信息化背景下会计数据加密算法研究

——以DES算法为例

吴艳红
湛江科技学院

摘　要：高速发展的网络对人们的工作和生活带来了越来越多的影响，也为人们的信息交流提供了便捷的渠道，进而改善了人们的生活和工作条件。但是，当数据通过网络传输时，存在安全隐患，尤其是重要的会计数据。一旦被犯罪分子截获和使用，可能会对数据所有者造成严重的危害。基于以上背景，本文的目的是研究在计算环境中使用DES算法对会计数据进行加密。本文运用了一种改进的量子遗传算法，并将其应用到DES算法的S-盒设计中，改善了S-盒的非线性，降低了差分均匀性，提高了DES算法的安全性。这种改进的DES算法通过使用两轮函数增加密钥长度和迭代处理，减少了迭代次数，进一步提高了算法的安全性，提高了加密过程的运算速度。发现DES算法的64个密文以及与原始密文相比改变的比特数在32位左右波动，说明了使用DES算法加密会计数据时应注意的问题。为了防止密钥丢失或泄露，密钥的有效性需要得到保证，这样才能保证成批的较短数据进行加密时保证它的安全性。

关键词：DES算法；会计数据；数据加密；加密算法

Research on Accounting Data Encryption algorithm under the Background of Informatization

-- Take DES algorithm as an example

Yanhong Wu
Zhanjiang University of Science and Technology

Abstract: The rapid development of the network has brought more and more influence on people's work and life, but also provides a convenient channel for people to have information exchange, and then improves people's living and working conditions.However, when the data is transmitted through the network, there are security risks, especially the important accounting data.Once intercepted and used by criminals, it can cause serious harm to the data owner.Based on the above background, the purpose of this paper is to study the use of the DES algorithm to encrypt accounting data in a computational environment.In this paper apply a modified quantum genetic algorithm and apply it to the S-box design of DES algorithm, which improve the nonlinearity of S-box, reduces the difference uniformity, and improves the security of DES algorithm. This improved DES algorithm reduces the number of iterations by increasing the number of functions, further improving the security of the algorithm and improving the operation speed of the encryption process.The discovery that the 64 cipherents of the DES algorithm and the number of bits changed from the original ciphertext fluctuate at about 32 bits explains the problems that should be paid attention to when using the DES algorithm to encrypt accounting data.To prevent key loss or leakage, the validity of the key needs to be guaranteed, so that a batch of shorter data is secure when it is encrypted.

Keywords: DES algorithm, accounting data, data encryption, encryption algorithm

本文系湛江市社科联学科共建项目“区块链技术背景下会计管理信息系统优化研究”（项目编号：ZJ21GJ03）阶段性研究成果。

一、引言与文献综述

当今社会是信息社会，数据是承载信息的基础。保证数据在传输过程中的安全具有重要的现实意义[1].当数据在网络上传输时，需要借助一定的媒体基础来完成，但是在通过网络进行数据传输的过程中，不可避免的会受到或多或少各种各样的攻击，这将影响数据的安全传输，是一个不小的威胁。数据拦截、中断、篡改和伪造、计算机病毒等都是数据安全传输的障碍。因此，提高网络传输过程中数据的安全，消除在传输过程中的各种威胁，通过有效地将DES加密算法应用到数据传输过程中，它可以有效地提高数据传输的安全性，避免其在传输过程中受到攻击，提供一个可靠的保证数据安全传输的加密方法。

在信息技术水平高的社会，其安全性不容忽视[6，7]。会计的信息资料包括很多，有发票类的、各种单据、各类账本和其他的会计基础资料。在会计信息化背景下，会计档案和资料有可能是纸质的，更多的是非纸质电子资料，在电子数据编辑、处理和管理的过程中，确保无纸化的电子资料的安全是非常重要的。开发人员、管理人员和用户需要仔细讨论该问题[8，9]。目前可以使用MD5、RSA、DES、AES、DSA等多种加密算法。其中，数据加密标准（DES）加密算法是一种对称加密方法，它是IBM在1972年开发的，更成熟的经典算法[10，11]。相对而言，DES加密速度快，算法简单实用，同时考虑安全性和效率要求[12，13]。本文描述了DES加密技术在会计数据处理中的应用，在保证效率的前提下实现了数据安全管理的目标[14，15]。

二、DES算法概述与设计

（一）DES算法加密原理

DES加密算法使用64位密钥，处理64位组明文或组密文。经过64位明文加密后，输出64位密文。64位密文被解密后恢复为64位明文。假设输入的64位纯文本为：$m_1m_2...\ m_i...\ m_{64}$（$1\leqslant i\leqslant 64$）；64位密匙是：$K=k_1k_2\cdots k_i\cdots k_{64}$（$1\leqslant i\leqslant 64$），其中56位为有效密钥，$k_8$、$k_{16}$、$k_{24}$、$k_{32}$、$k_{40}$、$k_{48}$、$k_{56}$、$k_{64}$均为奇偶位，在计算中不起作用。设T为循环迭代运算，整个加密过程可以用下式表示：

$$DES（M）=IP^{-1}（M）*T_{16}*T_{15}*...*T_2*T_1IP（M）\quad（1）$$

式中，IP为初始置换操作，IP^{-1}为逆初始置换操作。DES加密算法的加密流程图如图1所示。DES加密算法的加密流程可以概括为三个过程：初始置换操作、16轮迭代操作和逆初始置换操作。

（二）DES解密

DES是一种对称密码算法。解密和加密的过程是一样的。如果输入加密后的密文，就会输出明文，但是使用不同的密钥顺序。假设这16个重复操作中使用的子键

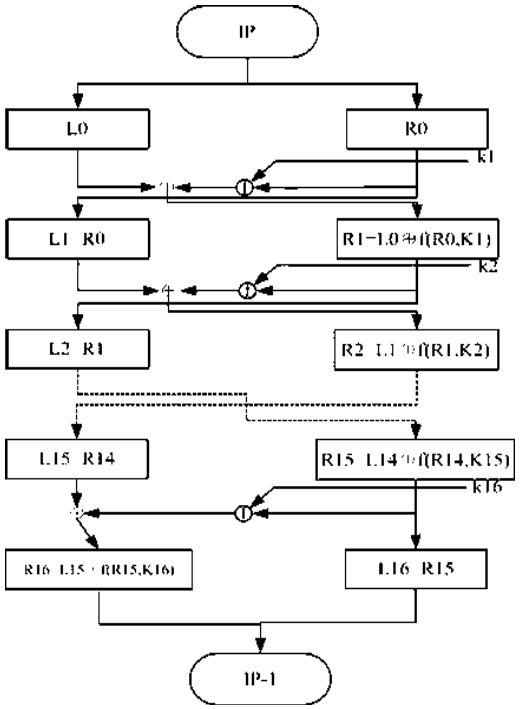

图1　加密流程图

为K_1，K_2，K_3，K_4，…K_{15}，K_{16}。解码时，从第一轮到第16轮使用的键为K_{16}，K_{15}，K_{14}，K_{13}，$K_{12}\cdots K_2$，K_1。换句话说，如果64位加密的文本作为纯文本输入，则解码过程的第一步。第一次使用K_{16}，第二次使用K_{15}，第16次使用K_1。相同的初始密匙生成加密和解密的子密匙，只是使用时顺序不同。初始置换和逆初始置换，解密与加密过程都一样。

（三）会计数据处理和传输过程

会计信息系统的数据处理包括录入、验证、审核、修改、删除和查询等基本操作。具体的数据处理流程为：采集会计信息、加工会计信息、储存会计信息、传递会计信息和输出会计信息。财务软件如金蝶、用友和SAP等都是企业集团常用的软件，这些企业集团是全国各地都有分公司，甚至全球，因此它们在全国、全世界范围内联网操作时，总是会有会计数据的传输，传输过程的安全问题不容忽视，因此采用DES加密算法，对会计数据加密，这样传输可以大大提高会计数据的安全性。会计数据编辑（添加、修改、删除等）的时候要考虑系统使用的业务类型、数据类型、状态等，财务软件系统是根据相关的业务规则处理批准的业务数据的。匹配业务规则时，将执行其中定义好的操作，而执行动作由程序代码实现。通过对企业会计准则的分析和抽象，将其业务规则对应的相关执行动作抽象为代码来实现。对于后续的业务规则编辑定义，映射执行操作。根据企业业务活动中不同的业务类型，梳理定义不同的业务执行动作集。分析会计数据的这些操作过程，是运用DES加密算

法的必要工作。

（四）文本化的密文

在信息化环境中，财务软件储存会计数据的方式通常是SQL数据库，通过账套来储存每个企业每个期间的财务数据，有文本类、数字类、日期类和逻辑类等等。在财务软件里导出数据，可以选择TXT、WORD、EXCEL等类型，TXT是纯文本文件，格式都是二进制的。当纯文本被加密为DES加密后，原始文本会变成非文本类型，数据存储或网络传输可能会出现问题。要解决这个问题，需要处理密文并将其转换为文本类型。将每个字节转换为与该字节对应的ASCII十六进制表达式。例如，字符“A”被转换为两个字符“41”，字符返回和换行被转换为四个字符“0D0A”。在发送和保存文本类型的数据时，文本化是确保安全的方法，但是数据长度增加了。所以在设计原始数据表格时要与加密数据的长度匹配。对文本加密后的文本进行解码时，必须将加密后的文本中的每两个字符拆分为组合，分析对应的十六进制值，恢复DES加密后的文本块，再进行DES解码。交换的重要功能是将对应的字符进行十六进制转换，并将对应的字符转换为十六进制。在文本化过程中可以考虑二次加密的方法，例如简单地改变数据位的XOR处理和字符序列，这样和DES一起运用，可以达到较高的加密效率和效果。

三、基于DES算法的会计数据加密的仿真验证分析

（一）实验帐套数据库中文本字段的加密处理

会计帐套中的基本信息、记账系统数据、用户名、身份证号码、联系方式、客户及供应商信息、库存名称等都是重要内容。一旦泄露，会给单位或个人带来安全风险。在开发过程中，底层的DES加密过程确保即使数据是由非法用户获得的，它也只能是密文，而纯文本内容是无法得知的。

此字段使用DES加密，并且值会发生大幅度变化。例如，密钥“12345678”可以对加密后的文本进行处理，但如果纯文本中的字符数不是8的倍数，则会添加空格。会计科目编码“1001”和“100201”的密文分别为“98b843260952f3b1”和“31e46014dbf66dcd”。“库存现金”这个会计科目的密文是“d171c6 dbb165019f”。会计帐套开始使用的日期密文为“2016年7月1日”。即“97bd605 ee088362016d67558ac2242f”，金额“1000.00”的密文为“77e70225251 d7487”。“00000000000”等特殊字符串加密，密文为“5f6a7d528e394f39”。综上可知，密文和明文的规则性是无法找到的。

因此可以将变长字符（VarChar）数据直接写入原始字段、固定长度字符串或其他类型的数据字段。VarChar字段必须设置为保存未加密的加密文本，也可以设置一个二进制文本字段来保存密文。考虑到效率问题，采用DES加密算法对会计数据加密时，可以选择只对某些字段进行加密，只要能达到安全需求即可，这样可以节约时间，提高效率。因为财务软件里的数据庞大，虽然DES处理速度较快，但是处理起来也是要耗用一定的时间，所以也要考虑时效问题。

（二）实验会计软件导出数据加密处理

财务软件如金地、用友等可以导出文件储存，类型可以选择导出Dbf文件、Excel文件、文本文件、Word文件等，也可以输出金蝶、用友等系统自定义的文件，自定义文件格式只能在金蝶、用友软件中打开，而其他格式的文件则可以由其他通用的软件打开，如Word文件可以在WPS、word2003–2016等地方打开，这就很容易泄露数据。因此涉及到导出的会计数据的加密，也可以执行DES加密。

在Excel表格文件或Vfp Dbf表中，可以加密表中的本地数据或整个文件。在文本文件、Word文件或自定义格式的会计软件文件中，可以对整个文件进行DES加密。在一些加密时，相关软件可以打开加密后的文本文件，但如果此时手动编辑加密后的文本，则无法解密，因此需要采取适当的保护措施。特别重要的机密数据采用多种手段确保数据安全。虽然采用DES加密，Word，Excel软件的原始加密方法也可以使用，压缩软件在压缩独立文件时也可以使用安全密码。

（三）会计数据密文分布分析

密文的分布是衡量加密算法安全性的一个重要指标。一个好的加密算法应该是均匀的，而不管明文分布是否均匀。如果密文分布不均匀，说明密文中存在一定的统计规律，攻击者通过纯密文攻击，可以利用这个统计特征来分析和破解算法。为了验证本文DES算法的安全性，对会计数据的明文文本使用DES算法进行加密，根据分布结果来分析该算法的安全性。

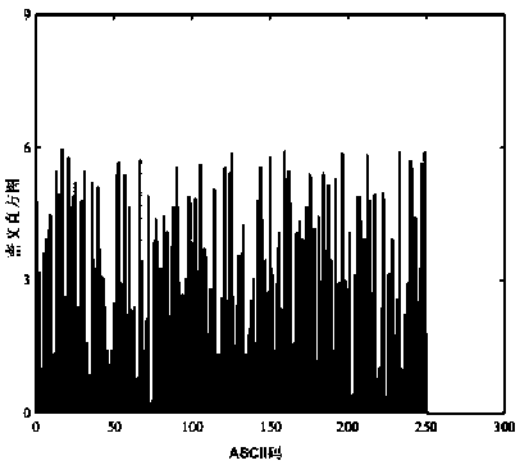

图2　密文直方图

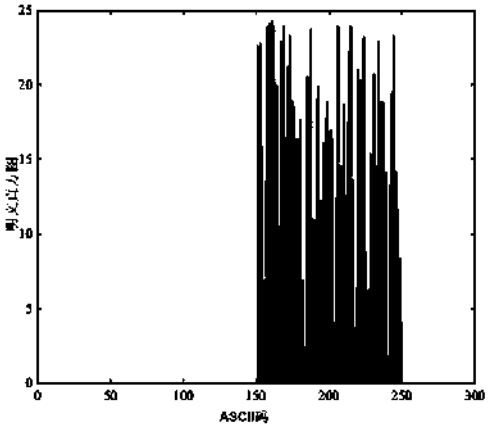

图3　明文直方图

因为在常规文本文件中字符的ASCII码在32–127之间，但是从图2可以看出，密文比较均匀地分布在0–255范围内，而明文分布在150–255范围内较为均匀，明文分布如图3所示。本文采用DES算法加密后得到的密文分布是均匀的，掩盖了加密前的分布规律，密文分析师无法通过统计特征来破解加密，因此可以有效地抵御解密攻击。

当加密算法生成的密文中0与1的比值接近于1时，说明该加密算法能够很好地将明文内容混淆为密文，能够有效地抵抗统计分析攻击。下面分别使用DES算法和一般算法对同一会计数据文本进行加密，然后分别计算初始明文和对应密文中0和1的个数。结果如表4所示。从表中可以看出，本文的DES算法和一般算法都可以减小明文中0和1个数的差距，但是DES算法中密文0和1的比值更接近于1，说明DES算法比一般算法具有更好的差分均匀性。

表4　初始明文与对应密文0、1个数的比较

数量和比例	明文	DES 算法密文	一般 算法密文
0的数量	1842	2147	2128
1的数量	2488	2183	2202
0的数量与 1的数量比值	0.7404	0.9825	0.9655

（四）会计数据的清晰文本敏感性分析

明文敏感性测试的目的是确定加密算法生成的密文对明文的变化是否非常敏感，明文的变化体现在同一个密钥位上。如果明文发生轻微的变化，对应的密文就会有很大的差异，说明加密算法对明文敏感，那么它对已知明文攻击和选择性明文攻击的抵抗能力很强。明文的灵敏度可以通过雪崩效应来衡量，即明文每一位的变化都会使密文的每一位发生变化的概率为0.5。为了验证本文提出的加密算法对明文敏感，随机生成一个长度为256位的初始密钥，并保持初始密钥不变。随机选择长度为64位的明文，然后按顺序选择每个明文。位反转得到仍然是64位长度的64位明文。本文所提出的算法用相同的密钥进行加密，生成长度为64位的64个密文组，将得到的64个密文与初始密文进行比较，结果如图5所示。

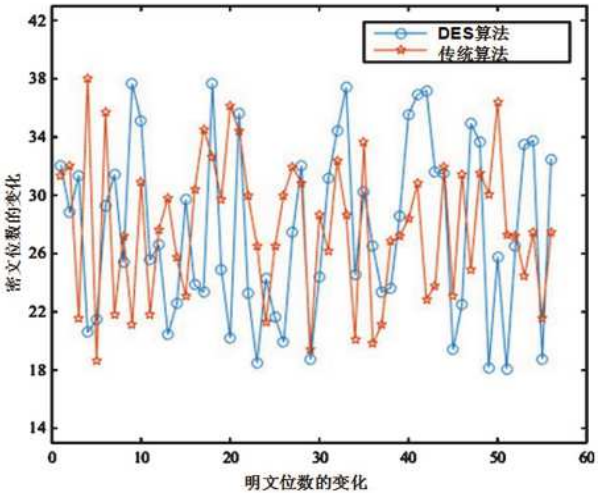

图4　明文敏感性比较

图4比较了本文DES算法与传统算法的明文敏感性。首先看DES算法的情况：从图4可以看出，当明文改变了1位，64位密文变化的数量在32位（最大的是40位，最小变化23位，平均变化位数为32.2656）左右波动，39位变化是在范围内的，占密文总数（64位）的比例为60.94%；其次看传统算法：如果明文改变1位，则密文变化位数也是32位（变化最多的是40位，最少变化17位，平均变化位数为31.5531）左右，范围内的变化是34位，占密文总数64位的53.13%。由这些数据可以说明本文的DES算法替换纯文本的能力要强于传统的算法，纯文本输入的每一位变化都会均匀地反映在每一位输出的密文上。

（五）运行速度测试及能量分析

一个密码系统是否合格最直观的表现就是它的运行速度。选择大小为1KB的文本文件使用DES算法进行加密和解密操作和本文的传统算法。比较了两种算法的运行速度。结果如表5所示。从表中可以看出，本文的DES算法耗时更短，加解密速度更快。与传统DES算法相比，速度提高了一倍左右。会计数据包一般为1KB左右。本文算法加解密时间约为1秒，可以满足会计数据的实时性需求。

表5　两种算法的加解密速度比较

算法	加密时间	加密速度	解密时间	解密速度
DES算法	1.114755秒	885.154 字节/秒	1.075704秒	927.562 字节/秒
传统算法	2.644188秒	367.018 字节/秒	2.360530秒	422.503 字节/秒

两种算法对不同大小文本的加解密耗时比较如图5所示。可以看出，无论数据量有多大，本文的DES算法都比传统算法快。

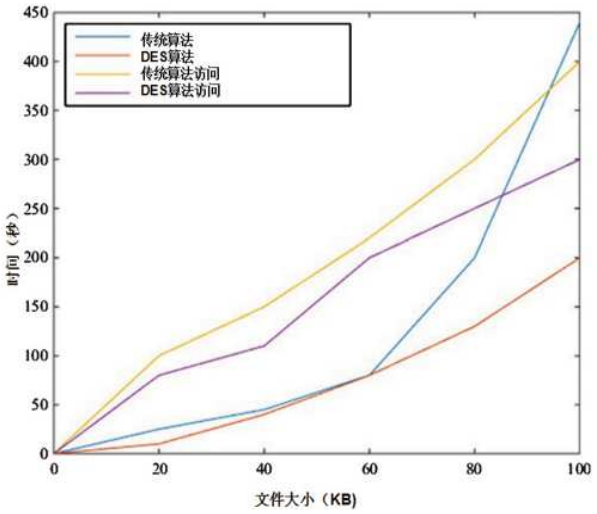

图5　两种算法的加密和解密时间比较

由于本文中的DES算法只使用异或、移位、置换和替换操作，而且解密过程和加密过程是逆序的，所以操作是相同的。因此，加密和解密操作时的计算量相对较小，计算消耗较低。此外，会计数据加密算法中的DES算法具有较低的能耗，本文的DES算法在传统算法的基础上进行了改进，减少了迭代次数，消除了初始排列和逆初始排列，因此消耗更少。

四、结语

加密技术不断发展，解密技术也在进步，因此之前安全的加密技术，在现在也不是那么安全。目前较多使用的是对称加密算法，对会计数据的加密起到了安全保障。本文主要研究DES算法，并对具体的步骤进行改进，让它更适合在无线网络的环境中安全传输。在分析总结了常用于会计数据加密的算法基础上，对DES算法和一般算法进行了比较。对所需要的存储空间进行了理论分析，并对其运行速度和通信带宽进行了仿真比较，分析了DES算法是最适合会计数据加密的算法。

参考文献：

[1]C.H. Chen, F.J. Hwang and H.Y. Kung, Travel Time Prediction System Based on Data Clustering for Waste Collection Vehicles, IEICE TRANSACTIONS on Information and Systems 102(7) (2019), 1374 - 1383.

[2]Yang Jiang, Guangfu Li and Weilong Che, A neutral dinuclear Ir (iii) complex for anti-counterfeiting and data encryption, Chemical Communications 53(21) (2017), 3022 - 3025.

[3]Liangliang Lu, Design of Wireless Blood Pressure Monitor and Its Data Encryption Method, Chinese Journal of Medical Instrumentation 42(3) (2018), 180 - 181.

[3]陆靓亮.无线血压计设计及其数据加密方法[J].中国医疗器械杂志，2018，42（03）：180-181+192.

[4]Amber Sultan, Xuelin Yang and A.A.E. Hajomer, Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON, IEEE Photonics Technology Letters (99) (2018), 1 - 1.

[5]Chen Shuai and Zhong Xian-xin, Research of Cipher Chip Core for Sensor Data Encryption, IEEE Sensors Journal 16(12) (2016), 1 - 1.

[6]Shadi Aljawarneh, Muneer Bani Yassein and We' am Adel Talafha, A Multithreaded Programming Approach for Multimedia Big Data: Encryption System, Multimedia Tools & Applications 77(6) (2017), 1 - 20.

[7]Baojiang Cui, Zheli Liu and Lingyu Wang, Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, IEEE Transactions on Computers 65(8) (2015), 1 - 1.

[8]Yinghui Zhang, Dong Zheng and Qi Li, Online/offline unbounded multiuthority attribute - based encryption for data sharing in mobile cloud computing, Security & Communication Networks 9(16) (2016), 3688 - 3702.

[9]D. Prashar, G. Chakraborty and S. Jha, Energy efficient Laser based embedded system for blind turn traffic control, Journal of Cybersecurity and Information Management 2(2) (2020), 35 - 43.

[10]Iti Sharma and C.P. Gupta, Making data in cloud secure and usable: Fully homomorphic encryption with symmetric keys, International Journal of Communication Networks & Distributed Systems 14(4) (2015), 379.

[11]Ghassan Sabeeh Mahmood, Dong Jun Huang and Baidaa Abdulrahman Jaleel, Data Security Protection in Cloud Using Encryption and Authentication, Journal of Computational & Theoretical Nanoscience 14(4) (2017), 1801 - 1804.

[12]Fu-Kuo Tseng and Rong-Jaye Chen, Towards Position- Aware Symbol-Based Searches on Encrypted Data from Symmetric Predicate Encryption Schemes, Ieice Trans Fundamentals A(1) (2016), 426 - 428.

[13]H. Abdel-Kader, M. Abd-El Salam and M. Mohamed, Hybrid Machine Learning Model for Rainfall Forecasting, Journal of Intelligent Systems and Internet of Things 1(1) (2020), 5 - 12.

[14]Sha Ma, Yi Mu and Willy Susilo, A Generic Scheme of Plaintext-Checkable Database Encryption, Information Sciences 429 (2017), 88 - 101.