MD5 加密技术在信息管理系统中的应用

邓霭霖

(1. 中山大学 数据科学与计算机学院， 广州 510006;)

摘要 ：信息的安全性已成为全社会关心问题，密码学研究也越来越被人所关注，而单向散列（ Hash ）函数是现代密码学的核心，最常见的散列算法有 MD5 、SHA、和 Snefru， MD5 是当今非常流行的优秀的典型 Hash 加密技术。针对当前网站建设和系统开发中用户信息等重要数据的安全问题，主要研究能够给用户密码进行加密的 MD5 算法。本文通过对 MD5 加密算法的研究，介绍了 MD5 算法的特性、算法原理及其算法流程。

关 键 词 ：MD5，加密算法，信息系统

Paper Title (use style: title)

ZHANG San[1], LI Si[2], LU Ren-jia[1]

(1. Dept. Name of Organization, Name of Organization, City ZIP, Country;

2. Dept. Name of Organization, Name of Organization, City ZIP, Country)

Abstract: Information security has become a problem of the whole society to care for, cryptography research was increasingly concerned, and one-way hash (Hash)function is the core of modern cryptography, the most common hashing algorithms MD5, SHA, and Snefru, MD5 is very popular in today's typical good Hash encryption technology. Website for the current security issues and user information systems development and other important data, the main research can give users the MD5 algorithm to encrypt passwords. MD5 algorithm is a relatively old, often widely used in the field of security. Through in-depth study of the MD5 encryption algorithm, and describes the characteristics of the MD5 algorithm, the algorithm principle and algorithm flow, and the practical application of the MD5 algorithm is given in a specific information management system, through the practical application of the results obtained in the test MD5 algorithm is a very safe and easy to use encryption algorithm.

Key words: MD5;encryption algorithm; information systems

一、绪论

随着网络通信技术和 Internet 之间的联系日益增强，出现了许多与网络安全有关的问题，例如对主机的攻击，网络上传输的信息被截取、篡改、重发等。由于它们对网络应用的发展和推进有着巨大的影响，所以密码体制就应运而生了。在一般情况下用户的资料信息是保存在数据库中，如果没有对数据库采取任何形式的保密措施，如果有人得到这些文件，那么所有的资料将会泄露。所以为了加强数据库的安全性，是非常有必要对数据库中的资料和文件进行加密，这样即使有人得到了数据，如果没有解密算法，同样不能查看数据库中的明文用户信息。对大量文件、资料、文档等储存加密，需要安全，高效的进行信息交换，同时此过程需要有效的组织和监控，对数据的存储和传输安全有着较高的要求。

（一）选题的背景及意义

随着网络技术的广泛应用，网络信息的安全将会得到越来越多的重视，最初的计算机程序上很少甚至没有安全性。直到后来人们才开始真正意识到数据的重要，才开始重视信息的安全。 MD5 加密技术是一种非常优秀的中间技术。通过该课题的学习，使我们能够更好的掌握 MD5 加密技术，在信息管理系统中做出更大的贡献。

（二）国内外研究情况

MD5 的全称是 Message-Digest Algorithm 5 （信息 - 摘要算法），早在 90 年代初由 MIT Laboratory for Computer Science 和 RSA Data Security Inc 的Ronald L.Rivest开发出来。 MD5 在 MD4 原有的基础上添加了 " 安全 - 带子 " （safety-belts）的概念。虽然 MD5 要比 MD4 更加复杂，但是它更加安全。 MD5 加密算法是一种免费的加密算法，它不但能对信息管理系统加密还广泛的应用于计算机，数据安全传输，数字签名认证等安全领域。

（三） **MD5** 的发展历史

MD5 是建立在 MD2 和 MD4 的基础之上的。它在 MD4 的基础上增加了 " 安全 - 带子 " （safety-belts）的概念。虽然 MD5 比 MD4 复杂度大一些，但却更为安全。这个算法很明显的由四个和 MD4 设计有少许不同的步骤组成。在 MD5 算法中，信息 - 摘要的大小和填充的必要条件与 MD4 完全相同。 Den boer 和 Bosselaers 曾发现 MD5 算法中的假冲突（pseudo-collisions），但除此之外就没有其他被发现的加密后结果了。

二、 **MD5** 算法介绍

（一） **MD5** 算法特点

MD5 算法具有一下特点：

1. 压缩性

任意长度的数据，计算出的 MD5 值长度都是固定的。

2. 容易计算

从原数据计算出 MD5 非常容易

3. 抗修改性

对原数据进行任何改动，即使只修改一个字节，但所得到的 MD5 值都有非常打区别

4. 弱抗碰撞

已知原数据和其 MD5 值，想找到一个具有相同 MD5 值的数据是很困难的

5. 强抗碰撞

想找到两个不同的数据，使它们具有相同的 MD5 值，是很困难的。

（二） **MD5** 算法原理

对 MD5 算法简要的叙述为： MD5 以512位的分组来处理输入的信息，并且每一分组又被划分成为 16 个 32 位的子分组，经过了一系列的处理后，算法的输出由四个 32 位的分组组成，将这四个 32 位的分组结合后将生成一个128位散列值。

1. 填充

在 MD5 算法中，首先需要将信息进行填充，使其位长对512求余后的结果等于448，即使其位长对512求余后的结果等于448，也必须要进行填充。因此，信息的位长将被扩展至N*512+448，N是一个非负整数，N也可以是零。

2. 添加长度

增加填充位之后，下一步就开始计算消息的原长，并将它加进填充后消息的末尾。首先去计算消

息的长度，不包含填充位。例如，如果原消息是1000位，则去填充472位，就是把它变成比512的倍数(即1536)少64位，但长度是填充位之前的长度（即1000），不是1472。

计算原始消息的长度（不包含填充部分）。并且附加到填充位与消息之后。该长度用64位表示。假如该消息的长度超过64位（也就是说，大于264），那么就只使用后64位。添加完成后，它就是最终的消息了（即，该消息是要散列的消息）

3. 将输入分成512位的块

4. 初始化链接变量

初始化四个链接变量，分别称之为A，B，C，D，它们都是32位的数字，这些链接变量的初始十六进制数值低字节在前 :A:01 23 45 67; B: 89 AB CD EF; C: FE DC BA 98; D: 76 54 32 10

5. 处理块

初始化之后，就开始实际算法了。这是个循环，对消息中多个512位块运行。

1）将四个链接变量复制到四个变量a,b,c,d中，使a=A,b=B,c=C,d=D。

2）将当前512位块分解成16个子块，每个子块为32位。

3）主循环一共有四轮，每轮都相似，每一个轮的操作，都要去处理一个块中的16个子块。这四轮中的第1步进行着不同处理，其他步骤是相同的。下面总结这四轮的迭代。每一轮输出的中间和最终结果都复制到寄存器abcd中，注：每一轮有16个寄存器。

①先是对b,c,d进行一次非线性的函数运算，此运算在四轮中都不同。

②把变量a加入第1步的输出中。

③把消息子块M[i]加入第2步的输出中。

④把常量t[i]加入第3步输出中。

⑤将第4步的输出循环向左移s位。

⑥把变量b加入第5步输出中。

⑦下一步的新abcd则是第6步的输出

三、 MD5加密算法与信息管理系统

（一）信息管理系统

以计算机为工具去收集、存储、分析和处理数据，得到管理人员需要的信息的系统。企业中的信息管理系统能很方便的帮助高级管理人员进行质量分析、市场预测、库存控制等工作。信息管理系统包含了很多方面，MD5也在很多不同领域的信息管理系统中应用。例如：电子商务、注册信息、数据库等等。

1. MD5在电子商务领域中的应用

在很多电子商务领域中，管理用户的信息账户是一种最常用的基本功能，尽管很多数据库服务器提供了这些基本组件，但是很多开发者为了管理起来更加方便依旧继续采用关系数据库进行管理。这种做法往往会将用户的密码过于简单的保存在数据库中，所以这些密码没有什么保密性。

2. MD5在数据库中的应用

网站往往将用户的账号和密码等信息使用非加密的方式储存到数据库，账号使用类为VarChar的UserCount字段，同样，密码也采用VarChar的password字段，但是如果采用加密方式来存储密码信息，就必须改变密码字段password的类型，MD5是单向加密算法，加密以后就无法解密，如果用户忘记或丢失密码，任何人都很难找回。这样，网站就失去了一项很重要的功能：获取忘记的密码。所以，如果采用这种加密方式的话，想要修改资料就必须将用户重新注册。

四、 MD5加密算法的安全性

可以看出，MD5是非常复杂的。Rivest为了让MD5不会对两个不同的消息产生出相同的消息摘要，于是想让MD5算法变得更加复杂，更加随机。MD5的一个属性是，消息摘要中的每一位是

输入中的每一位的某个函数。使用 MD5 时，两个消息产生相同的消息摘要概率为226次操作的数量级。如果给出一个消息摘要，要求出它的原消息，则需要多达 2128 次的操作。

MD5 曾经遭到如下攻击：

1.Tom Berson虽然找到了对四轮分别生成相同消息摘要的消息，但是找不到四轮同时生成相同消息摘要的消息。

2.Den Boer 与 Bosselaers 证明在一个512位块上执行 MD5 的时候，会对链接变量寄存器 a b c d 中的两个不同的值产生相同的输出，称为冲突，但这个冲突不会推广到四轮各 16 步的完整 MD5 中。

3.Dobbertin 提出了对 MD5 最严重的攻击，两个不同的512位块进行 MD5 操作时，可以得到相同的128位输出，但没有推广到完整消息块。

4. 在 2004 年，以山东大学王小云为首的团队破解了 MD5 和 SHA-1 两大文摘算法，震惊了全世界。

综上所述，在企业和普通用户使用的时候，从算法上破解依旧十分困难，因此 MD5 加密算法依然是一个相对安全的加密算法。

综上所述，在企业和普通用户使用的时候，在算法上破解依旧十分困难，因此 MD5 加密算法依然是一个相对安全的加密算法

五、结论

MD5 算法是由 MD2 、 MD3 和 MD4 一步步改进而来。因为它的算法相对复杂，所以 MD5 在计算速度上做出了相应的牺牲，但就目前普通的应用范围来讲， MD5 算法还是能够完全胜任的，而且还没有出现过其它或者新的例如叫做 MD6 之类的算法来代替。所以 MD5 在未来加密算法领域里还有相当大的应用价值，一段时间内不会被超越。实践证明，在网站的建设和应用系统的开发过程中通过引进 MD5 算法，会非常有效的提高用户重要信息的安全性，所以 MD5 加密算法是一种十分优秀的信息加密算法。

本文不但讲解了 MD5 算法的原理，而且还研究了 MD5 算法在信息管理系统中是如何运用的。通过理论分析和实践了解了 MD5 算法是如何对信息管理系统进行加密的。通过对 MD5 算法安全性的分析，得出 MD5 算法在当前的计算机领域里还是非常安全可靠的。当今社会，随着企业信息和网络数据的膨胀，确保数据安全的重要性与日俱增，所以数据加密技术的应用，发展和前景是非常重要的。

参考文献 **：**

中文著作类：

[1] 魏晓玲.MD5加密算法的研究及应用[D].延安大学计算中心，2010.

[2] 孙忠林，赵卫东等．高级用户权限加密管理技术 [J]. 计算机研究， 2003 .

[3] 杨 波．现代密码学 [M]. 北京：清华大学出版杜， 2003 .

[4] 杨义先，林晓东．信息安全综论 [M]. 北京：电信科学出版社，1998.

[5] 杨 明，齐望东 ．密码编码学与网络安全 [M]. 北京：电子工业出版社， 1997.

[6] 潘清芳．使用 MD5 加密数据库系统的设计 [J]. 第3 卷第 2 期 :77-143.

[7] 喻 谦 ．基于 MD5 算法的用户身份认证系统研究[D].华北电力大学， 2013.

[8] 陆琳琳.MD5算法的技术研究及性能优化 [D].吉林大学， 2005.

[9] 王新忠．电信系统中用户接入网管理信息的安全技术[D].华中科技大学， 2006.

[10] 郭珊琼.MD5数据加密算法的研究与实现 [D].武汉理工大学， 2007.

外文著作类：

[1] R.Rivest.The MD5 Message-Digest Algorithm.RFC1321 ， Oct 1992.

[2] Haller N ． The S／KEY One2Time Password System[z].RFC 1760 ， February 1995.