论文检测综合报告(专业版)

温馨提示：红色代表抄袭、蓝色代表引用、黑色代表自写。（专业版适合个人初稿自查、至尊版适合定稿检测）

passmore学术不端检测系统（网址：https://www.passmore.cn）

标题： 无

作者： 无

报告编号： C4185817AC0042F58253211ECE722B73

检测时间： 2021-05-14 22:22:35

检测字数： 20249

总相似度:37.57% 引用率:9.36% 复写率:28.21% 自写率:62.43%

检测范围

◎ 中国期刊库　◎ 中国图书库　◎ 硕士论文库
◎ 博士论文库　◎ 会议论文库　◎ 报纸库
◎ 网友专利库　◎ 网友标准库　◎ 百科库
◎ 网页库　◎ 网友共享库　◎ 自建库
◎ 工作总结　◎ 思想汇报　◎ 项目申报书

一、全文标红

文件加密网络传输系统的设计与实现

摘 要：信息化时代的到来使得数据安全面临着极大地风险挑战，数据与人类的生活息息相关，保护数据的安全就是保护人类生命财产的安全；其中网络安全技术即是能够阻止网络中传输的数据被蓄意或恶意破坏、更改的行为的主要措施之一。当前，相对实用的方法是对网络上传输的数据进行加密，但是数据加密必须依赖于成熟的数据加密算法，而对称密钥体制的典型代表DES算法就是目前非常成熟的数据加密算法。对称加密算法DES的成功设计不但确保了用户个人数据以及重要文件的安全，而且还为数据的安全传输提供一个切实可行的方案。[1]通过对人们想要发送的文件数据进行加密操作，使得数据泄露的可能性大大降低，也使他们发送的数据能够及时、高效和安全地发送给他们想要发送的人。本文提出了一种在windows操作系统下实现文件加密的新技术方案。它以加密技术作为基础，为保密文件的快速、安全传输提供了一种实用的操作模式，也为建立完善、严格的计算机网络安全机制提供了实践依据。

本课题设计并实现了一个文件加密网络传输系统。系统的实现将引入一种web应用开发技术；前端即网页部分负责显示数据、与用户的交互等，主要采用的技术有Bootstrap，Jquery，JavaScript，ajax等；后端主要是在MyEclipse下使用Java语言编写处理这些业务逻辑的程序。系统采用浏览器/服务器体系结构模式。浏览器端使用的对象分为两类：用户和管理员；服务器端则使用MySQL数据库作为服务的提供方。用户主要实现的功能有注册、登录个人账号、模糊查询、分类查看、文件加密传输、文件解密接收、个人信息维护等；管理员的主要功能是身份认证、用户管理、分类管理、文件数据量统计、个人信息维护等。

关键词：DES算法；加密技术；文件传输；数据加解密

Design and implementation of file encryption network transmission system

Abstract:With the advent of the information age, data security is facing great risks and challenges.Data is closely related to human life.To protect data security is to protect human life and property;Among them, network security technology is one of the main measures to prevent the data transmitted in the network from being deliberately or maliciously destroyed or changed.At present, the relative practical method is to encrypt the data transmitted on the network, but the data encryption must

rely on the mature data encryption algorithm.The typical representative of symmetric key system des algorithm is the very mature data encryption algorithm.The successful design of symmetric encryption algorithm des not only ensures the security of user's personal data and important files, but also provides a practical scheme for the safe transmission of data.[1]Through encrypting the file data that people want to send, the possibility of data leakage is greatly reduced, and the data they send can be sent to the people they want to send in a timely, efficient and safe manner.This paper presents a new technology scheme of file encryption in Windows operating system.It takes encryption technology as the foundation, provides a practical operation mode for the fast and safe transmission of confidential documents, and also provides practical basis for establishing a perfect and strict computer network security mechanism.

This paper designs and implements a file encryption network transmission system.The implementation of the system will introduce a web application development technology;The front end is the web part, which is responsible for displaying data and interacting with users.The main technologies used are bootstrap, jQuery, JavaScript, AJAX, etc;The back-end mainly uses Java language to write programs to deal with these business logic under MyEclipse.The system adopts browser / server architecture mode.There are two kinds of objects used in browser: user and administrator;The server side uses MySQL database as the service provider.The main functions of users are registration, login personal account, fuzzy query, classified view, file encryption transmission, file decryption receiving, personal information maintenance, etc;The main functions of administrator are identity authentication, user management, classification management, file data statistics, personal information maintenance, etc.

Key words:DES algorithm;encryption technology;file transmission;data encryption and decryption;

目　录

文件加密网络传输系统的设计与实现

1概　述

1.1项目开发的意义

互联网时代，人们的许多工作开始依靠网络的辅助，因为它不仅节省了时间，改善了沟通，而且提高了工作效率。互联网的出现给我们带来了很多的便利，但是在网络应用到实际生活中的同时也随之带来了各种各样的网络安全问题，因此网络安全问题就成为了社会各界关注的重点问题。

其中文件数据安全就是人们所普遍关注的网络安全问题之一，由于一份文件可能包含许多价值量很高的机密信息或者个人的一些隐私和敏感信息，因而文件中的数据信息一旦被黑客窃取和泄露，损失是难以想象的；于是，在发送文件时，加密操作对于确保文件安全至关重要。

随着我国科学技术水平的不断提高和信息技术的不断发展，人们对网络数据信息的安全性和可靠性提出了更高的要求，信息安全已成为网络通信领域的一个重要研究课题。[2]与其说信息是一个由各种数据类型组成的宏观范畴，不如说数据是信息的载体和重要组成部分；因此，为了保证信息的安全性和机密性，一些数据保护措施必须被予以执行。例如，以加密算法作为支撑的加密技术就能够有效保障数据的安全；换句话说，即使加密的文件信息被泄露或窃取，但是其内容依然是安全的，因为非法人员不知道用户设置的密钥，所以无法正确解密文件，因而也就获取不到什么有效信息；从目前网络技术的发展趋势来看，数据加密技术的应用不仅是解决数据安全问题的有效途径，也是最实用的手段。

1.2 项目开发背景

随着国家大数据战略的持续推进和深化，以大数据为主导的产业革新不断涌现，各种“互联网+”应用和服务大大缩短了企业与用户之间的距离。人工智能等技术广泛应用于城市管理、金融、医疗、交通、住房、生产等领域。数据采集终端越来越多，传输速度越来越快。在万物互联、人机互动、天地融合的智能网络空间中，个人用户已经成为重要的数据生产者和消费者；数据在21世纪正扮演着一种重要的角色，不仅作为机器学习以及深度学习等人工智能技术的基础，而且已被视作智能化时代企业制胜的关键因素；同时，数据作为一项重要资产，受到安全威胁的程度也越来越严重，数据遭泄露和滥用的现象极为普遍，个人隐私保护面临重要挑战。

1.3 国内外研究现状

美国早在1977年就已经制定了自己的数据加密标准（分组密码）；但是除了具体的算法外，从未对外公布过详细的设计规则以及方法。伴随着美国数据加密标准的诞生，研究人员开始对分组密码进行深入的研究和探讨，同时也设计出了大量的分组密码，并给出了一系列的评价标准。日本和苏联等其他国家也提出了各自的数据加密标准。然而，处于这些分组密码算法当中并且能被大众普遍接受和认可的算法却寥若晨星。目前，我国的做法是针对每一种或每一种安全产品开发算法，算法以及源程序都不开放。这样，对算法的需求就比较大，从而产生了兼容性和互操作性等问题。

此刻，非数学密码学理论和技术（包含信息不可见性、量子密码学、生物特征识别理论和技术）在世界范围内受到了广泛的关注和讨论。信息隐藏是指通过在网络环境下将机密信息隐藏在大量信息中的一种方式，这项技术将在未来的网络环境中保护文件数据不被破坏方面发挥非常重要的作用；尤其像数字水印、图像叠加、隐藏协议和子信道等这些理论和技术已经引起了学者们的广泛关注。从1996年至今，世界上举办了许多关于信息隐藏的专业研讨会。基于生物学特性的理论和技术已经发展起来，目前应用较多的主要有手形识别、指纹识别、语音识别、视网膜识别、虹膜识别、人脸识别、DNA识别等；其他理论与技术也在不断形成，与此同时，相关产品也相继形成。这些产品由于成本高而没有得到广泛的应用。1969年，威斯纳在哥伦比亚大学第一次创造性的提出了共轭编码的理论概念。不幸的是，他的想法当时没有被接受。十年后，起源于共轭编码概念的量子密码学理论和技术取得了惊人的进步；一方面，单光子密钥交换协议已被普遍应用在商用光纤和自由空间中；另一方面，英国电信实验室通过利用三十千米长的光纤信道顺利实现了每秒两万比特密钥的分配；这些耀眼的成就促使欧洲一些国家的政府不谋而合的组织来自大学或研究机构的科研人员投入到量子密码学的研究事业当中。迄今为止，主要有三种类型的量子密码学理论：一种是基于单个光子量子信道的不确定性原理；二是基于量子相关信道中的贝尔原理；第三种是基于两个非正交量子态的特性。但还有许多问题需要近一步探究。例如，寻找相对应的量子效应以研究出更多的量子密钥分发协议，量子加密理论的形成与完善，量子密码学协议安全性分析方法的探索，量子加密算法的发展，量子密码的实用性，一般来说，非数学密码学的理论和技术仍在探索当中。

1.4 项目内容安排

在信息时代，数据和信息面临着巨大的风险，为了实现网络通信线路上文件和数据的安全传输，设计一种基于DES加密算法的文件传输系统已成为迫切需要。论文总共分为七章，第一章为项目概述，第二章至第六章为文件加密系统的核心内容，分别对密码学理论基础、DES算法的原理以及整个系统的设计与实现做了详细说明。

第一章简要介绍了文件加密传输系统方案研究的意义和背景，以及国内外学者目前对密码学应用研究的现状。

第二章为密码学的基础知识，主要介绍密码学当中的一些专业术语的含义以及密码体制的定义，同时也对DES加密算法做了简要的描述，对其几种工作模式和优势做了简略的分析。

第三章是关于DES加密算法原理的介绍，其中重点讨论了算法运算过程中所蕴含的几个关键部分，分别是明文的初始置换、子密钥的生成过程、迭代运算过程以及终止逆变换；原理部分的阐述直接与加密、解密过程联系在了一起，所以，只有充分理解加解密的原理，才能更好的实现功能。

第四章论述了系统的设计，主要介绍了项目实现了什么样的系统、系统的功能需求以及数据库的设计等。

第五章是系统的实现，进一步讨论了系统中每个功能是如何一步步操作实现的。

第六章为文件加密传输系统的测试，其中简要论述了系统测试的目的并展示文件加密传输、解密接收等部分功能的测试结果。

2对称加密算法原理

2.1密码原理

加密技术是以密码学原理为基础，保证计算机通讯、网络和所有信息系统安全的一种理论和技术基础。通常意义上的加密是指利用一种或多种方式对信息进行处理以掩盖其真实内容的过程，加密的数据称为密文；另一方面，解密意味着将未知的加密内容以某种方式转换成原始内容的处理过程，解密后的数据则被称作明文。明文用M表示，对于计算机来说是指简单的二进制数据；密文用C表示，也是二进制数据。明文M在加密函数E的作用下输出密文C，在数学上可用公式E（M）=C来表示这一运算过程；同理，解密函数D作用在密文C上可以得到明文M，可用数学公式表示成D（C）=M。现代密码学使用密钥K，它可以是许多数值中的任意一个。密钥K的可能取值范围被定义为密钥空间，且密钥K在加密运算和解密运算中同时被使用，如此加密函数变成E（M）=C，解密函数变成D（C）=M。"[3-6]"

文件数据在传输的过程中，若使用对称加解密算法，则收发双方需提前约定好密钥，且使用的算法要求一致。即发送方发送文件时，输入密钥并选定算法对文件进行加密；接收方收到文件时，通过输入商定的密钥并选择相同的算法对文件进行解密。密文在公共通信线路上传输时，如果被截获，窃取者收到的是不可读的乱码，无法获得原始数据。

0

密钥　　密钥

1

明文　　密文　　明文

2

图2-1 加密解密过程

2.2密码体制

密码体制的语法定义如下：

（1）明文信息空间：字母表上的一组字符串。

（2）密文消息空间：可能的加密消息集。

（3）加密密钥空间K：可能的加密密钥集。

（4）解密密钥空间K'：可能的解密密钥集。

（5）有效的密钥生成算法：NK×K'。

（6）有效的加密算法E：M×KC。

（7）有效的解密算法D：C×K'M。

对于整数l，(l)输出长为的密钥对(ke,kd)K×K',

对于keK和mM，将加密变换表示为c=E(m)，读做“c是m在密钥ke下的加密”；将解密变换表示为m=Dd(c)，读做“m是c在密钥kd下的解密”。对于所有的mM和所有的keK,一定存在kdK'：Dd(E(m))=m。

在单钥密码体制中，因为只有一把密钥，所以加密消息的一方必须共享自己的密钥给即将收到已加密消息并对其解密的另一方，即加密、解密使用相同的密钥。kd=ke的情况赋予了单钥密码体制另一个名称：对称密码体制(Symmetric Cryptosystem)。[7]

一个设计密码必须具备的条件表在1883年被Kerchoffs列出。在这个列表中存在着一个被普遍认可的理论，即kerchoffs原理；现代密码分析的标准假设是密码算法、密钥长度以及密码文本可以被攻击者知晓。由于对手最终可以获得信息，因此在评估密码强度时最好不要依赖信息的机密性。结合Shannon对密码系统的语义描述以及kerchoffs原理，我们可以总结出如下好的密码系统：

（1）加密算法E和解密算法D各自不能含有隐藏或私有的部分。

（2）E在整个加密消息空间中均匀地分布具有重要意义的消息；随机分布也可以通过一些随机内部运算得到。

（3）E和D在密钥使用正确的情况下应该是实际有效的。

（4）不使用正确的密钥，从密文中恢复出相应的明文是一个困难的问题，它仅由密钥参数的大小决定，通常取长度为s的密钥，以至于解决这个问题所需要的计算资源量级超过了p(s)，p是任意多项式。[7]

2.3 DES算法

DES是一种世界公认的标准加密格式，自产生到现在已有许久的历史,算是比较可靠的算法。20世纪70年代初，在数据加密需求日益增长的形势下，设计出一种能够实现对不同类型数据进行加密的通用算法显得十分必要，为此美国国家安全局便对这种加密技术提出招标；Horst Feistel依据美国IBM公司在二十世纪中后期研究出的Lucifer算法，经过一步步的计算与推导，最终演变出了DES算法；其在1976年11月23日被美国国家安全局定义为标准的加密算法，同时也被称为数据加密标准。[9]

DES在对文件数据实施加解密操作之前首先要对数据进行分割，因为用户传输的文件信息被机器翻译为二进制表示形式，所以将连续的二进制位划分为许多个大小为64bit的分组，然后在执行算法的入口依次输入每个分组，这些分组经过算法的加密运算在输出端口生成若干同样大小的密文分组，将其整合便得到整个密文；发送者与接收者在使用该算法进行加解密的过程中，会输入相同的密钥，不同之处在于密钥的生成方式，因而也称其为对称加密算法。密钥长度是56位，也可以是任意的56位数，并且可以随时更改密钥。[8]

DES算法由三个输入参数组成：密钥、数据和模式。输入密钥为8字节64位；同样数据入口也采用8字节64位,在数据上分为两种需要加密和需要解密的

数据;模式入口是算法的工作模式也分为两种,即加密模式和解密模式。[8]

算法的加密和解密流程:如果模型是加密的,则数据由密钥加密,DES的输出以数据加密的(64位)形式生成;如果模型被解密,则数据由加密形式的密钥解密,并作为DES的输出结果恢复到显式形式的数据(64位)。[8]

对于通信网络的两端,双方就同一密钥达成一致,在密钥的通信始端对传输的主要数据进行加密,加密后的数据以密文的形式在通信网络中传输(比如电话通信网),在数据传输到达目的地后,使用相同的密钥对文件数据进行解密,并重新构建成数据的代码核心,其能够保证数据是安全、完整、未被篡改的原因在于确保了密钥的一致性。

随着网络技术的飞速发展,相应的网络信息加密技术也取得了长足的进步;同时,算法的加解密能力以及执行效率已成为评价加密技术质量的主要手段。经过大量实践证明,DES算法在加密和解密能力上都很优秀,且已经得到人们的认同,许多人也开始对它进行研究。它的出现也给网络文件传输带来了可靠的保障。

2.4 DES算法加密模式

在实际操作中,DES算法根据其加密算法规定的明文包的大小将数据分成若干个64位加密块,接着以块为单位依次进行加密操作;根据编码模式的区别将其划分为以下四种不同的加密模式。

(1)电码本模式(ECB)

ECB模式是DES加密的基本工作模式。在该模式下,各个明文块按照一定的顺序进行独立加密,并相应地生成众多独立的密文块,且后面每个明文块经过加密运算后得到的结果与前面生成的密文块没有关联;这种模式下的优点是,在算法的执行过程当中不仅可以采用并行处理机制来加速加密和解密操作流程,而且每个密文块中的错误都不会作用到后面要传输的明文块;这种模式的缺点是易于公开明文数据模式。

(2)分组密码链路模式(CBC)

在CBC模式下,第一个加密块与定义好的初始向量IV进行异或运算,然后加密。在对后续的明文块进行加密之前,首先要使本次待加密的明文块与前一次生成的密文块做异或运算,之后再对生成的结果实行加密。每个块的加密结果都受到之前所有块内容的影响,所以即使同一块明文在整个明文中出现多次,也会产生不一样的密文。如果密文内容被剪切、粘贴、替换,或者在网络传输过程中出现错误,那么后续的密文就会被破坏,甚至无法顺利解密恢复;与此同时,并行处理技术在这种模式下不能够用来提升加密操作的速度,但是可以用来加速解密操作的完成。这是该模式的优缺点。

(3)密文反馈方式(CFB)

在CFB模式中,用于明文块加密的算法可以视作流密码加密机来使用;流密码加密机在实际运用中能够根据操作需要自行调整每个块的大小。每个待加密的明文块与前一个加密生成的密文块进行异或运算后生成密文;因而,如果某个明文块在加密的过程中出现错误而产生不正确的密文块,那么这种错误将会流水似的作用到后面每个待加密的分组;尽管在整个明文中出现多个相同的明文块,然而这些块经过加密运算后的输出结果都不尽相同。在该模式中,为了加密第一块,必须选择初始向量IV,并且该初始向量每次必须是唯一的和不同的;同时,在这种模式下很难使用并行处理来加速加密操作。

(4)输出反馈模式(OFB)

OFB和CFB大致相同。两者都是将每个块的明文与前一块加密后的结果进行异或运算然后生成密文。不同之处在于,OFB模式下前一个块加密后的结果是独立生成的,每个块的加密结果不受所有前一个密文块内容的影响。所以,即使在传输过程中有一些数据块丢失或出现错误,也不会造成完全无法解密的现象。在此模式中,只有先定义一个初始化的向量IV,才能实现首个明文块的加密,不然难以运用并行处理机制来提高加密的效率。

2.5 DES算法优势分析

(1)在数据加密方面的优势

如今,世界许多国家已经将DES加密算法视为自己的数据加密标准;同时,这些国家对数据加密算法的评价也很高,这意味着该加密算法能够满足自身对数据加密的要求。具体表现如下:一是数据保护功能质量高,同时可以避免数据的非法泄露,防止数据在未经授权的情况被随意改变;其次,数据加密算法具有一定的复杂性,而且破译难度很大。目前,穷举法是解密加密算法的代表性技术。换言之,如果有人想解密这个算法,他们必须花费比平时更多的时间和精力,而且与他们能得到的相关好处相比,效果是非常明显的;即使我们选择了一台每秒能进行数百万次计算的现代计算机,借助穷举法探索破解加密算法的方法同样需要很长时间;不过,尽管算法本身具有复杂、抽象的特性,但是整个密码系统却没有对此提出具体的需求。DES算法只是加密算法的基础和核心内容;最后,根据DES加密算法的流程可以知道,该加密方法非常高效并广泛应用于金融、通信等行业;同时,该算法也经常用于ATM中的数据加密。[12]

在计算机通信方面的优势

DES数据加密算法在美国得到了很高的评价,该算法在加密应用中起着非常重要的作用,可以满足各种加密需求;同时也可以运用在计算机通信当中。[11]在加密的时候,主要体现为:第一,在使用数据加密算法进行数据加密的过程中,应当有效的满足不同的数据保护要求,增强数据保护的可靠性。同样,因为这种加密算法可以制止不法人员对传输过程中的数据修改的违禁行为,所以,其不仅提高了数据的安全性,而且也保证了数据的有效性;第二,在DES数据加密算法当中,因为算法本身具有一定的复杂性,所以在一定程度上确保了计算机通信技术中的安全需求,也实现了应用效果的最优化。同时,加密算法的复杂性也增加了解码的难度系数,提高了数据传输的安全性。最后,即使DES加密算法在某种意义上实现了对数据的保护功能,可是,数据的安全性不能仅由算法的复杂性体现出来,而应该由整个加密系统的可靠性来决定。接收端收到对方发送过来的文件后,无法直接查看文件内容,需要执行解密程序后才能获取信息。因此,DES加密算法在计算机通信领域中具有广泛的适用范围。[12]

3 DES算法的设计原理

3.1 DES加密算法框图和流程图

3

图3-1 加密算法框图

4

图3-2 加密算法流程图

3.2 初始置换

对于用户要传输的明文数据M，首先对其进行分组，每组64位，然后对输入的每个分组使用如表3-1所示的IP（Initial permutation）初始变换，按照从左向右、从上向下的顺序进行置换操作。[10]

表3-1 IP初始置换表

<table><tr><td>58</td><td>50</td><td>42</td><td>34</td><td>26</td><td>18</td><td>10</td><td>2</td></tr><tr><td>60</td><td>52</td><td>44</td><td>36</td><td>28</td><td>20</td><td>12</td><td>4</td></tr><tr><td>62</td><td>54</td><td>46</td><td>38</td><td>30</td><td>22</td><td>14</td><td>6</td></tr><tr><td>64</td><td>56</td><td>48</td><td>40</td><td>32</td><td>24</td><td>16</td><td>8</td></tr><tr><td>57</td><td>49</td><td>41</td><td>33</td><td>25</td><td>17</td><td>9</td><td>1</td></tr><tr><td>59</td><td>51</td><td>43</td><td>35</td><td>27</td><td>19</td><td>11</td><td>3</td></tr><tr><td>61</td><td>53</td><td>45</td><td>37</td><td>29</td><td>21</td><td>13</td><td>5</td></tr><tr><td>63</td><td>55</td><td>47</td><td>39</td><td>31</td><td>23</td><td>15</td><td>7</td></tr></table>

参照上表，原始分组的第58位经初始置换变为新建分组的第1位，原始分组的第50位经调换成为新建分组的第2位，以此类推。

3.3 子密钥的生成

PC-1变换

首先，用户输入64位的密钥，然后根据密钥交换表PC-1进行变换。

表3-2 密钥交换表PC-1

<table><tr><td>57</td><td>49</td><td>41</td><td>33</td><td>25</td><td>17</td><td>9</td></tr><tr><td>1</td><td>58</td><td>50</td><td>42</td><td>34</td><td>26</td><td>18</td></tr><tr><td>10</td><td>2</td><td>59</td><td>51</td><td>43</td><td>35</td><td>27</td></tr><tr><td>19</td><td>11</td><td>3</td><td>60</td><td>52</td><td>44</td><td>36</td></tr><tr><td>63</td><td>55</td><td>47</td><td>39</td><td>31</td><td>23</td><td>15</td></tr><tr><td>7</td><td>62</td><td>54</td><td>46</td><td>38</td><td>30</td><td>22</td></tr><tr><td>14</td><td>6</td><td>61</td><td>53</td><td>45</td><td>37</td><td>29</td></tr><tr><td>21</td><td>13</td><td>5</td><td>28</td><td>20</td><td>12</td><td>4</td></tr></table>

按照表PC-1的规律，原密钥的第57位转换为新密钥的第1位，原密钥的第49位更换为新密钥的第2位，其余位同样操作；此变换将用户输入的64位密钥缩减为56位，去除了原密钥的第8、16、24、32、40、48、56、64位（奇偶校验位）。

循环移位

通过上一轮产生的密钥C和D（1i16）根据循环移位表的操作，移位得到本轮需要的密钥C和D，同理可得到16轮迭代所需要的子密钥。

表3-3 循环移位表

<table><tr><td>轮数</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr><tr><td>移位数</td><td>1</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td></tr></table>

（3）PC-2变换

将除去奇偶校验位获得的56位新密钥拆分成左右两个部分，每个部分各28位，分别定义为C和D；接着使C和D依照循环移位表的规则循环左移1位得到C和D，再将C和D组合生成的56位密钥遵循表3-4的次序进行变换。

表3-4 密钥压缩替换表PC-2

<table><tr><td>14</td><td>17</td><td>11</td><td>24</td><td>1</td><td>5</td></tr><tr><td>3</td><td>28</td><td>15</td><td>6</td><td>21</td><td>10</td></tr><tr><td>23</td><td>19</td><td>12</td><td>4</td><td>26</td><td>8</td></tr><tr><td>16</td><td>7</td><td>27</td><td>20</td><td>13</td><td>2</td></tr><tr><td>41</td><td>52</td><td>31</td><td>37</td><td>47</td><td>55</td></tr><tr><td>30</td><td>40</td><td>51</td><td>45</td><td>33</td><td>48</td></tr><tr><td>44</td><td>49</td><td>39</td><td>56</td><td>34</td><td>53</td></tr><tr><td>46</td><td>42</td><td>50</td><td>36</td><td>29</td><td>32</td></tr></table>

对照上表，经过循环移位、组合而成的密钥中的第14位替换为新密钥的第1位，第17位替换为新密钥的第2位，其余位依次类推；可见，这种变换通过压缩密钥的方式，从而形成每轮迭代使用的子密钥K（1i16）。

3.4 迭代运算（以16轮当中的1轮做分析）

迭代过程结构图如下所示，其可以被分解为以下几个部分：

5

图3-3 DES加密算法的轮结构图

（1）E盒拓展

用户输入的明文数据M经过分组、初始变换等操作产生新的64位数据，将这64位数据划分成左、右两个部分，然后将右半部分32位数据根据表3-5的定义进行转换操作，从而使右半部分数据的位数拓展成与子密钥的位数相同。

表3-5 E拓展置换表

<table><tr><td>32</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr><tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr><tr><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td></tr><tr><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr><tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr><tr><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td></tr><tr><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>1</td></tr></table>

（2）异或运算

将拓展置换所得到的结果与子密钥K（1i16）做异或运算，输出为48位新数据。（注：这里是根据迭代的轮数选择参与运算的子密钥）

S盒非线性操作

将异或运算得到的48位数据，分割为8个大小为6bit的分组，每个分组对应一个S盒，通过S盒非线性运算将6位输入转变成4位输出。

表3-6 S1

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>14</td><td>4</td><td>13</td><td>1</td><td>2</td><td>15</td><td>11</td><td>8</td><td>3</td><td>10</td><td>6</td><td>12</td><td>5</td><td>9</td><td>0</td><td>7</td></tr><tr><td>1</td><td>0</td><td>15</td><td>7</td><td>4</td><td>14</td><td>2</td><td>13</td><td>1</td><td>10</td><td>6</td><td>12</td><td>11</td><td>9</td><td>5</td><td>3</td><td>8</td></tr><tr><td>2</td><td>4</td><td>1</td><td>14</td><td>8</td><td>13</td><td>6</td><td>2</td><td>11</td><td>15</td><td>12</td><td>9</td><td>7</td><td>3</td><td>10</td><td>5</td><td>0</td></tr><tr><td>3</td><td>15</td><td>12</td><td>8</td><td>2</td><td>4</td><td>9</td><td>1</td><td>7</td><td>5</td><td>11</td><td>3</td><td>14</td><td>10</td><td>0</td><td>6</td><td>13</td></tr></table>

表3-7 S2

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>15</td><td>1</td><td>8</td><td>14</td><td>6</td><td>11</td><td>3</td><td>4</td><td>9</td><td>7</td><td>2</td><td>13</td><td>12</td><td>0</td><td>5</td><td>10</td></tr><tr><td>1</td><td>3</td><td>13</td><td>4</td><td>7</td><td>15</td><td>2</td><td>8</td><td>14</td><td>12</td><td>0</td><td>1</td><td>10</td><td>6</td><td>9</td><td>11</td><td>5</td></tr><tr><td>2</td><td>0</td><td>14</td><td>7</td><td>11</td><td>10</td><td>4</td><td>13</td><td>1</td><td>5</td><td>8</td><td>12</td><td>6</td><td>9</td><td>3</td><td>2</td><td>15</td></tr><tr><td>3</td><td>13</td><td>8</td><td>10</td><td>1</td><td>3</td><td>15</td><td>4</td><td>2</td><td>11</td><td>6</td><td>7</td><td>12</td><td>0</td><td>5</td><td>14</td><td>9</td></tr></table>

表3-8 S3

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>10</td><td>0</td><td>9</td><td>14</td><td>6</td><td>13</td><td>15</td><td>5</td><td>1</td><td>13</td><td>12</td><td>7</td><td>11</td><td>4</td><td>2</td><td>8</td></tr><tr><td>1</td><td>13</td><td>7</td><td>0</td><td>9</td><td>3</td><td>4</td><td>6</td><td>10</td><td>2</td><td>8</td><td>5</td><td>14</td><td>12</td><td>11</td><td>15</td><td>1</td></tr><tr><td>2</td><td>13</td><td>6</td><td>4</td><td>9</td><td>8</td><td>15</td><td>3</td><td>0</td><td>11</td><td>1</td><td>2</td><td>12</td><td>5</td><td>10</td><td>14</td><td>7</td></tr><tr><td>3</td><td>1</td><td>10</td><td>13</td><td>0</td><td>6</td><td>9</td><td>8</td><td>7</td><td>4</td><td>15</td><td>14</td><td>3</td><td>11</td><td>5</td><td>2</td><td>12</td></tr></table>

表3-9 S4

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>7</td><td>13</td><td>14</td><td>3</td><td>0</td><td>6</td><td>9</td><td>10</td><td>1</td><td>2</td><td>8</td><td>5</td><td>11</td><td>12</td><td>4</td><td>15</td></tr><tr><td>1</td><td>13</td><td>8</td><td>11</td><td>5</td><td>6</td><td>15</td><td>0</td><td>3</td><td>4</td><td>7</td><td>2</td><td>12</td><td>1</td><td>10</td><td>14</td><td>9</td></tr><tr><td>2</td><td>10</td><td>6</td><td>9</td><td>0</td><td>12</td><td>11</td><td>7</td><td>13</td><td>15</td><td>1</td><td>3</td><td>14</td><td>5</td><td>2</td><td>8</td><td>4</td></tr><tr><td>3</td><td>3</td><td>15</td><td>0</td><td>6</td><td>10</td><td>1</td><td>

td>13</td><td>8</td><td>9</td><td>4</td><td>5</td><td>11</td><td>12</td><td>7</td><td>2</td><td>14</td></tr></table>

表3-10 S5

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>2</td><td>12</td><td>4</td><td>1</td><td>7</td><td>10</td><td>11</td><td>6</td><td>8</td><td>5</td><td>3</td><td>15</td><td>13</td><td>0</td><td>14</td><td>9</td></tr><tr><td>1</td><td>14</td><td>11</td><td>2</td><td>12</td><td>4</td><td>7</td><td>13</td><td>1</td><td>5</td><td>0</td><td>15</td><td>10</td><td>3</td><td>9</td><td>8</td><td>6</td></tr><tr><td>2</td><td>4</td><td>2</td><td>1</td><td>11</td><td>10</td><td>13</td><td>7</td><td>8</td><td>15</td><td>9</td><td>12</td><td>5</td><td>6</td><td>3</td><td>0</td><td>14</td></tr><tr><td>3</td><td>11</td><td>8</td><td>12</td><td>7</td><td>1</td><td>14</td><td>2</td><td>13</td><td>6</td><td>15</td><td>0</td><td>9</td><td>10</td><td>4</td><td>5</td><td>3</td></tr></table>

表3-11 S6

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>12</td><td>1</td><td>10</td><td>15</td><td>9</td><td>2</td><td>6</td><td>8</td><td>0</td><td>13</td><td>3</td><td>4</td><td>14</td><td>7</td><td>5</td><td>11</td></tr><tr><td>1</td><td>10</td><td>15</td><td>4</td><td>2</td><td>7</td><td>12</td><td>9</td><td>5</td><td>6</td><td>1</td><td>13</td><td>14</td><td>0</td><td>11</td><td>3</td><td>8</td></tr><tr><td>2</td><td>9</td><td>14</td><td>15</td><td>5</td><td>2</td><td>8</td><td>12</td><td>3</td><td>7</td><td>0</td><td>4</td><td>10</td><td>1</td><td>13</td><td>11</td><td>6</td></tr><tr><td>3</td><td>4</td><td>3</td><td>2</td><td>12</td><td>9</td><td>5</td><td>15</td><td>10</td><td>11</td><td>14</td><td>1</td><td>7</td><td>6</td><td>0</td><td>8</td><td>13</td></tr></table>

表3-12 S7

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>4</td><td>11</td><td>2</td><td>14</td><td>15</td><td>0</td><td>8</td><td>13</td><td>3</td><td>12</td><td>9</td><td>7</td><td>5</td><td>10</td><td>6</td><td>1</td></tr><tr><td>1</td><td>13</td><td>0</td><td>11</td><td>7</td><td>4</td><td>9</td><td>1</td><td>10</td><td>14</td><td>3</td><td>5</td><td>12</td><td>2</td><td>15</td><td>8</td><td>6</td></tr><tr><td>2</td><td>1</td><td>4</td><td>11</td><td>13</td><td>12</td><td>3</td><td>7</td><td>14</td><td>10</td><td>15</td><td>6</td><td>8</td><td>0</td><td>5</td><td>9</td><td>2</td></tr><tr><td>3</td><td>6</td><td>11</td><td>13</td><td>8</td><td>1</td><td>4</td><td>10</td><td>7</td><td>9</td><td>5</td><td>0</td><td>15</td><td>14</td><td>2</td><td>3</td><td>12</td></tr></table>

表3-13 S8

<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>13</td><td>2</td><td>8</td><td>4</td><td>6</td><td>15</td><td>11</td><td>1</td><td>10</td><td>9</td><td>3</td><td>14</td><td>5</td><td>0</td><td>12</td><td>7</td></tr><tr><td>1</td><td>1</td><td>15</td><td>13</td><td>8</td><td>10</td><td>3</td><td>7</td><td>4</td><td>12</td><td>5</td><td>6</td><td>11</td><td>0</td><td>14</td><td>9</td><td>2</td></tr><tr><td>2</td><td>7</td><td>11</td><td>4</td><td>1</td><td>9</td><td>12</td><td>14</td><td>2</td><td>0</td><td>6</td><td>10</td><td>13</td><td>15</td><td>3</td><td>5</td><td>8</td></tr><tr><td>3</td><td>2</td><td>1</td><td>14</td><td>7</td><td>4</td><td>10</td><td>8</td><td>13</td><td>15</td><td>12</td><td>9</td><td>0</td><td>3</td><td>5</td><td>6</td><td>11</td></tr></table>

S盒的具体运算过程如下：由定义可知B表示一个6位的输入块，依据如上定义的S1函数表，计算S1(B)的方法是：使B的第一位和最后一位组合，因为两位二进制位能够表示的数的范围为00--11，即十进制0~3，所以该数可以对应表格中的某一行，设字母I表示这个数；接着将B中间的四位二进制进行组合，设字母J表示这个数，由于四位二进制表示的范围在0000--1111之间，即十进制0~15，故J总能对应表中的某一列；查找表中第I行第J列的数字，该数字介于0到15之间，可以由四位二进制唯一表示，这个结果就是函数S1输入B以后得到的输出S1(B)。例如，当输入B=011011时，第一位是0，最后一位是1，这两位组合为01，即代表行号数是1；中间4位是1101，换算成十进制数为13，其决定列号数为13；此时查找表中的第2行第14列得到数字5，用四位二进制数表示为0101，因此输出结果是0101，也表明S1(011011)=0101。其余的S盒运算以同样的方式可算得结果。

（4）P盒置换

由上述可知，每个S盒产生一个4位输出，则8个S盒总共产生32位输出，将上面得到的32位数据作为P盒运算的输入，按照P盒置换表进行变换。

表3-14 P盒置换表

<table><tr><td>16</td><td>7</td><td>20</td><td>21</td></tr><tr><td>29</td><td>12</td><td>28</td><td>17</td></tr><tr><td>1</td><td>15</td><td>23</td><td>26</td></tr><tr><td>5</td><td>18</td><td>31</td><td>10</td></tr><tr><td>2</td><td>8</td><td>24</td><td>14</td></tr><tr><td>32</td><td>27</td><td>3</td><td>9</td></tr><tr><td>19</td><td>13</td><td>30</td><td>6</td></tr><tr><td>22</td><td>11</td><td>4</td><td>25</td></tr></table>

参考上表，将原数据的第16位转变为新数据的第1位，将原数据的第7位变换为新数据的第2位，其余以此类推。

（5）异或运算

一方面，使本轮起始输入的左半部分数据与经过P盒置换表运算输出的数据执行异或运算，产生的结果被用来作为下一轮输入的右半部分数据；另一方面，本轮初始输入的右半部分数据直接进入下一轮作为输入的左半部分数据；截止到这里，一轮迭代运算过程已经结束。

3.5 终止逆置换

经过16轮的迭代运算可以得到L和R，此时交换这两部分数据的顺序变为R和L，将这两部分的数据合并作为终止置换的输入数据，按照终止置换表进行变换。

表3-15 终止置换表

<table><tr><td>40</td><td>8</td><td>48</td><td>16</td><td>56</td><td>24</td><td>64</td><td>32</td></tr><tr><td>39</td><td>7</td><td>47</td><td>15</td><td>55</td><td>23</td><td>63</td><td>31</td></tr><tr><td>38</td><td>6</td><td>46</td><td>14</td><td>54</td><td>22</td><td>62</td><td>30</td></tr><tr><td>37</td><td>5</td><td>45</td><td>13</td><td>53</td><td>21</td><td>61</td><td>29</td></tr><tr><td>36</td><td>4</td><td>44</td><td>12</td><td>52</td><td>20</td><td>60</td><td>28</td></tr><tr><td>35</td><td>5</td><td>43</td><td>11</td><td>51</td><td>19</td><td>59</td><td>27</td></tr><tr><td>34</td><td>2</td><td>42</td><td>10</td><td>50</td><td>18</td><td>58</td><td>26</td></tr><tr><td>33</td><td>1</td><td>41</td><td>9</td><td>49</td><td>17</td><td>57</td><td>25</td></tr></table>

按照表3-15的规则，使输入数据的第40位转变为新数据的第1位，第8位变换为新数据的第2位，其余位按同样的方式进行调换；这步操作完成后得到的64位新数据就是单个分组最终加密后的密文。

4 系统设计

4.1 系统概要设计

本课题的设计采用了Web应用开发技术，在DES加密算法的基础之上实现了一个文件加密网络传输系统。整个应用系统基于B/S的架构模式被划分成两个部分：浏览器端和服务端。服务端是指可以提供后台服务并由许多个用户共享的应用程序；浏览器部分为每个用户所专有，主要用来执行前台功能，如完成用户界面显示、接收数据输入和向后台数据库发送请求并接收返回结果等。浏览器的使用对象主要有用户和管理员；服务器端的应用程序为数据库。系统整体可以划分成身份认证、系统管理、文件传输、加解密和文件管理等这几个应用模块且其所有功能的实现都是在后台通过编写程序完成；系统结构设计图如图4-1所示。

6

7

8

9

10

11

12

图4-1 系统结构设计图

4.2 系统总体功能设计

系统浏览器端的使用对象主要有两类：用户与管理员；

用户部分：a）注册、登录；

b）模糊查询，用户可以通过输入文件的名称来检索文件信息；c）分类查看，按照文件的分类进行文件信息查看；

d）文件传输，选择文件以后，对文件进行加密传输；

e）文件接收，获取文件后在线解密查看文件信息或下载到本地查看，也能够对文件进行归类管理；

f）个人信息维护；

（2）管理员部分：a）登录；

b）用户管理，对注册的用户进行增删改查操作；

c）分类管理，对文件区分类别进行增删改查操作；

d）文件数据量统计，按照时间段查看文件传输数量并以图形chat报表展示；

e）维护个人信息；

4.3 数据库设计

文件加密网络传输系统的实现过程中所涉及到的一些数据信息，如密钥、用户信息、文件信息的存储使用服务端数据库存储，服务器上采用MySql数据库管理系统。在数据库中分别建立用于存储个人数据信息的用户、管理员信息表；文件信息表，主要记录文件的类型和名称；文件统计表，主要用于记录各个用户时间端内发送的文件数量等。

5 系统实现

5.1 用户登录验证

从安全的角度来看，对于一个文件加密传输系统来说，系统本身的安全等级显得非常重要。如果不进行身份认证而允许任何用户随意进入系统，则

可能存在非法用户冒用他人的身份进行发送文件甚至窃取文件数据信息等不法行为，从而造成严重的后果，因此系统必须实施严格的访问控制策略。

目前，访问控制的常用手段有三种：自主访问控制、强制访问控制和基于角色的访问控制；本系统在登录时选择应用较为广泛的基于角色的访问控制方式原因有两点，其一：自主访问控制和强制访问控制的安全性不足；其二：基于用户的机制使得添加用户的操做以及实时性的功能操作较为困难。

系统将客户端的使用对象分为管理员和普通用户两类，第一次使用时首先要注册，个人信息被保存在服务端的数据库中，后面登录的时候，以用户输入的登录信息作为有效关键字查询用户信息表，如果表中有相对应的记录，则认定当前用户为合法用户，从而允许用户进入系统；如果在表中没有找到对应的记录，则显示用户名或者密码错误信息。

5.2 系统管理模块

管理员或者用户可以通过登录认证方式进入系统，以此使用系统相应的功能。系统基于角色分配相应的权限。用户只能看到自己的个人信息和有关文件的信息，可以使用近似搜索功能快速检索相关文件并在相应的用户权限中更改自己的密码；与普通用户相比，管理员不仅可以查看自己的信息，还可以查看所有已注册的用户信息，添加、删除和更改当前用户数，更改自己的密码和用户密码。

5.3 文件传输模块

当用户想要发送文件给另一个用户的时候，首先在自己的数据库当中浏览并找到要发送的文件，然后选择文件的发送对象，最后点击发送即可；与此同时，当有用户发送文件给自己时，可在自己的数据库中看到对方发送过来的文件，可点击下载按钮，选择文件的保存路径，待下载完成后查看文件信息，也可点击查看按钮在线阅读文件内容。

5.4 加解密模块

此模块为系统的核心构件，系统通过线性同余法随机产生一个64位的密钥，对明文进行加密以及对密文进行解密；所以不管待发送信息的用户将要传输什么文件给另一个用户，都需要经过加密处理，使得信息以密文的方式在网络信道上传输；而作为接收方的用户想要获取文件数据信息的时候必须先进行解密操作，否则难以获得有效数据，即若是文档，则不经过解密操作会以乱码的形式显示文档内容，若是图片，就会显示图片已损坏不可看，这在一定程度上保护了用户的个人信息安全，从而确保自己传输的信息被正确的对方接收和查看。

5.5 文件管理模块

在用户与用户传输信息的过程中，信息的类别不是单一的，例如文件类型的有pdf、word，纯文本信息的有txt，图片有jpg、png等，管理员可对这些类型执行增删改查操作，同时用户也可以根据类型查看文件；系统也会在不同的时间段实时统计用户发送的数据量，并以图形chat报表的形式显示。

6 系统测试

6.1测试目的

测试的目的应是尽可能少地使用人力、物力和时间来检测系统中的各种隐藏缺陷和故障，并通过修复潜在的漏洞与缺陷来提高系统的质量和避免安全风险；同时，测试不仅是一项旨在评估程序或系统有效性的活动，而且也是对系统运行效果的度量和评价的过程，借此来验证系统的整体水平是否满足用户的需求，从而为用户选择和接收系统提供更直接有效的依据。

6.2 测试结果

7 结束语

本文在深入研究DES加密算法原理的基础上，提出了一种文件加密传输设计方案，有效地保证了用户之间信息的安全可靠传输，以防止文件数据在传输过程中被窃取和泄露。基于加密算法的文件传输系统经过多次的调试与修改，最终实现了文件传输、文件加密、文件接收、文件解密等主要功能。

在老师的精心指导与周密安排下，历时近两个月的毕业设计终于顺利完成；毕业设计是对即将毕业的同学们的一次重要考验，它不仅要求我们综合运用所学理论知识与技能，还要求我们具备一定的研究问题、分析问题和解决问题的实践能力。通过完成毕业设计，可以使我们巩固所学知识并将大学四年所学到的知识进一步融汇贯通，理论联系实际，将其投入到实际的应用当中。

在毕业设计的初始阶段，由于对加密算法的不熟悉，导致工作进度迟迟没有进展，很是焦虑，也尝试过很多办法，但都以失败而告终。但一次次的失败经验告诉我，车到山前必有路，坚持下去一定能够找到解决的方法。就这样，我在一次次的尝试过程中逐渐地找到了思路，我提前构思好系统要实现哪些主要功能，同时思考某些功能的实现要依赖于什么算法，程序设计使用什么开发工具和什么开发语言，系统采用什么架构以及使用什么框架来搭建整个项目等等，然后就对自己感到非常陌生的算法做深入的研究直到自己搞懂算法的原理，前期理论工作都完成以后，就可以进入实践环节了；实践环节对我来说也是一项艰难的任务，因为自己的编程水平有限，调试程序的能力也很欠缺，所以出现了很多错误，多次造成项目的失败，最终，通过学习别人的代码，上网查阅资料，实现了系统的基本功能。

毕业设计的完成，不仅标志着大学教育阶段的结束，也为我们的学校教育和生活注入了浓墨重彩的一笔！但是学习永远不会结束，一个学习阶段的结束也预示下一个学习阶段的到来，无论如何，我们要继续学习并掌握新的知识以更新我们的知识体系；最重要的是将获取的各种知识运用到实践当中，从而提升自己的综合能力。

本文对基于加密算法的文件系统的研究取得了一定的成效，但由于个人能力和时间有限，系统还有很多的改进之处，主要包括以下几点：

（1）系统的加解密密钥传输问题没有考虑全面，虽然传输的文件信息实现了加密，但从一定意义上分析可知，密钥的加密传输显得更为重要，因为密钥一旦被截获，信息加密也无实际意义。

（2）繁琐的密钥管理问题，一对用户就要管理一个密钥，那么多对用户之间就要管理多个密钥，具有一定的开销。

（3）系统的整体安全性有待提升，可结合RSA算法或增加数字签名功能以进一步优化。

参考文献
[1]赵萍.保护文件传输中DES加密算法在数据安全中的应用[J].黑龙江科技信息,2017(14):176.
[2]李翔宇,于景泽.DES加密算法在保护文件传输中数据安全的应用[J].信息技术与信息化,2019(03):23-25.
[3]贾伟,朱磊.DES加密算法在网络通信中的实现[J].网络安全技术与应用,2020(03):34-36.
[4]肖迪尹，付红. DES加密算法在通信中的运用[J].电子世界，2017(17).
[5]曾清扬. DES加密算法的实现[J].网络安全技术与应用，2019(07).
[6]杨波.现代密码学（第四版）[M].北京：清华大学出版社，2017,01.
[7]刘建伟，王育民.网络安全（第三版）[M].北京：清华大学出版社，2017，05.
[8]耿欣月.基于des算法的文件加密研究[J].信息与电脑(理论版),2020,32(03):44-46.
[9]李中豪.关于网络信息安全中DES数据加密技术的研究[J].数码世界,2018(8).
[10]余启航,李斌勇,杨雄凯,姚瑶.DES加密算法的过程分析研究[J].网络安全技术与应用,2018(02):43-44.
[11]李玲玲.计算机数据通信对DES数据加密算法的应用研究[J].数码世界,2018(12).
[12]黄海荣,马君英.DES数据加密算法在计算机通信中的应用[J].信息技术与信息化,2019(12):98-100.
致　谢
过去总是期待着夏天，因为会有暑假在等着我，但这个夏天却没有暑假了，只剩下毕业与告别。
感谢那些在我生命中最重要的时刻与我同行的人，你们是那般的可爱又迷人，让人难忘又不舍，也不知道是否还能与你们相遇在未来，此时的告别最想对你们说的就是感谢与祝福。
无论是老师，还是同学，都给予了我无微不至的关怀，不只是学习上的，还有生活上的，我在学校收获到的最珍贵的东西不只是知识、学位证和毕业证，还有那些无论如何都放不下的友情，祝你们前程似锦、未来可期。
论文写着写着就写完了，人走着走着宿舍就空了，看着空荡荡的宿舍，内心感慨万千；同时，由衷地感谢校领导、答辩老师、指导老师对我的指点与照顾，让我能够顺利的通过毕业答辩，也更加坚定了我努力提高学术能力的信念！感谢你们给我信心、给我光芒，让我不再心存负担无力向前，你们是我大学阶段遇到的贵人!
正所谓桃花潭水深千尺，不及老师教我情，您的恩怀我一定不会忘记的，感谢您耐心地给我一遍又一遍的答疑解惑，您这么好的老师以后一定能够受到学生的爱戴。请允许我用最诚挚而淳朴的祝福语感谢您！
最后还要感谢我的父母。“父兮生我，母兮鞠我。抚我畜我，长我育我，顾我复我，出入腹我，欲报之德，昊天罔极！”当初拿到论文选题时，我最真实的想法就是“这必定是一个短绠汲深的任务”，但我不仅挺过了难关，而且还成功的拿到了毕业证和学位证，感谢你们把我培养得这么好，养育之恩感天动地没齿难忘。
感谢每一位愿意看完我论文的老师，你们辛苦了！再次对各位老师表示衷心的感谢！
附　录

二、相似详情

序号	标题	文献来源	作者	发表时间
1	网络安全的 试题1(附答案) - 百度文库	学位论文		
2	MySQL数据库(一)——基本介绍_初叙-CSDN博客_mysql数据库介绍	互联网		
3	用户登录功能的实现-CSDN论坛	会议		
4	教育资源库体系结构与功能.ppt_人人文库网	互联网		
5	方位词in , on , to 的用发和区别_360问答	学位论文		
6	文件加密的重要性以及加密方法- 百度文库	互联网		
7	文件传输加密的重要性- 知乎	文献期刊		
8	得到的子密钥序列与明文进行异或运算.doc	本地库		
9	云存储数据机密性保护方法技术_技高网	本地库		
10	网工常见面试题(二)_加密	互联网		
11	计算机网络安全中数据加密技术的应用	图书		
12	2019年人工智能考试答案.docx	互联网		
13	数据安全 治理白皮书_安恒信息 - 道客巴巴	互联网		
14	第三章 密码 学	会议		
15	第三章密码学	互联网		
16	文本加密服务网站设计【文献综述】 - 百度文库	学位论文		
17	计算机网络与信息安全课件-第4章密码学-金锄头文库	互联网		
18	基于熵的信息隐藏算法研究- 道客巴巴	互联网		
19	DES加密算法的研究与实现的开题报告_图文 - 百度文库	文献期刊		
20	国内外 信息 安全研究现状及发展趋势 - 百度文库	互联网		
21	量子加密在视频通信中的应用 - 道客巴巴	互联网		
22	国内外信息安全研究现状及发展趋势	互联网		
23	浅谈网络信息安全与防护 - 道客巴巴	互联网		
24	量子密码 - 豆丁网	本地库		
25	DES加密算法重点 详解.doc	互联网		
26	加密与解密技术原理(密码学)_木_木的博客-CSDN博客_加密解密原理	图书		
27	第四章系统设计 本 章主要 根据 需求 分析的结果和要求进行系统...	互联网		

28	大学 计算机 基础知识选择题 - 百度文库	互联网		
29	计算机网络课件(蔡开裕)——Ch9 网络安全- 道客巴巴	互联网		
30	第四章密码学基础1_图文_百度文库	文献期刊		
31	北邮《网络与信息安全》期末复习题(含答案) - 百度文库	互联网		
32	网络与信息安全--期末复习题 - 百度文库	互联网		
33	电子商务判断 选择 题课后答案 - 百度文库	文献期刊		
34	办公自动化保密管理(一).ppt	文献期刊		
35	密码学概论系统课件.ppt	互联网		
36	第2章现代密码学精讲课件.ppt-全文可读	文献期刊		
37	软考信息安全工程师笔记(第二章--密码学基础与应用)_夜司晨的博客-...	互联网		
38	信息安全技术与实施第四章习题 - 百度文库	互联网		
39	数字签名的算法及应用分析_爱学术	互联网		
40	Java密码学原型算法实现——第二部分:单钥加密算法- CSDN博客	文献期刊		
41	第十六章计算机密码学	互联网		
42	第3章数字签名与身份认证技术.PDF	学位论文		
43	基于DES算法的文件加密研究- 道客巴巴	互联网		
44	计算机网络安全教程(第三版)第九章简答题答案_Long_UP的博客-...	互联网		
45	DES加密算法原理_张维鹏的博客-CSDN博客	互联网		
46	一种简易的文件安全传输系统的设计与实现_图文_百度文库	互联网		
47	密码 算法 原理与实现: DES加密算法 _慢雾的博客-CSDN博客	学位论文		
48	AES 加密 算法_旋转的Kumamon的博客-CSDN博客	图书		
49	CBC加密 - 百度文库	学位论文		
50	信息安全习题答案2-4章_文档之家	学位论文		
51	CBC 加密 原理及攻击 - Hanamizuki花水木 - 博客园	会议		
52	...大数据私房菜的个人空间 - OSCHINA - 中文开源 技术 交流...	互联网		
53	对称 加密算法 之分组 加密的 六种工作 模式 (ECB、CBC、PCB...	会议		
54	流密码 —— 使用块密码 实现的 流密码 - 简书	学位论文		
55	密码学第一次实验报告:DES算法与差分攻击- 简书	互联网		
56	CBC加密原理及攻击- Hanamizuki花水木- 博客园	本地库		
57	AES加密与Base64编码(加解密、签名系列)_zp17764507932的博客-...	图书		
58	密码学第一次实验报告:DES算法与差分攻击- 简书	会议		
59	密码学(五)_Airths 的博客-CSDN博客	图书		
60	分组对称 加密模式 ECB-CBC-CFB- OFB 介绍 - 百度文库	互联网		
61	信息安全实验报告DES加密算法-金锄头文库	本地库		
62	密码学题库_Lee notes-CSDN博客	图书		
63	MD5 加密算法的安全性 分析与改进_图文 - 百度文库	互联网		
64	0836《信息 安全 》西南大学网教19秋作业答案 - 百度文库	互联网		
65	[原创]DES算法的介绍以及实现(含上次DES程序1.0的源码) - ...	会议		
66	DES算法加密_数据结构与算法_qq_36339794的博客-CSDN博客	互联网		
67	网络信息安全第2章密码技术 - 豆丁网	文献期刊		
68	...03(AES算法)_reforever的博客-CSDN博客_rijndael算法不存在弱密钥	互联网		
69	微型计算机原理及应用第四版课后答案_图文 - 百度文库	互联网		
70	DES实验报告 - 百度文库	图书		
71	B/S中的三层架构和MVC设计模型_颺灏的博客-CSDN博客	本地库		
72	Java Web基础——JavaEE第一次作业- 彭争杰- 博客园	图书		
73	基于模糊查询技术的文件检索系统研究- 道客巴巴	学位论文		
74	使用 C 语言 查看 一个 文件夹 中所有 文件 及目录_zhangge3663...	学位论文		
75	如何给 文件 资料 加密传输 - 百度经验	文献期刊		
76	用户管理系统之增删改查操作_Dragon_Python的博客-CSDN博客_...	互联网		
77	【期末复习】带着问题看网络信息安全_不忘初心,护天下安全...	图书		

78	... 强制访问控制和基于角色的访问控制, 它们具有不..._考试...	学位论文		
79	用户登录界面用户登录界面用来实现对用户的管理。登录时用户需要...	文献期刊		
80	...培养 我们综合运用所学 知识独立地分析问题和解决问题的...	图书		

三、免责申明

- 报告编号系送检论文检测报告在本系统中的唯一编号.
- 本报告为中国学术不端论文检测系统算法自动生成，仅对您所选择比对资源范围内检验结果负责。