基于 DES 算法的文件加密研究

耿欣月

（辽宁师范大学海华学院，辽宁 沈阳 110000）

摘 要：在网络时代，计算机应用到了各个方面，与之匹配的网络技术也在快速发展，网络间通信数据大量增加。传输的数据如用户个人信息、商务数据或者其他方面的文件，都涉及每位用户的机密，因此采用加密技术保护文件就显得很重要。为了提高网络中数据传输的安全性，笔者利用 C# 作为文件加密软件的开发软件，通过针对对象进行程序设计，在数据加密以及密码设置上采用 DES 加密算法，能够满足用户对文件的安全性要求。

关键词：DES 算法；文件加密；C++

中图分类号：TP309.7 **文献标识码：**A **文章编号：**1003-9767（2020）03-044-03

Research on File Encryption Based on DES Algorithm

Geng Xinyue

(Liaoning Normal University Haihua College, Shenyang Liaoning 110000, China)

Abstract: In the network era, computers are applied to all aspects, and the matching network technology is also developing rapidly, and the communication data between networks is increasing greatly. The transmitted data, such as personal information, business data or other documents, all involve the confidentiality of each user, so it is very important to protect the documents with encryption technology. In order to improve the security of data transmission in the network, the author uses C# as the development software of the file encryption software, through the object-oriented programming, in the data encryption and password setting, the DES encryption algorithm can meet the user's requirements for file security.

Key words: DES algorithm; file encryption; C++

0 引言

信息安全是一个综合性的跨科学领域，涉及数学、密码学、计算机、通信控制、人工智能、安全工程、人文科学和其他科学，是近年来发展快速的一个热门领域。信息对抗和互联网安全是信息安全的核心，它的研究和发展工作将是强有力的，以推动和促进与信息安全相关的学科研究与发展[1-2]。

网络技术的不断发展使人们的生活变得更加丰富，而且工作效率和生产效率都得到有效提高，在网络技术带来极大便利的同时，网络安全问题也成为一个不可避免的话题。连接在互联网上的计算机每时每刻都有被黑客攻击的可能，在网络上发送和接收的文件也有可能被黑客拦截，而这种不安全的因素在 TCP/LP 协议中肯定会有的，因此必须对重要的文件进行加密。为了保证数据的安全性，有必要利用计算机网络安全技术、密码学和计算机网络相关的知识，设计一个文件加密软件对文件进行加密和解密。

1 课题现状及发展趋势

1.1 发展和问题

目前，计算机网络技术和计算机信息技术飞速发展，已经大量应用在国防、军事、电子商务行业、服务业和医疗等方面。可以说每一个企业，甚至是每一个生活在这个时代的人都离不开计算机，使用计算机管理数据，而且政府也利用互联网给广大的群众提供了很方便的服务。无论是个人信息还是部门信息，这些信息都应以电子形式存储在一台机器上，然后再进行处理和交付。

简单来说就是，要保证这些重要数据在计算机的存储过程中是完整的、没有被改变或泄露；必须保证这些重要数据在整个传输过程中没有缺失、保证真实性、可以被读取。人们传输数据的最终目的是使数据传输到目的地后仍能使用，所以有必要在不影响电子文件可控性的情况下提前确保存储

作者简介：耿欣月（1997—），女，满族，河北承德人，本科在读。研究方向：计算机科学与技术。

的安全性。

1.2 电子文档的存储威胁

要保证数据能正常使用，在存储技术的安全问题上应考虑以下几个方面。第一，电子文件的合法创建和存储。第二，对电子文件确认修改和删除情况。第三，保护电子文件的信息安全。第四，确保数据不泄露。第五，避免在数据传输过程中出现信息缺失。第六，阻止来自网络的数据入侵者，防止数据被盗取或者被破坏。

数据在存储问题上面临的威胁主要表现在以下几个方面。第一，冒充。这主要表现为非法的数据入侵者侵入计算机后对数据操作，使计算机认为该数据是合理的。第二，否认。这一表现与上面的冒充行为有很大联系，计算机需要知道来访者身份时否合理，还会通过验证来访者的方法，让其他来访者承认自己的行为合理。第三，数据泄露。泄露表现为非法入侵者进入计算机系统后对数据进行盗取（如果盗取的数据十分重要，如金融方面的数据，则会对其他人员造成严重影响，甚至产生利益损失）。第四，数据丢失。计算机数据往往存储在硬盘或者是软盘，作为一种物理存在的东西在使用中可能出现遗失或者被偷盗，相对于其他行为这是被动的泄露行为。第五，数据被销毁。当非法入侵者盗取数据后，可能会私自删除或者修改数据，使传输的数据无法使用。

1.3 国内现状及发展趋势

现在国内关于如何对电子数据及相关重要文件进行保护的问题上，主要通过建立防火墙和研发扫描工具对网络数据进行安全性检查。防火墙技术实际上是一种特殊的系统程序，在所有数据到达计算机内部前，都会经过计算机外部网络检测和筛选。这是网络安全的第一个障碍。访问控制功能上增加一个访问权限，不同的用户在访问数据时有不同的权限，同时每一位用户在访问时必须提供正确的身份，并在传输时对数据进行加密。采用加密算法对用户储存或者传输的数据进行处理，能够使非法用户很难对信息进行解密，从而阻止了数据被非法用户窃取。这种方法使用的是抽象算法，可以保证抽象数据的完整性并实现不可抵赖性。

在安全技术方面，我国与其他国家至少有 5 ～ 10 年的差距。这主要是由两个原因造成的：一方面，我国的应用技术发展总体滞后；另一方面，我国的网络技术在商业领域还不广泛，而且技术水平较其他国家低。我国在网络技术上起步晚，但近年来发展速度飞速提升，在某些领域上逐渐赶上其他发达国家。20 世纪 80 年代中期，我国就已经逐步发展网络安全技术和网络保密系统，而且慢慢地将相关安全系统应用到其他行业。其中的一些技术在安全性和实用性上都赶超了其他国家。20 世纪 90 年代中期，我国互联网技术迎来了新的机遇，在这个新时期实现了快速发展，正在孕育新的飞跃。

2 相关知识介绍

2.1 DES 算法描述

DES 是一种世界公认的标准加密格式，自产生到已有 15 年的历史，算是比较可靠的算法。在 20 世纪 70 年代初，由于需要对不同算法进行加密，使各通信在传输上互不干扰，就需要研发出一种通用的算法，因此美国的安全局对这种技术提出招标。在加密技术研发靠前的 IBM 公司最先提出 Lucifer 算法，这种算法最终改名为 DES 算法。美国安全局最终是在 1976 年 11 月 23 日将 DES 算法定为标准的加密算法。

DES 其实是通过数据分组进行加密，在分组上采用的是 64 位分组，具体就是在加密算法的输入端为输入 64 位明文，而输出的为 64 位密文，它在两端算法上都是采用分组加密（但密钥的设置上有区别）的对称加密算法。密钥的长度为 56 位，它也可以是任意的 56 位数，而且可以随时更改密钥。

DES 算法由密钥（Key）、数据（Data）、模式（Mode）3 个入口参数组成。密钥入口上是 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。

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）。

对于通信网络的两方，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，使用相同的密钥对密码数据进行解密，并重新构建构成数据的代码核心。通过确保密钥和密码的一致性，能够保证数据是安全的、完整的、未被篡改的。

随着网络技术的快速发展，与之对应的网络数据加密也在快速进步，在评判加密技术好坏上主要以算法加密和解密的能力为主。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带来了可靠的保障。

2.2 文件加密的方法

2.2.1 非对称加密技术

使用不同密钥的加密和解密方式称为非对称式加密，大多数情况下一般有两个密钥，称为公钥（public key）和私钥（private key），它们需要同时配合起来使用，不然就不能打开加密的文件。公钥是公共密钥，私钥是只有所有者才知道的密钥。在通信中，如果采用对称加密技术，密钥就不能让其他人知道，但如果采用非对称加密技术就可以公开一个密钥，而不必担心其他人知道密钥后对自己数据造成威胁。只要自己有另一半密钥（即私钥）就可以对加密的数据解密，

这样也可以保证传输的数据不会泄漏。

与对称加密技术类似，非对称加密技术也是公开密钥的一部分，不过它还有一个非公开的私钥。在密钥加密的过程中，分为加密和解密两部分，因此就产生了加密密钥和解密密钥，为了方便技术交流，加密部分可以公开，但解密部分只有加密者知道。加密者通过采用对方的公钥文件对文件进行加密，而解密者是通过用自己的私钥进行解密处理，加密方法使得不可能从加密密钥推断出解密密钥。

2.2.2　对称加密技术

对称式加密是使用相同密钥的加密和解密方式，通常称为“会话密钥”，这种密钥技术使用的较多，典型采用对称加密技术的是美国安全局最初使用的 DES，在密钥长度上为 64 位。

对称加密技术利用的是对称密码系统，在对称密码中，加密方和解密方使用同一个密钥。DES 算法是在加密过程中常用的对称加密算法。DES 算法是一种强块密码，使用移位变换和替代变换进行重复利用。实质上，它属于一种具有很强的抗解码能力的密码系统。

3　DES 算法的实现

文件加密软件主要由选择文件、输入密码、加密、解密、保存路径设置等几个部分组成。用户可以通过文件加密和解密等功能完成文件的加密和解密操作。

文件加密软件是一种特殊的算法，它可以改变原始信息数据，使未经授权的用户即使获得已加密的信号但又不知道解密的方法，也无法理解信息的内容。为了实现这个功能，对目标文件进行有效的加密，生成加密文件，保证信息的安全性；同时，可以对加密文件进行解密，使文件还原，以确保可以正常使用以前的文件。

3.1　DES 算法密钥的生成

用户通过输入密码的方式生成传统文件加密系统的密钥，如果密码过短，那么密码的安全性就低，如果密码过长或者密码十分复杂，会容易忘记。因此，本文在针对这个问题上采用的是统一管理密钥，文件进行加密和解密操作后的密钥都会保存在软件中，而且还会随着数据的传递出现。所以这种存储方式是不安全的，密钥可能会在传递过程中泄露，因此需要将密钥与计算机分开。只要密钥是独立存在的，就可以保证密钥的安全，其他智能卡或者模拟程序也不能读取密钥。因此，生成密钥可以从以下几个方面出发：第一，可以在算法上进行改进，比如将椭圆曲线算法（ECC）应用到加密算法中，会比 DES 的算法快上百倍；第二，由于网络文件数量庞大，因此如何对它集中进行加密值得研究；第三，在协议中如何有效、安全地传输数据；第四，如何安全使用不可逆的加密体制。

3.2　DES 算法的加密操作

加密数据时要先选择待加密的源文件，并改变加密文件的首选路径，在对密源文件加密的时候则不能对路径操作，整个加密步骤都需要输入加密密码。用户可以选择易于记住但不易被其他人猜到的英文、数字和符号的结合作为密码。用户可以采用不同的方式记写，然后再进行解密步骤。

在加密过程中，加密数据由初始向量和密钥变换 16 次后数据就转换成密文。然后开始计算源文件的大小，并确定缓冲区的大小，在这个过程中还要不断改变加密流的大小。在加密过程中需要定义一个标准的算法例子，才能把数据成功转化成加密流。在数据转换程中，一次能转换 1 000 字节，在读取后就关闭源文件，每读取一次并转换完成后再进行下一次换换，直到完成所有数据加密。经过加密后，找到加密文件，可以看到全部是密文形式，文件大小和加密前一样。

3.3　DES 算法的运行效率

生活中用的最多的是 Word 和 Excel 文档，如果能对这些数据进行加密，文件安全性就能提高，不过每次都需要输入密码进行解密，会影响工作的效率，因此需要寻找一种更加方便的办法。基于此，提出了访问控制的加密形式，访问控制不会改变文件数据内容，仅仅增加了一个访问权限。它在 NTFS 文件系统中，提供了一个权限设置和密码设置的功能，可以让其他用户在特定的目录中进行浏览，用户只要输入正确的密码就能浏览其他文件，并且可以进行其他存取操作。

4　结　语

本文首先研究了国内外文件加密软件的现状，进而研究了基于 DES 算法的文件加密技术。利用混合加密系统自定义算法对文件进行加密，在提高加密安全性的同时，可以让加密更加快速、方便。

参考文献

[1] 陈倩 , 陈建敏 . 基于 Python 语言的 3DES 算法优化策略 [J]. 计算机产品与流通 ,2019(11):152.

[2] 曾清扬 .DES 加密算法的实现 [J]. 网络安全技术与应用 ,2019(7):33-34.