserName	Varchar(Max)	Not null	无	用户名（加密）
UserMessage	Varchar(Max)	null	无	密保（加密）
UserPassword	Varchar(Max)	Not null	无	密码（加密）
UserLogin	Varchar(5)	Not null	false	是否已登录

表格 4-2 用户公钥环

列名	数据类型	可否为空	默认值	说明
KeyID	Varchar(100)	Not null	无	公钥 ID
UserID	Varchar(50)	Not null	无	用户 ID
PuKey	Varchar(Max)	Not null	无	公钥
OwnerTrust	Int	Not null	无	用户信任度

表格 4-3 用户私钥环

列名	数据类型	可否为空	默认值	说明
KeyID	Varchar(100)	Not null	无	公钥 ID
UserID	Varchar(50)	Not null	无	用户 ID
PuKey	Varchar(Max)	Not null	无	公钥
EPrKey	Varchar(Max)	Not null	无	私钥（加密）

4.1.2 总体结构设计

本系统使用十个类实现上述目标，大致结构显示如图 4-1 总体设计图所示。图中的箭头相连的表示类或模块之间的调用关系，当然并不是绝对的，但几乎 95%以上的调用都是按照下图中的指示进行的。

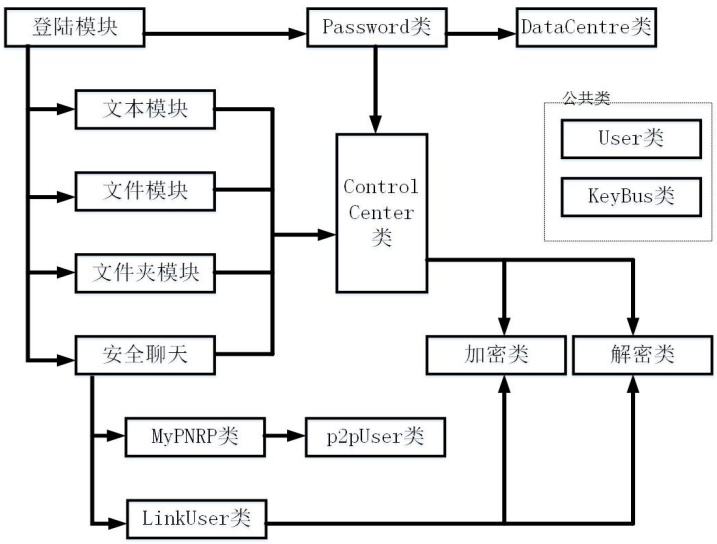

图 4-1 总体设计

其中重要的类有六个是：

加密类（程序中的命名是 EncryptionArithmeticPGP）处理加密操作，程序中所有的 PGP 加密都是该类中的函数完成的。

解密类（程序中的命名是 DecryptionArithmeticPGP）处理解密操作，程序中所有的 PGP 解密过程都是该类的函数完成。

ControlCenter 类全是静态成员变量，主要功能传递参数，程序的每一部分都有或多或少从中获取需要的信息。

Password 类管理着程序中安全性最重要的部分——密钥，用户的注册，获取密钥，等有影响安全的操作全封装在此类中。

DataCentre 类访问数据库管理类，所有的数据库操作全封装在此类中。因为数据库是用户安全的重要堡垒，所以本系统不允许随意一个线程都可以访问数据库。并且几乎所有的访问数据库操作都是 Password 类参与的，所以程序中 DataCentre 类几乎专门为 Password 类服务（如图所示）。

MyPNRP 类又是一个重要的类，它管理 P2P 的注册、检测与解析。

剩余的四个类，主要做辅助功能。KeyBus 类主要功能是传递或暂存密钥；User 类主要功能是传递或暂存用户信息；p2pUser 类主要功能是存储 MyPNRP 类检测出的用户信息；linkUser 类主要功能是存储与本机用户建立 TCP 连接的用户的信息，并承担部分存储加解密信息的功能（如图所示）。

简单来说，就是用户经过登陆模块后就可以自己选择想要使用的模块。这里在主界面里使用了 tabControl 控件、panel 控件两者结合产生了四个模块自由选择的功能，并且各模块代码分开便于管理和维护。主界面如图 4-2；

图 4-2 主界面

4.1.3 模块详细设计

登陆模块：登陆模块分登录、注册和改密三部分。

登录的时候，当用户输入合法的用户名和密码之后，点击登录，首先检测用户名是否已注册，以及密码是否是 8-16 位，不合法则提示用户重新输入。合法之后创建 Password 类的对象（这是建立前面提到的两个 AES 对象），调用其中的 Login 函数。该函数首先将用户输入的密码用用户 ID 产生的 AES 加密，之后与数据库中读出的密码比较。如果

相等则解密私钥，加载公私钥，登陆成功进入主界面。如果不等，则提示用户密码错误如图 4-3 所示。

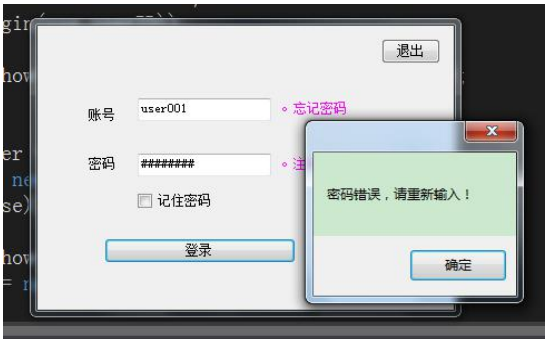

图 4-3 登陆界面及提示

注册部分，进入注册界面自动生成一个当前可用的用户 ID。这个个功能通过一个循环检测函数，直到找到数据库中没有注册过的 ID 把它显示出来。之后用户需要完善信息，点击注册时检测的信息有 ID 是否合法（因为本系统允许用户自定义）、用户名不能为空、密保信息不能为空、密码长度是否合适和两次密码是否一致等信息。都合法后，生成 Password 类的对象，执行 Password 类里边的 Register 函数，该函数的执行参看第三章总体设计中用户帐号安全的分析。

改密部分，首先要求检测账号是否为注册账号，之后要求用户填写用户名和密保信息。通过 Password 类的 Censor 函数检查用户名和密保信息是否均正确，只有两者都正确的时候才能进行下一步。检查方法和登录时密码的检测方法一样，不对数据库中的信息解密，而是对用户的输入加密之后和数据库比较。当用户通过检测，就可以输入新的密码，这是其实改密一定成功了。后面系统进行的操作是，在 Censor 检测成功的时候就把用户的原密码读出来了，用原密码对私钥解密，再利用新密码对私钥加密存入到数据库中。

字符串加密模块：点击加密按钮就调用加密类对用户输入的字符串加密，并显示加密后的密文，模拟邮件文本加解密。点击加密详情可以查看全部的中间过程生成的数据。解密和解密详情类似。加解密算法内部实现第三章已进行了详细的阐述。效果如图 4-4；

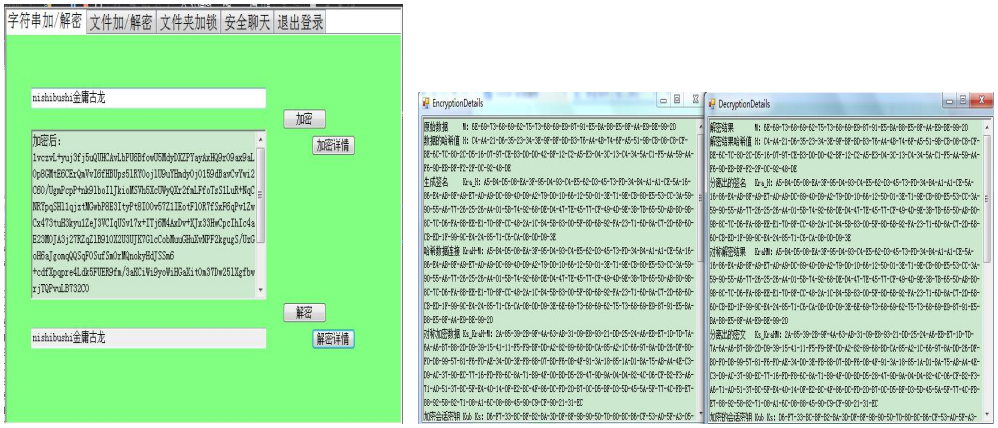

图 4-4 字符串加密界面及中间数据显示

文件加解密模块：这个模块主要是调用了 C#的库函数 FileStream 类里边的对二进制数据的读写操作。首先把读到系统中的文件的二进制数据经过加密类加密，然后再写到指定的文件中，模拟邮件附件加解密过程。并把加密结果显示出来，效果显示如图 4-5。解密过程类似，只不过是加密类变成了解密类。

图 4-5 文件加解密

文件夹加锁模块：这个模块的技术原理是根据微软提供的文件夹特殊后缀实现的，其实就是把文件夹的后缀改了。这个可能没注意过，文件夹也是可以有后缀的，但这个后缀不能通过手工的办法实现。C#中 DirectoryInfo 类中的 MoveTo 方法可以轻松的改掉 DirectoryInfo 对象初始化的文件夹对象的后缀名。改完之后这个文件夹就会呈现相应的状态不能打开。这里找到了四种可用的状态（64 位 Windows 7 测试没问题），文件夹名字后面添加下面的字符串就会显示出相应的效果。

".{2559a1f2-21d7-11d4-bdaf-00c04f60b9f0}";显示一个锁的图标并且手动不能打开该文件夹

".{645FF040-5081-101B-9F08-00AA002F954E}";显示回收站的图标并且双击进入本机的回收站无法看到文件夹内部真实的文件

".{2559a1f1-21d7-11d4-bdaf-00c04f60b9f0}";显示一个蓝背景的问号并且不能打开该文件夹

".{7007ACC7-3202-11D1-AAD2-00805FC1270E}";显示网络适配器的图标并且双击进入网络适配器选择无法看到文件夹内部原来的文件

这个方法很容易就能够被攻击者通过程序的方法强行破解掉。但是这样做也是有意义的：首先可以屏蔽掉一般的攻击者；其次可以做一个警示作用的标志，例如你有许多加密文件，把它们放到一个上锁的文件夹里，可以警示别人这个文件夹不允许一般人访问；还可以与文件加解密模块相结合，实现对文件夹上锁就对文件夹里的内容也加密存储，删除明文文件，双重加密保护。

本系统对这一部分的实现是选择文件夹，系统会自动检测该文件夹是否已经加锁。若未加锁，则将加锁相关的部分的按钮打开使用；若已加锁，则将解锁的按钮打开。关于这个锁本质是向选择的文件夹中加入一个 XML 文件，这个文件中保存用户输入的锁密码的密文（经过 PGP 加密）。当解锁的时候，那个 XML 中的密文读出解密，再与用户输入的密码比较。如果相同则删除 XML 文件，去掉文件夹后缀；如果不同则告诉用户密码错误，然后什么也不做。效果显示如图 4-6：

图 4-6 文件夹模块

安全聊天模块：安全聊天模块首先调用 MyPNRP 类里边的 registerPeer 函数，该函数主要功能是完成本用户 PNRP 注册功能，并开启在注册端口的 TCP 监听功能。创建一个新的线程循环调用 MyPNRP 类里边的 Resolve 函数，该函数每隔 500 毫秒检测一次 PNRP 中的注册用户。如果有新用户则添加新的 p2pUser 对象到 userList 列表中,并在用

户界面显示；如果用户退出，则将其从列表中移除，并在界面移除。同时还开启一个线程，循环监听开启监听的端口，一旦有其他用户连接就与之连接，并添加 linkUser 对象到 linkUser 列表，产生并开启对应的接收数据线程。

当用户在界面点击右边列表中的其他用户时，改变对话窗口上面的显示对话状态的标签，显示用户当前对话的对方用户名。同时如果没有建立连接，则在后台建立与对方的 TCP 连接，此时使用 linkUser 对象中生成的加解密类对象与对方约定密钥。当点击发送按钮，则将用户在输入窗口键入的内容，使用与对方账户约定的密钥加密发送。（注：约定密钥，其实就是告诉对方所使用的加密密钥和解密密钥的公钥 ID。这里并不传递公钥，而只是传递 ID，这也是为了安全考虑）

若用户并没有任何操作，但是有其他用户要与之对话。建立连接的时候双方就会相互约定密钥。只要对方开始发送消息，本用户窗体会自动显示此时的聊天状态，并把对方发过来的消息显示在聊天窗口。效果图显示如图 4-7、图 4-8：

图 4-7 聊天模块 1

此时用户“尚聪”向用户“天空”建立连接，但并未发送消息（即点击右边列表操作）。

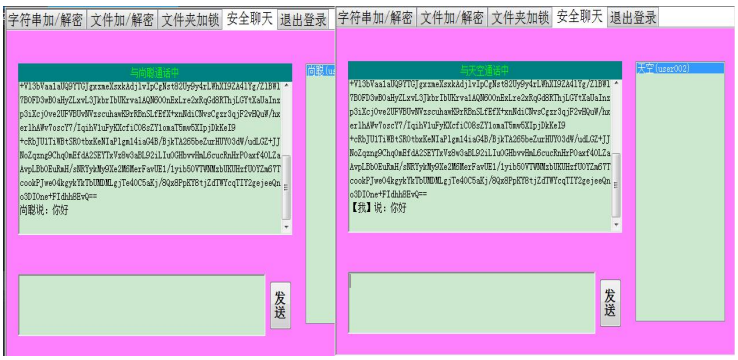

图 4-8 聊天模块 2

此时用户“尚聪”向用户“天空”发送了消息“你好”。效果如图，自始至终用户“天空”未进行任何操作。

4.2 测试与分析

限于客观原因，这里对系统只进行白盒测试。测试用例设计涉及注册、登录、改密、字符串模块、文件模块、文件夹模块、安全聊天模块。为了便于测试和总结，将测试分为两部分：登录前的测试和登陆后的测试。

4.2.1 登录前测试

注册测试：试例一，注册时不填用户 ID，其他信息合法。

试例二，注册时填写注册过的 ID，其他信息合法。（结果显示图 4-9）

试例三，注册时不填用户名，其他信息合法。（结果显示图 4-10）

试例四，注册时不填密保信息，其他信息合法。

试例五，注册时不填密码，其他信息填写合法。

试例六，注册时两次密码输入不一致，其他信息填写合法。

试例七，填写密码时密码长度小于 8，其他信息合法。（结果显示图 4-11）

经过测试以上情况均被系统拒绝注册，并给出了合适的提示。分析结果：符合软件开发要求，用户容错性良好。（试例太多，故仅截图部分以示结果）

图 4-9 试例二

图 4-10 试例三

图 4-11 试例七

登陆测试：试例一，输入未注册的账号。（结果显示图 4-12）

试例二，不输入帐号，直接登陆。（结果显示图 4-13）

试例三，输入长度不够的密码。（结果显示图 4-14）

试例四，登录已经登陆的账号。（结果显示图 4-15）

经过测试系统均决绝以上用户登录，并给出提醒，所以符合目标要求。测试结果如下图：

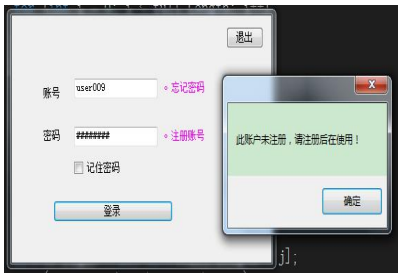

图 4-12 试例一

图 4-13 试例二

图 4-14 试例三

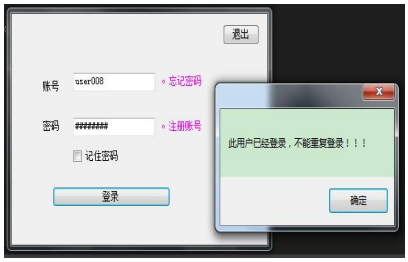

图 4-15 试例四

改密测试：试例一，改密时输入未注册的账号。

试例二，改密时用户名输错，其他信息无误。（结果显示图 4-16）

试例三，改密时密保信息输错，其他信息无误。

试例四，改密时用户名和密保信息均输错。

试例四，改密时输入新密码小与 8 位。

试例五，改密时两次输入密码不一致。（结果显示图 4-17）

经测试上述五种情况，均拒绝了改密的继续，系统符合软件工程的需要。部分试例截图如下：

图 4-16 试例二

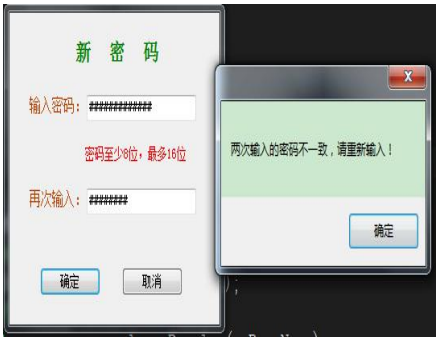

图 4-17 试例五

4.2.2 登录后测试

字符串模块测试：试例一，输入为空加密测试。（结果显示图 4-18）

试例二，重复点击加密测试。（结果显示图 4-19）

试例三，重复点击加密详情测试。

试例四，重复点击解密，解密详情测试。

测试结果输入为空的时候加密会弹出窗口提示；重复点击加密重复对相同的数据再加密一次；重复点击加密详情和解密详情会弹出多个详情窗口，但只有第一个拥有中间数据；重复点击解密，会不断地重复解密相同的内容。

分析：虽然有些地方不如尽如人意，但整体上没有太大问题。软件测评合格。

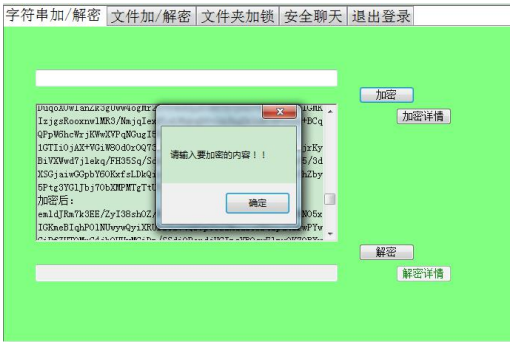

图 4-18 试例一

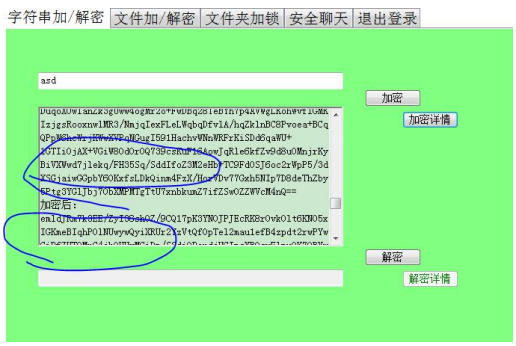

图 4-19 试例二

文件加解密模块测试：

试例一，未选择加密文件直接进行加密。

试例二，选择了加密文件未指定加密后文件的存储路径。（结果显示图 4-20）

试例三，加密后文件的存储路径指定不正确。（结果显示图 4-21）

测试结果试例一与试例二均给出了合理的提醒，但是试例三测试出错，用户不能输入错误的路径进行文件加解密。

分析：程序容错性出了问题，不符合标准，需要改进。软件测评不合格。

图 4-20 试例二

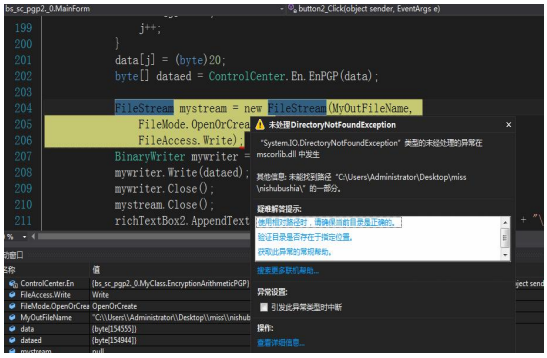

图 4-21 试例三

文件夹加锁模块测试：

试例一，选择一个未上锁文件夹加锁，之后尝试打开文件夹。（结果显示图 4-22）

试例二，选择一个已经上锁的文件夹输入错误密码解锁。

试例三，对上述两种方法运用各种锁都是一次。

经过测试软件实现了上述试例的测试，四种锁都没问题与目标描述一致。

分析：符合软件工程的设计构想。软件测评良好。

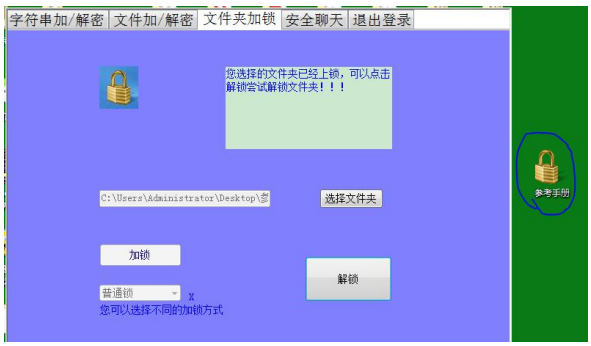

图 4-22 试例一

安全聊天模块测试：

试例一，未选择聊天对象，点击发送消息。（结果显示图 4-23）

试例二，输入窗口为空的情况下，点击发送消息。（结果显示图 4-24）

试例三，三个聊天者相互对话测试。（如，1 对 2 说，2 对 3 说，3 对 1 说）（结果显示图 4-25）

经过测试为选择聊天对象点击发送按钮，会弹出提示消息。输入为空的情况下，仍然将空消息加密发给对方。三者相互聊天，经测试符合系统设计的目标，三者之间不会混乱。每次发送的都是联系人里选中的对象，每一次收到消息，窗口的聊天对象都会转向消息来源方（即右边联系人被选中）。

分析：发送消息的输入框没有检测是否为空，除此之外其他测试都是合格的。

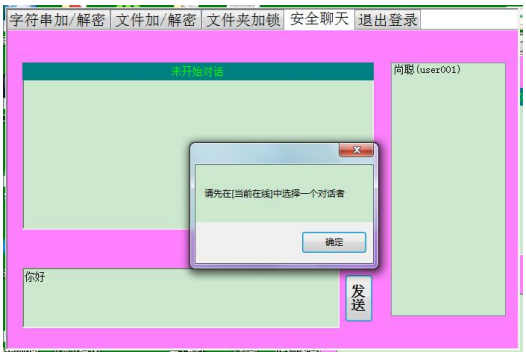

图 4-23 试例一

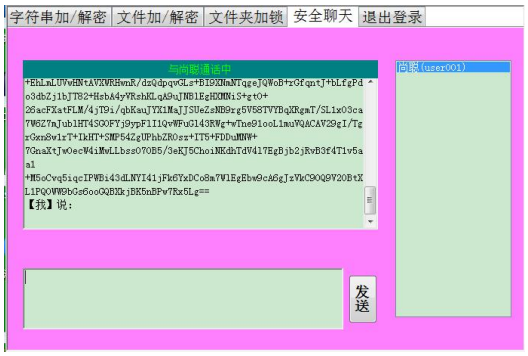

图 4-24 试例二

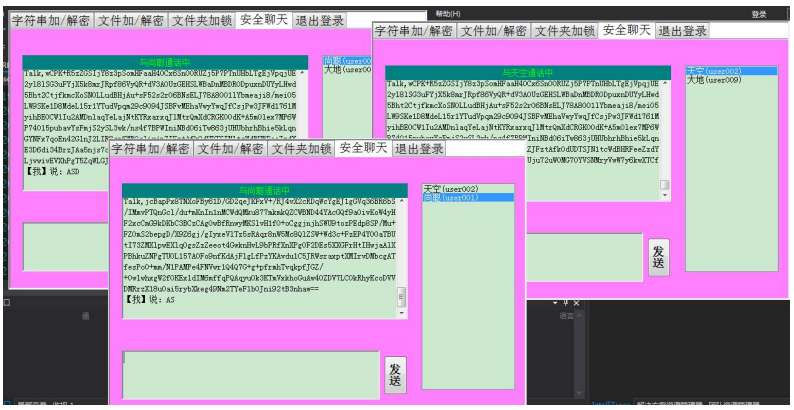

图 4-25 试例三

4.2.3 测试结果总体评价

经过多组针对性测试，确实发现了一些不足之处，也有错误存在。本次测试，登录模块无错误，字符串模块有重复加解密的问题，文件模块有不能容错的情况，文件夹模块无问题，安全聊天模块有发空消息的问题等。

4.3 本章小结

本章详细地说明了，电子邮件加密算法 PGP 系统的总体设计以及各个模块的详细设计。电子邮件正文加密，电子邮件附件加密，电子邮件传输安全，三方面全方位保证

了电子邮件使用中的安全性。根据本设计经过编码后很容易就实现了测试中的效果。测试结果显示了程序健壮的一面，但也表露了不足之处，有待进一步完善。

第 5 章 总结与展望

设计基本实现了电子邮件加密算法 PGP 的加解密过程，加密类与解密类为各个模块提供了统一的加密标准。根据电子邮件加密算法 PGP 的加解密模型，运用 RSA、AES 以及 SHA-512 等当前应用最广泛的密码学算法，所以安全性是有保证的。功能模块分为字符串模块、文件加解密模块、文件夹加锁模块和安全聊天模块，分别实现了邮件文本加密保护、邮件文件保密、邮件网络信息安全的功能。本系统这样的设计，一方面展示了电子邮件加密算法 PGP 的强大功能，PGP 加密的思想方法可以用于希望保护的任何地方；另一方面向用户展示了信息安全在计算机各个方面的表现，并且确实做到了对各种数据的保护。另外，设计本身也细节之处体现着安全，如用户信息的加密保护。总体上来说这个设计是完整的。更加安全的数据处理方法、更加简洁美观的界面设计思路等，限于编者能力原因，暂时还没有实现。尽管设计在实现上存在着这些不足，但是电子邮件加密算法 PGP 的思想的展示以及基本目标功能的实现是完美的。

经过本次设计，熟悉了常见的加密算法的基本原理，并能够运用这些算法做一些简单的加解密操作。深入了解了电子邮件加密算法 PGP 的实现与应用。对计算机安全有了一个新的认识。

相信随着技术的发展，社会意识也会不断变化，用户的安全性会一步步地提高。但是不排除各种攻击者的技术也在不断的提高，所以未来每个人都要学点信息安全，毕竟全民的安全意识的提高才是安全性真正的提高。保护安全的人与破坏安全的人是一对矛盾，但破坏者具有主动出击的优势。如果保护着没有绝对的实力让攻击者望而却步，那么保护着面对的将是自己的“安全地带”，被一步一步的蚕食的悲惨命运。所以研究密码学保护信息安全必须成为全民的行动，才能抵抗一次又一次来自攻击者的“出击”。

参考文献

[1] 马俊. C#网络应用编程（第 2 版）[M].北京: 电子工业出版社, 2010.244-311

[2] 斯托林斯. 密码编码学与网络安全: 原理与实践: 第5版[M].北京: 电子工业出版社,2012.404-436

[3]冯伟.大数据及其安全的产业纵深[J].信息安全与通信保密,2014(10):20-30

[4]郑瑞梅.浅谈加密技术的方法及应用[J].信息技术,2005(5):57-58

[5]杨柳.密码学在网络安全中的应用[J].通讯世界,2016(1):216-258

[6] Jay Glynn. C#高级编程[M]. 北京: 清华大学出版社, 2014.1393-1408

[7]廖蓉晖.DH 密钥体制在 VoIP 通信中的应用[J].通信技术,2015(03):367－370

[8]蔡俊辉,张晓云.电子邮件安全性分析[J].电脑知识与技术,2010(5):823-1826

[9]高建华.电子邮件安全技术研究[J].网络安全技术与应用,2006(5):50-52

[10]杨丽丽.PGP 在电子邮件安全中的应用[J].太原城市职业技术学院学报,2009(5):150-151

[11]祝凯捷.密钥安全及其在虚拟化技术下的新发展[J].密码学报,2016(1):12-21

[12]刘雅丽.PGP 保护电子邮件的研究[J].孝感学院学报,2005(5):78-85

[13] 王天芹. 密码理论与技术[M]. 开封: 河南大学出版社, 2010.78-116

[14]邹伟,张智.树形异步即时通信密码协议的研究[J].通信技术,2016(1):87-91

[15]郑瑞梅.浅谈加密技术的方法及应用[J].信息技术,2005(5):57-58

[16]杨波.现代密码学(第 2 版)[M].北京:清华大学出版社,2010.330-342

[17]谢希仁.计算机网络(第 6 版)[M].北京:电子工业出版社,2014.300-324

[18]李中伟.智能电网信息安全防御体系与信息安全测试系统构建[J].电力系统自动化,2016(40):147-151

[19]林珊,宁国宁,赵之霖.中文分词在邮件过滤系统中的应用[J].华南理工大学,2013(2):35-37

[20]Douglas R Stinson.密码学原理与实践(第二版)[M].北京:电子工业出版社,2003.57-136

[21]Pelzl C.常用加密技术原理与应用[M].北京:清华大学出版社,2012.95-174

致　谢

跟跟跄跄地忙碌了两个月，我的毕业设计课题也终将告一段落。点击运行，也基本达到预期的效果，虚荣的成就感在没人的时候也总会冒上心头。但由于能力和时间的关系，总是觉得有很多不尽人意的地方，譬如功能不全、外观粗糙、底层代码的不合理……数不胜数。可是，我又会有点自恋式地安慰自己：做一件事情，不必过于在乎最终的结果，可贵的是过程中的收获。以此语言来安抚我尚没平复的心。

毕业设计，也许是我大学生涯交上的最后一个作业了。想籍次机会感谢四年以来给我帮助的所有老师、同学，你们的友谊是我人生的财富，是我生命中不可或缺的一部分。我的毕业指导老师王老师，虽然我们是在开始毕设时才认识，但她却能以一位长辈的风范来容谅我的无知和冲动，给我不厌其烦的指导。在此，特向她道声谢谢。

大学生活即将匆匆忙忙地过去，但我却能无悔地说：“我曾经来过。”大学四年，但它给我的影响却不能用时间来衡量，这四年以来，经历过的所有事，所有人，都将是我以后生活回味的一部分，是我为人处事的指南针。就要离开学校，开启研究生之路，这是我人生历程的又一个起点，在这里祝福大学里跟我风雨同舟的朋友们，一路走好，未来总会是绚烂缤纷。

附件：

外文原文

In recent years, information security, network security and cyberspace security have become high frequency words in the non-traditional security field at home and abroad. In the security strategy and policy documents, in the names of appropriate national authorities and in the news reports and the terminology of the theoretical and academic researches, as well as in various related activities, these concepts appear at the same time, but the logic boundaries are not clear. As a result, it is necessary to make an in-depth study in order to reach a clear understanding on the logic starting point of information security research and practice, and form academic norms in the basic theoretical research of information security with the consensus of people inside and outside the concerned field. Based on the recent literature in the field of global information security, in particular relevant policies in various countries, and combined with related practical activities, this paper tries to make certain preliminary discussions on such concepts as information security, network security, cyberspace security and their relationships with each other.

Using comparative methodology, this paper lists the usages of information security in all kinds of literature in 2000-2014 and makes a comparison. It finds that since entering the 21st century, information security has become the focus of national security in all countries. There are both theoretical studies and explorations of state secrets, commercial secrets and personal of information security technology standards and the draft of international codes of conduct. Information security has become one of the most important non-traditional security field concerning the global overall security and integrated security. This paper also analyzes the rich connotation of information security and a series of related concepts, such as information warfare, information sovereignty, information territory and others.

This paper focuses on studying the connection and differences between information security, network security and cyberspace security. Through a comparative analysis of the relevant policy documents and academic research topics, it discovers that the three words, information security, network security and cyberspace security, are often used

interchange-ably or in parallel, but there has appeared the development trend of information security moving towards network security and cyberspace security.

This paper expounds on the fact that information security, network security and cyberspace security have three similar aspects and three different aspects. The similar aspects are: they all belong to the field of non-traditional security; they all focus on information security; and they can be used interchangeably, but with different implications. The different aspects are: they are derived from different backgrounds; they are concerned with different connotations and with different extensions.

In summary, information security, network security and cyberspace security have interrelated aspects, as well as their own unique aspects. Information security can be loosely regarded as related to all kinds of information security issues; net-work security can refer to various types of security issues brought about by the network technology; cyberspace security is specifically related to the problems in the cyberspace, which is one of the five spaces, parallel to the land space, sea space, sky space, and the universal space. 1 fig. 3 tabs. 34 refs.

With the rapid development of the information technology, the information security of the network has been already extremely urgent. In the network, a large amount of information especially stored and transmitted on Internet is threatened with security at any time. E-commerce concerns the business secret of the principal part of e-commerce as one of the valuable sensitive information. So, while relevant units or enterprises carry on the electronic commercial activity, they must solve the network information security issues. This is being implemented or to be implemented in each of the units and E-commerce enterprises must address an important issue. The paper researches the information security technology for E-commerce. In highlighting the basis of the principles of E-commerce security technology, this paper describes the fundamental security issues and solutions of E-commerce applications.

From the E-commerce's concept and security this paper analyses the information encryption technology, the digital fingerprint, the digital signature, the digital time stamp, the digital certificate, the safe authentication agreement, the information hideaway technology and the firewall technology of the use of E-commerce. Finally it proposes the shopping environment and commercial city in Internet of the Jiangsu School Supermarket(Home Market Supermarket) that is constructed by using ASP, SQL the Server database and so on as developing platform. It is an convenient way to the general teacher and student in campus and it solves electronic commerce security problem and has obtained the good effect.

With the rapid development and popular application of network technology, information security becomes more and more important in the construction of electronic government. And the digital signature technique is the foundation and guarantee of the information security. It can be applied to electronic government to offer some services, such as identity authentication service, authority to control service, information privacy service, datum integrality serving and undeniable service, forming a safe environment to electronic government.

This thesis mainly includes five parts to discuss the application of the digital signature technique on the electronic government. At the first, we introduce the definition, principle and wide application prospect of digital signature technique. In the second part, the general digital signature algorithms in digital signature technique are analyzed and compared, and by studying the algorithm we choose the safe and practical algorithm. In the third part, after analyzing the information security of electronic government in China, for the situation of electronic government in our country, we propose a PKI trust model, some application mode of digital signature, and some digital signature schemes. In the fourth part, based on the new digital signature schemes, a system of digital signature is carried out and applied in the electronic government system. It offers effective information safety assurance for electronic government system. Finally, we also give out some future research direction about the application of the digital signature technique in the electronic government according to the present developing status.

With the continuous information of global economy and social development, e-government has become the critical factor to weigh the information level of the society, administration and service capability of government, even the comprehensive national strength. The development of e-government is a process to fully apply advanced information technology and vigorously promote government's affairs to be done from traditional and manufactured to computer-based and automated. However, during the process, security problem has become one of the major factors to cumber the development. Cryptography is the core technique in the field of information security which has been playing an important role in the e-government nowadays. Identity authentication is one of the basic applications of cryptography techniques. Owing to the difficulty and complexity of cryptography system, to comprehensively, deeply and accurately understand and master the cryptography technique applied in e-government system, especially the identity authentication techniques, is of great importance.

In this thesis, we generally introduce the information security techniques used in e-government (especially cryptography techniques), focus on the field of identity

authentication. We summarize first the application and development of information security and identity authentication in e-government system, then analyze the mainstream identity authentication techniques. On this basis, we re-examine, review and deeply probe into the famous Cramer-Damgard Identity Authentication Protocol, point out some security problems in implementation, put forward new security properties identity authentication running concurrently on Internet. For then we design and prove a new protocol category of identification scheme satisfying the proposed security property. What we mentioned above brings benefit and more understanding to the identity authentication profound protocol and accurate especially the identity security of group when it runs currently on the Internet, help conduct to more complete and profound apprehension and analysis on the identity authentication's application in e-government security practise, better achieve applications in security of e-government.

Existing methods provide some level of protection,- better or worse,- yet each of them has significant drawbacks. So far, most current systems and secure protocols have used only three types of cryptographic primitives: encryption, key agreement and digital signatures. More high level tasks, like authentication, are achieved by combining those primitives in some way in a Protocol.

Internet authentication started with pretty basic passwords: a user entered the password in the web-form, password was sent via HTTP to the server, server verified the password and lets the user in. That was in the early days of the small Internet. At that time attackers were limited by having very little experience on how Internet works. Even if some had basic networking knowledge, they did not have equipment, tools or software (which was very expensive at that time) to do the attacks. Also, the attacks themselves were pointless because of the little commercial value of the information which traversed the Internet at that time. Eventually growth of the Internet and availability of the knowledge, software and tools created a first network attacker: HTTP passwords were easily stolen by simplest passive network sniffers and protocol analyzers.

Next step was to change passwords to some values which were useless for passive eavesdroppers: people started hashing the password. Since both server and user had the same password, they could produce identical hashes of those and compare them, with user sending the hash to server. It seemed that attackers couldn't get the password, because reversing a

hash function is computationally “almost impossible”. This solution saved the day… for just a little while! Attackers used two ways to overcome this:

First: many people make their passwords “easy-to-remember”, so they attackers hashed a big set of popular words and by knowing the hash, could easily “lookup” the original password if it happened to be from the produced “dictionary”: a dictionary attack was invented.

Second: even if someone used complex password, attackers just used the hash directly to authenticate with the server with a “modified browser”. They did not enter the password in the form, but injected hash directly to HTTP stream: an active attack was invented.

It was clear now that HTTP traffic had to be encrypted. However, since communicating parties were located far away from each other a key agreement was used and was eventually broken by attackers: man-in-the-middle was proposed.

The history continues: the more sophisticated schemes for protecting the transmission of passwords are proposed, the better and smarter attacks are designed to defeat them. Wouldn’t it be great to avoid transmitting the passwords at all?

Most of engineers who just begin developing cryptographic tools, seem very pleased when they have their first success in turning a piece of data to a random-looking string using some key and recovering the original data. The problem is that most of the engineers stop at this point. As we know from Schneier’s law:

Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break. They think that if the output is indeed random-looking and nobody knows the key, they are safe. So, one can always find low-security encryption schemes, hardcoded keys or initial vectors, improper usage of encryption modes etc. even in production software. And, although your output looks random-like, a sophisticated attacker with proper tools and mathematical background will surely find patterns, side-channel leaks, perform cryptanalysis and eventually will recover the data. Even large companies get into trouble with this, so what makes you special?

Different schemes involving bcrypt, pbkdf2 or any ‘encrypt then compare’ frameworks provide only a fragment of security system instead of complete solution. This does not provide sufficient level of security at all.

Passwords are still widely used in HTTP to give users access to restricted resources. However, despite the long history of updates of authentication protocols, still there is some room for attacks. A security-aware user will never attempt to enter their password on a website, if that website does not provide a HTTPS connection for entering such credentials. This means that even today HTTP authentication mechanisms by themselves are pretty weak. Let's check the simplified high-level picture of HTTP authentication:

First of all, the server authenticates the client, but client does not authenticate the server. So the clients has no idea whom they sends their credentials. Moreover, HTTP authentication does not define confidentiality, so anyone can at least know that a certain web resource has certain userbase simply by observing traffic.

Although in recent authentication protocols users do not send passwords directly, sending hashes (which is one-way irreversible function) of their passwords instead, passive eavesdroppers can still collect this information and use more complex techniques (like dictionary attacks to recover the password).

Previous authentication mechanisms did not use server nonces, so a simple replay attack was possible. Even today many browsers support such older mechanisms for compatibility reasons, so a man-in-the-middle can forge messages between client and server and perform a downgrade attack.

外文译文

本文论述“信息安全”概念的出现和发展,依据近年来全球信息安全领域的文献资料,并结合与之相关的实践活动,阐述“信息安全”、“网络安全”、“网络空间安全”三者的联系与区别。信息安全可泛称各类信息安全问题,网络安全指称网络所带来的各类安全问题,网络空间安全则特指与陆域、海域、空域、太空并列的全球五大空间中的网络空间安全问题。三者均类属于非传统安全领域,都聚焦于信息安全,可以相互使用,但各有侧重;三者的概念不同,提出的背景不同,所涉及的内涵与外延不同。理清三者的关系,有助于在信息安全研究与实践的逻辑起点上形成清晰的认知,在信息安全的基础理论研究中形成业界内外公认的学术规范。

随着信息技术的飞速发展,网络信息安全保障已迫在眉睫。在网络上,尤其是在互联网上存储和传输着的大量信息,随时受到安全威胁。电子商务作为极具价值的敏感信息之一,关系到电子商务主体单位的商业秘密。所以,在相关单位或企业进行电子商务活动的同时,必须解决其网络信息的安全保密问题。这是每个正在实施或将要实施电子商务的单位和企业必须正视的一件重要事情。本文对电子商务的信息安全技术进行研究,在重点研究电子商务安全技术原理的基础上,针对与电子商务应用相关的基本安全问题及解决方案进行了深入的探讨。

本文从电子商务的概念和安全问题着手,分析了电子商务行业采用的信息加密技术、数字指纹、数字签名、数字时间戳、数字证书、安全认证协议、信息隐藏技术和防火墙技术等多种安全技术。最后提出了使用 ASP 开发工具、SQL Server 数据库等为开发平台,构建江苏省教育超市(好买得超市店)的网上购物环境,方便校园内广大师生购物,建立“好买得”江苏省教育超市网上商城,解决了电子商务中的安全问题,取得了较好的效果。

随着网络技术的迅速发展和日益普及,电子政务建设和发展中的信息安全越来越显得重要。而数字签名技术是信息安全理论与技术的基础和重要保证,使其应用于电子政务中,可以提供身份认证服务、权限控制服务、信息保密服务、数据完整性服务和不可否认服务。从而,为电子政务提供了一个安全的环境。

本文主要从以下五个方面对数字签名技术在电子政务中的应用进行分析与研究:第一是对数字签名技术进行介绍,阐述其定义、原理和广阔的应用前景;第二是对数字签名技术中的常用数字签名算法进行分析和比较,通过研究选取安全实用的数字签名算法;第

三是针对我国电子政务中的信息安全进行分析,提出了适合国情的电子政务的 PKI 信任模型,数字签名的使用模式以及一些数字签名方案;第四是以提出的数字签名方案为核心,设计一个数字签名系统,应用于电子政务系统中,为电子政务系统提供有效的信息安全保证。最后,本文根据目前的发展状况,提出了数字签名技术在电子政务中应用的进一步的研究方向。

随着全球经济和社会发展不断信息化的大趋势,“电子政务”已成为衡量社会信息化的程度和一个国家政府机构的管理、服务能力,乃至综合国力的重要因素。发展电子政务,就是要充分应用现代信息技术,大力推进政府信息化的进程。然而,在这一进程中,安全问题成为阻碍其发展的重要因素之一。在互联网技术迅猛发展的今天,信息安全技术在电子政务安全中起着至关重要的作用。信息安全的核心技术是密码技术,而身份认证又是密码学的基本应用之一。

由于密码系统的困难性和复杂性,对应用于电子政务系统信息安全中的密码技术,特别是身份认证技术,进行全面、深入以及准确的理解和把握是非常重要的。

本文综合介绍应用于电子政务安全的信息安全技术(特别是密码技术),并重点关注身份认证技术。我们首先对电子政务系统信息安全和身份认证技术发展和应用进行了概述,并对目前主流身份认证技术进行分析总结。在此基础上,对著名的 Cramer-Damgard 身份认证协议进行重新审查、思考和深入探讨,指出其在实际应用中的安全问题,并提出了身份认证协议互联网运行的几种新的安全属 J 性,在此基础上设计和证明了一类满足新安全性要求的身份验证协议。这有利对身份认证协议一一尤其当其在互联网上并发运行时的组身份安全性一一有更深入和精确的理解,有助于当在电子政务安全实践中应用身份识别技术时进行更全面及深入的理论理解和实践测评, 更好地开展电子政务安全工作。

现有的方法提供一定程度的保护，或好或坏，但他们每个人都有显著的缺点。到目前为止，大多数当前的系统和安全协议只使用了三种类型的密码原语的：加密，密钥协议和数字签名。更多高层次的任务，如身份验证，是由那些原语中的协议某种方式相结合而实现。互联网认证开始很基本的口令:用户输入到网页形式的密码,密码是通过 HTTP 发送到服务器，服务器验证密码，并允许在用户那是在小互联网的初期。当时袭击者通过让互联网是如何工作的经验非常少的限制。即使有一些基本的网络知识，他们没有设备，工具或软件（这是非常昂贵的，当时）做攻击。此外，攻击本身是因为其中穿过因特网当时的信息的小商业价值毫无意义的。最终，知识，软件和工具的互联网和可用性

的增长创造第一网络攻击：HTTP 密码很容易被简单的无源网络嗅探器和协议分析仪被盗。

下一步是要更改密码的一些价值观这是无用的被动偷听者：人们开始散列的口令。由于服务器和用户都有过相同的密码，他们可以生产这些相同的哈希值，并比较它们与用户发送哈希服务器。看起来，攻击者无法获得的密码，因为倒车的哈希函数在计算上是“几乎不可能”。该解决方案化险为夷.....只是一小会儿！攻击者使用两种方法来解决这个问题：

第一：很多人做他们的密码“易记”，所以他们袭击者散列一个大集的流行词和通过了解哈希，可以很容易地“查找”原密码，如果它正好是从生产的“字典”：字典攻击被发明。

第二：即使有人使用复杂的密码，攻击者只需使用的散直接与有“修改的浏览器”的服务器进行身份验证。他们没有在表单中输入密码，而是直接注入哈希 HTTP 流：主动攻击的发明。很显然，现在的 HTTP 流量必须进行加密。但是，由于通信双方都远离对方使用了密钥协商，并最终被打破的攻击：人在这方面的中间人提出。历史不断：为保护密码的传输更复杂的方案建议，更好，更聪明的攻击的目的是打败他们。那岂不是巨大的，以避免在传输所有的密码？

大多数工程师谁刚开始开发的加密工具，显得非常高兴，当他们在使用一些关键的转弯一块数据到一个随机字符串，寻找和恢复原始数据的第一次成功。的问题是，大部分的工程师在此时停止。我们知道从 Schneier 的定律：

任何人，从最无能爱好者最好的密码破译，可以创建一种算法，他自己无法突破。

他们认为，如果输出确实是随机看，没有人知道密钥，它们是安全的。因此，人们总能找到低安全加密方案，硬编码的钥匙或初始向量，加密方式等，即使在生产软件使用不当造成的。而且，虽然你的输出看起来是随机的状，一个熟练的攻击者有适当的工具和数学背景一定会找到的图案，侧信道泄漏，执行密码分析，最终将恢复数据。即使是大公司陷入这种麻烦，所以你有什么特别的？

涉及 bcrypt，PBKDF2 或者“加密再比较”不同的方案框架提供了唯一的安全系统，而不是完整的解决方案的一个片段。这根本不提供安全的足够的水平。

密码仍然广泛用于 HTTP，使用户访问受限资源。然而，尽管认证协议更新的历史长河中，仍然有一定空间的攻击。一个安全意识的用户将永远不会尝试在网站上输入自己的密码,如果网站不提供进入这样一个证书的 HTTPS 连接。这意味着,即使自己今天 HTTP

验证机制是相当薄弱。让我们来看看 HTTP 认证的简化的高层次的画面：

首先，服务器验证客户端，但客户端不验证服务器。所以，客户不知道他们所发送的凭据。此外，HTTP 认证没有定义的机密性，所以任何人都可在至少知道某个网络资源有一定的用户群简单地通过观察流量。

虽然在最近的认证协议的用户并不直接发送密码，发送哈希（这是单向不可逆的功能）的密码，而不是被动窃听仍然可以收集这些信息，并使用更复杂的技术（如字典攻击来恢复密码）。

上一页身份验证机制不使用服务器随机数，这样一个简单的重放攻击是可能的。即使在今天，许多浏览器都支持的兼容性等原因较旧的机制，所以一个人在这方面的中间人可以伪造客户端和服务器之间的邮件，并进行降级攻击。

毕业设计任务书

（电子邮件加密技术及应用）

一、毕业设计目的

毕业设计是本科毕业生在大学期间最后一个综合性教学环节，是学生书本知识深化与升华的重要过程，是学生对实际应用的预演或实践，它对学生综合素质与实际应用能力的培养具有重要和深远的意义。通过本次毕业设计以期到如下目的：

1、培养学生综合运用所学的知识与技能分析与解决问题的能力，并巩固和扩大学生的课堂知识综合运用所学过的基础理论和专业知识，以提高分析和解决实际问题的能力。

2、熟悉软件开发的过程，培养学生分析问题，灵活应用软件工程知识、数据库知识和高级语言编程等解决问题的能力；要求学生学会查阅、使用各种专业资料、网上资源，培养学生通过各种形式获取学习知识的能力；

3、提高科技论文写作等方面的能力，培养学生严肃认真的科学态度和严谨求实的工作作风，培养学生勇于创新和开拓进取的精神。

4、促使学生向工程技术人员转变，培养学生树立正确的设计思想和掌握现代设计方法。

二、主要内容

电子邮件在发送的过程中容易被不法分子篡改、截取等；存储中也容易病毒感染、泄密、丢失及被篡改等；恢复中存在乱码、病毒等威胁。电子邮件给人们带来了便利的同时也带来了很大的安全隐患。凡是经常使用电子邮件的人都必须注意，在收发电子邮件时，对任何可疑邮件应加强防备，这样才能使一些垃圾邮件和病毒邮件被拒于信箱之外。而对于从事网络安全研究的人员，只有研究出功能强大的邮件安全保护系统，才能从根本上解决问题。

PGP(Pretty Good Privacy)是对电子邮件在 Internet 上的通信安全而设计的一种公钥加密系统，它是一个强有力的加密软件包，被用于加密电子邮件、重要文件及数字签名，以保证信息在网络上的传输安全。

研究电子邮件加密算法 PGP 模型的实现原理及过程，编写系统模拟实现 PGP 加解密流程。系统能够对邮件文本，邮件附件等数据利用电子邮件加解密算法 PGP 实现加密与

解密。要能够实现模拟网络通信中的应用，并保证一定的数据安全性。

系统主要设计内容：

1、研究 PGP 加解密的完整过程。

2、对 PGP 过程中用到的加解密算法进行研究并尝试实现。

3、实现简单的应用程序，并加入 PGP 算法来保护数据的安全性。

4、对成果进行分析，总结其合理成分以及不足之处，并尝试在以后的工作学习中努力发挥优势弥补不足。

三、重点解决的问题

1、PGP 加密的实现原理

2、如何保证网络传输中安全性

3、网络传输的实现方法

四、主要技术指标或主要参数

开发环境

操作系统：Windows7

数据库：SQL Server 2008

编程工具：Visual Studio 2013, C#语言。

五、基本要求

1、用户界面要求

本系统要求所有界面为窗体形式，方便用户使用。系统的界面要求模块分布美观，便于用户操作，不要太多窗口跳转。要求系统界面美观，各个子系统界面风格一致，整体感强。

2、运行安全性要求

在信息系统中，安全性是必须考虑的核心问题。欺骗、窃听、病毒和非法入侵都在威胁着信息系统的安全，因此要求整个系统安全可靠，提供必要的安全防护措施，以确保系统安全高效地运行。

3、适应性要求

本系统要求扩展性强，还可以在今后在原有的基础上进行功能扩充，管理其他数据。而且操作方式相对简单，用户接口友好。

如果在开发过程中，需求有所变化，在一定的范围内是可以适应开发计划的实施的。

4、成果要求

整个系统的设计要求工作量饱满，各个子系统界面风格统一，容易实现各个子系统的集成，要求程序配置简单，移植方便，整个系统要经过严格的测试，操作逻辑要合理，运行过程要流畅，系统运行中不允许出现严重错误。拟开发的系统要求具备界面友好，操作方便、交互性强、安全稳定、维护代价低等特点。

六、其它（包括选题来源）

从老师拟定的多个课题中自选。

指导教师：　　年　月　日

华北水利水电大学本科生毕业设计开题报告

学生姓名	尚聪聪	学号	201215019	专业	计算机科学与技术
题目名称	电子邮件加密技术及应用				
研究或设计概述	电子邮件是最常用的一种网络应用，因其涉及个人隐私等敏感话题，所以电子邮件的安全性备受关注。Email 系统主要由邮件分发代理（MDA）、邮件传输代理（MTA）、邮件用户代理（MUA）以及邮件工作站组成。因此，邮件系统的安全目标是：（1）邮件分发安全，阻止垃圾邮件和开放转发，并查杀已知病毒；（2）邮件传输安全，必须保障邮件传输的机密性和完整性；（3）邮件用户安全，用户浏览邮件过程中需要确认用户的身份，防止邮件被非授权访问。针对这些安全目标常用的措施有：（1）身份认证，用户在接收、发送、转发邮件过程中，必须经过身份认证，以避免邮件被窃取篡改，并且要求认证的口令强度要足够抵抗口令攻击；（2）加密、签名，在传输中，必须采用加密和签名措施来保证邮件的机密性和完整性。 PGP 是采用对称加密算法和非对称加密算法相结合来对 Email（或文件存储）提供安全的协议，它通过加密、签名和认证来保护邮件内容的机密性、完整性和抗否认性。PGP 的实际操作由 4 类服务组成：认证（数字签名）、保密（消息加密）、压缩和电子邮件兼容性。 PGP 加密详细步骤：用 SHA-512 生成消息散列（Hash）码，采用 DSS 或者 RSA 算法，用发送者的私钥加密该消息摘要并将其加入消息中。采用 AES 算法，使用由发送者生成的一次性会话密钥加密消息。使用 RSA 算法中接受者的公开密钥加密该会话密钥并将其加入到消息中。使用 ZIP 算法来实现消息压缩以便存储或传输。为电子邮件应用程序提供透明性，一个加密的消息可能会用基数 64 转换成一个 ASCII 码字符串。				
主要内容	实现 PGP 的加密过程和解密过程，并且将其运用到字符、文件以及聊天数据的加密、认证与解密。具体来说就是采用 SHA-512 生成消息散列码，用加密方的私钥对消息散列码加密（签名），把消息和签名连接在一起用一次性会话密钥加密，再用接收方的公钥对会话密钥的密钥加密，之后和会话密钥加密后的数据一起发给接收方。接收方首先用自己的私钥解密出会话密钥，再用会话密钥解密出消息以及签名，对消息采用 SHA-512 生成同样的消息散列码，并用发送方的公钥验证消息的完整性及保密性。				
主要参考文献	[1]廖蓉晖，王娟，彭凯.DH 密钥体制在 VoIP 通信中的应用[J].通信技术,2015,48(03):367－370. [2]祝凯捷,蔡权伟,林璟锵,荆继武.密钥安全及其在虚拟化技术下的新发展[].密码学报,2016,3(1):12-21. [3]杨柳.密码学在网络安全中的应用[J].通讯世界,2016,3(1):216. [4]李中伟,佟为明,金显吉.智能电网信息安全防御体系与信息安全测试系统构建[J].电力系统自动化,2016,8(40):147-151 [5]郑瑞梅.浅谈加密技术的方法及应用[B].信息技术,2005:5,57-58				

	[6]邹伟,张智.树形异步即时通信密码协议的研究[J].通信技术,2016:1,87-91 [7]冯伟.大数据及其安全的产业纵深[J].信息安全与通信保密,2014,(10):20-30 [8]杨波.现代密码学(第2版)[M].北京:清华大学出版社,2010. [9]Douglas R Stinson.密码学原理与实践(第二版)[M].北京:电子工业出版社,2003 [10]Paar,Pelzl C.深入浅出密码学-常用加密技术原理与应用[M].北京:清华大学出版社,2012.
采取的主要技术路线或方法	查阅加密书籍、网络安全书籍和编程书籍， 首先实现PGP加密过程和解密过程。 然后分模块分项目实现简单的数据接受、发送、导入和导出等编程的方法。 再给这些方法加上加解密的实现。 最后将各个模块整合，使用统一管理的密钥和加解密模块。 中间遇到的问题通过独立思考，上网查询，查阅资料，同学讨论，求助老师等方式予以解决。
时间安排	第3、4周：认识阶段，查看书籍和小组交流的手段，探讨网络安全，研究加密算法，首先弄明白要研究的是什么，怎么去研究等基本问题； 第5、6周：加解密算法实现，尝试多种渠道边学习边编写加解密算法，并尝试用新的思路方式去解决所遇到的问题； 第7、8周：编写各个模块，字符加解密、文件加解密、网络通信数据的加解密，优先实现各个模块功能，尤其是网络聊天程序的编写； 第9周：加解密测试，完善各个模块，即各个模块中完成加解密算法的加入及测试； 第10、11周：模块整合，最后测试，完成项目； 第12周：完成论文，程序后期界面交互等友好性修改； 第13周：答辩； 第14周：整理资料；
指导教师意见	签 名： 年 月 日
备注	