**安徽职业技术学院**

**毕   业   论   文**

   题 目 数据加密技术的应用研究

学生姓名    王 朝 虎

学     号    2014237260

专    业   软件技术

班     级  软 件 1422

指导教师       李 军 老 师

二0一七年二月

目 录

第一章 引言 4

第二章 数据加密技术的发展过程 4

2.1 1949年以前 5

2.2 1949～1975 年期间 5

2.3 1976年至今 6

第三章 常用的加密方式 8

第四章 数据加密技术的研究 9

4.1 加密的常用方法 9

4.2 加密的实现原理 10

4.2.1 数据加密、解密基本过程 10

4.2.2 对称式密钥加密技术 10

4.2.3 公开密钥加密技术 11

4.2.4 对称密钥和公开密钥相结合的加密技术 13

4.3 主要应用 13

4.3.1 加密技术在电子商务方面的应用 14

4.3.2 加密技术在VPN中的应用 14

4.4 加密性能优劣 15

4.4.1 对称加密算法 15

4.4.2 非对称加密算法 15

4.4.3 对称加密算法和非对称加密算法的比较 15

第五章 未来发展趋势 16

数据加密技术的应用研究

摘 要：信息安全是当今社会非常重要的问题之一。数据安全是信息安全的重要组成部分，如何确保数据安全可靠，是信息领域中非常重要的课题。对重要的数据进行加密处理，是保证数据安全的重要手段之一。研究数据加密技术与方法不仅有非常重要的学术意义，同时也具有非常重要的现实意义。

病毒、黑客的猖獗使身处今日网络社会的人们感觉无所适从。现代的电脑加密技术就是适应了网络安全的需要而应运产生的，它为我们进行一般的电子商务活动提供了安全保障，如在网络中进行文件传输、电子邮件往来和进行合同文本的签署等。其实加密技术也不是什么新生事物，只不过应用在当今电子商务、电脑网络中还是近几年的历史。

在TCP／口协议中，传输的数据都是以明文进行传输的，所以存在固有安全缺陷，解决这一问题的重要手段就是数据加密．在现代网络通信中，人们的安全意识越来越强烈，密码学的应用也越来越广泛。本文主要介绍数据加密技术的相关技术及其应用。

**关键词：**数据加密技术、对称式加密、非对称式加密、密钥

# 引言

随着计算机技术的革新，对网络的通信安全要求水平水涨船高，与此同时，各种各样的网络信息窃取和破坏也使得社 会各领域在对计算机安全方面的需求日益强烈。

总的来说，计算机的信息安全包涵了两个层面的要求：一方面是对计算机信息的存储安全要求；另外一方面就是对计算机网络的通信安全要求。在对计算机安全存在的威胁中人为因素要比非人为因素的影响大得多，人为的安全威胁又分为被动攻击和主动攻击。其中被动攻击主要影响计算机的数据保密性，常用的手段有六个：一是对通信线路上传递信息的窃取和监听；二是对窃取和监听的数据分析；三是冒充用户身份；四是对网络中传播的信息进行篡改；五是拒绝确认所发信息；六是其他手段。

进入九十年代之后，计算机网络的发展和Internet的广泛、深入的应用，特别是利用它来开展电子商务活动，又推动了数据加密技术的发展，出现了许多可用于金融系统和电子交易中的技术和规程，安全电子交易协议（SET）和安全套接层规程（SSL）已被广泛用于Internet/Intranet服务器和客户机的产品中，成为事实上的标准。可见，近年来崛起的数据加密技术，又成为一门年轻的科学。

# 数据加密技术的发展过程

从出现加密概念至今，数据加密技术发生了翻天覆地的变化，从整体来看数据加密技术的发展可以分为三个阶段。

## 1949年以前

早期的数据加密技术还很简单，复杂程度不高、安全性较低，大部分是一些具有艺术特征的字谜，因此这个时期的密码被称为古典密码。随着工业革命的到来和二次世界大战的爆发，密码学由艺术方式走向了逻辑-机械时代。数据加密技术有了突破性的发展，先后出现了一些密码算法和机械的加密设备。不过这时的密码算法针对的只是字符，使用的基本手段是替代和置换。替代就是用密文字母来代替明文字母，在隐藏明文的同时还可以保持明文字母的位置不变；而置换则是通过重新排列明文中字母的顺序来达到隐藏真实信息的目的。

## 2.2 1949～1975 年期间

从1946年2月世界上第一台计算机在美国诞生到1975 年，计算机技术发展迅速，特别是计算机的运算能力有了大幅提升，这使得基于复杂计算的数据加密技术成为可能。

简而言之，计算机将数据加密技术从机械时代提升到了电子时代。虽然这个时期使用的加密算法还是基于替代和置换思想的加密算法，但由于巧妙运用了计算机的高运算能力，这些加密算法在复杂程度和安全性上得到了提高，例如″置换表″算法和字/字节循环移位和异或操作。″置换表″算法是所有加密算法中最简单的一种。这种算法是将每一个数据段（总是一个字节）对应着″置换表″中的一个偏移量，偏移量所对应的值就输出成为加密后的文件。加密程序和解密程序都需要一个这样的″置换表″。这种加密算法比较简单、加密解密速度都很快，但实用性差。黑客只要找到″置换表″就可以完全识破整个加密方案。在实际应用中，往往使用多张″置换表″进行加密，并按照伪随机的方式来使用每张表。经过这样改进后，即使黑客获得了明文和密文，要破译这个加密方案也是非常困难的。

与″置换表″算法相比，字/字节循环移位和异或操作是一种更好的加密算法而且只有计算机可以做。如果把一个字或字节在一个数据流内做循环移位，使用多次的左移或右移，就可以迅速的产生一个加密的数据流。这种方法是很好的，破译它也很困难。如果在加密数据流的基础上再使用异或操作（按位做异或操作），就会使破译密码变得更加困难。如果再使用伪随机的方法，即首先使用 fibbonaci 数列并对数列所产生的数做模运算，得到一个结果，然后循环移位这个结果的次数，将使破译密码变的几乎不可能！但是，使用 fibbonaci数列这种伪随机的方式所产生的密码对解密程序来讲是非常容易的。

## 2.3 1976年至今

公开密钥密码体制的概念于1976年由美国密码学专家狄匪（Diffie）和赫尔曼（Hellman）提出，是现代密码学的重大发明，将密码学引入了一个全新的方向。用抽象的观点来看,公钥密码体制就是一种陷门单向函数。如果说一个函数 f是单向函数, 那么对其定义域中的任意 x 都易于计算 f（x）,而对 f 的值域中几乎所有的 y, 即使当 f 为已知时要计算 f- l（y）也是不可行的。但如果给定某些辅助信息（陷门信息），则易于计算 f- l（y）, 因此称单向函数 f 是一个陷门单向函数。公钥密码体制就是基于这一原理而设计的,将辅助信息作为秘密密钥。这类密码的安全强度取决于它所依据的问题的计算复杂度。

基于公钥概念的加密算法就是非对称密钥算法，这种加密算法有两个重要的原则：第一，要求在加密算法和公钥都公开的前提下，其加密的密文必须是安全的；第二，要求所有加密的人和掌握私人秘密密钥的解密人，计算或处理都应比较简单，但对其他不掌握秘密密钥的人，破译应是极困难的。随着计算机网络的发展，信息保密性要求的日益提高，非对称密钥加密算法体现出了对称密钥加密算法不可替代的优越性。

近年来，非对称密钥加密算法和 PKI、数字签名、电子商务等技术相结合，保证了网上数据传输的机密性、完整性、有效性和不可否认性，在网络安全及信息安全方面发挥了巨大的作用。

目前比较流行的非对称密钥加密算法主要有两类：一类是基于大整数因子分解问题的，其中最典型的代表是RSA算法；另一类是基于离散对数问题的，如ElGamal算法和影响比较大的椭圆曲线公钥密码体制。虽然公钥密码体制是非常重要的一种技术，实现了数字签名的概念，提供了对称密钥协定的切实可行的机制，使安全通信成为可能。但非对称密钥加密算法并不是完美的，这类算法普遍存在算法复杂、运行速度慢的缺点。除了公开密钥密码体制概念外，混沌理论对近年来的数据加密技术也产生了深远的影响。由于混沌系统具有良好的伪随机性、轨道不可预测性、对初始状态及控制参数的敏感性等特性，而这些特性恰恰与密码学的很多要求是吻合的，

因此当1990年前后混沌理论开始流行时混沌密码学也随之兴起。经过十多年的发展，基于混沌理论的混沌密码学已经成长为现代数据加密技术中的一个重要分支。混沌密码学的研究方向大致可以分为两个方向：一类是以混沌同步技术为核心的混沌保密通信系统；另一类是利用混沌系统构造新的流密码和分组密码。

# 常用的加密方式

我们所研究的数据加密技术，并不是单单一种。一般说来，从数据加密的方法上分，数据加密技术可以分为两种：动态数据加密技术和静态数据加密技术。动态数据加密技术是指当数据经过网络时，数据在数据库服务器和客户端之间的相互传送，这种传输过程中数据的加密技术就是动态数据加密技术。这种方法可以有效的阻止会话攻击。现实生活中，这种动态数据加密技术已经被广泛的应用了。静态数据加密技术是指对存在于数据库中的数据进行加密处理。这种静态加密技术还没有广泛的应用。

# 数据加密技术的研究

## 加密的常用方法

加密技术通常分为两大类：“对称式加密”和“非对称式加密”。 对称式加密就是加密和解密使用同一个密钥，通常称之为“SessionKey”，这种加密技术目前被广泛采用，如美国政府所采用的DES加密标准就是一种典型的“对称式”加密法，它的SessionKey长度为56Bim。DES使用56位密钥对位的数据块进行加密，并对位的数据块进行16轮编码。与每轮编码时，一个48位的“每轮”密钥值由56位的完整密钥得出来。DES用软件进行解码需用很长时间，而用硬件解码速度非常快。当时DES被认为是一种十分强大的加密方法。 非对称式加密就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“公钥”和“私钥”。这里的“公钥”是指可以对外公布的，“私钥”则不能，只能由持有人一个人知道。它的优越性就在这里，因为对称式的加密方法如果是在网络上传输加密文件就很难把密钥告诉对方，不管用什么方法都有可能被别窃听到。而非对称武的加密方法有两个密钥，且其中的“公钥”是可以公开的，也就不怕别人知道，收件入解密时只要用自己的私钥即可以，这样就很好地避免了密钥的传输安全性问题。

非常著名的非对称式加密算法就是RSA了，RSA算法是基于大数不可能被质因数分解假设的公钥体系。一个对外公开的为“公钥”(Publickey)，另一个不告诉任何人，称为“私钥”(Privatekey)。这两个密钥是互补的，也就是说用公钥加密的密文可以用私钥解密，反过来也一样。假设用户甲要寄信给用户乙，他们互相知道对方的公钥。甲就用乙的公钥加密邮件寄出，乙收到后就可以用自己的私钥解密出甲的原文。由于别人不知道乙的私钥，所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。另一方面，由于每个人都知道乙的公钥，他们都可以给乙发信，那么乙怎么确信是不是甲的来信呢?那就要用到基于加密技术的数字签名了。甲用自己的私钥将签名内容加密，附加在邮件后，再用乙的公钥将整个邮件加密。这样这份密文被乙收到以后，乙用自己的私钥将邮件解密，得到甲的原文和数字签名，然后用甲的公钥解密签名，这样一来就可以确保两方面的安全了。

## 加密的实现原理

### 数据加密、解密基本过程

通常情况下，人们将可懂的文本称为明文 ( plaintext)，将明文变换成的不可懂的形式的文本称为密文 ( ciphertex t)，把明文变换成密文的过程叫加密 ( encipher)。其逆过程即把密文变换成明文的过程叫解密 ( decipher)。密钥 ( keyword)是用于加解密的一些特殊信息，它是控制明文与密文之间变换的关键 ，它可以是数字、词汇或语句。密钥分为加密密钥 ( EncryptionKey)和解密密钥(DecryptionKey)。完成加密和解密的算法称为密码体制(CipherSystem)。传统的密码体制所用的加密密钥和解密密钥相同，形成了对称式密钥加密技术。在一些新体制中，加密密钥和解密密钥不同，形成非对称式密码加密技术，即公开密钥加密技术。数据加密或解密变换过程如图1所示。

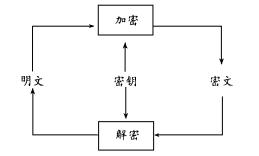


图1 加密或解密变换

### 对称式密钥加密技术

1. 基本概念

对称式密钥加密技术是指加密和解密均采用同一把秘密钥匙，而且通信双方必须都要获得这把钥匙，并保持钥匙的秘密。当给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。故它也称为秘密钥匙加密法。

1. 加密算法

实现对称式密钥加密技术的加密算法主要有以下两种：

1. DES( Data Encryption Standard)算法

DES即数据加密标准，是1977年美国国家标准局宣布用于非国家保密机关的数据保护。这种加密算法是由IBM研究提出来，它综合运用了置换、代替、代数多种密码技术，把信息分成 64位大小的块，使用56位密钥，迭代轮数为 16轮的加密算法。

1. IDEA( International Data Encryption Algorithm )算法

IDEA是一种国际信息加密算法。它是 1991年在瑞士E TH Zurich由 James Massey和 XueiiaLai发明，于1992年正式公开，是一个分组大小为 64位，密钥为128位，迭代轮数为八轮的迭代型密码体制。此算法使用长达 128位的密钥，在效地消除了任何试图穷尽搜索密钥的可能性。

1. 对称式密钥加密技术的优缺点

对称式密钥加密技术具有加密速度快，保密度高等优点。但也有其缺点：

1. 密钥是保密通信安全的关键，发信方必须安全、妥善地把钥匙护送到收信方，不能泄露其内容，如何才能把密钥安全地送到收信方，是对称密钥加密技术的突出问题，可见，此方法的密钥分发过程十分复杂，所花代价高。
2. 多人通信时密钥的组合的数量，会出现爆炸性的膨胀，使密钥分发更加复杂化，n个人进行两两通信，总需要的密钥数为 n( n- 1) /2。
3. 通信双方必须统一密钥，才能发送保密的信息。如果发信者与收信人是素不相识的，这就无法向对方发送秘密信息了。

### 公开密钥加密技术

1. 基本概念

公开密钥加密技术要求密钥成对使用，即加密和解密分别由两个密钥来实现。每个用户都有一对选定的密钥，一个可以公开，即公共密钥，用于加密。另一个由用户安全拥有，即秘密密钥，用于解密。公共密钥和秘密密钥之间有密切的关系。当给对方发信息时，用对方的公开密钥进行加密，而在接收方收到数据后，用自己的秘密密钥进行解密。故此技术也称为非对称密码加密技术。

1. 加密算法

公开密钥加密算法主要是RSA加密算法。此算法是美国MIT的 Rivest、 Shamir和 Adleman于1978年提出的，它是第一个成熟的、迄今为止理论上最为成功的公开密钥密码体制，它的安全性基于数论中的Euler定理和计算复杂性理论中的下述论断：求两个大素数的乘积是容易的，但要分解两个大素数的 乘积，求出它们的素因子则是非常困难的，它属于NP—— 完全类。RSA加密、解密过程由密钥生成、加密过程和解密过程组成。

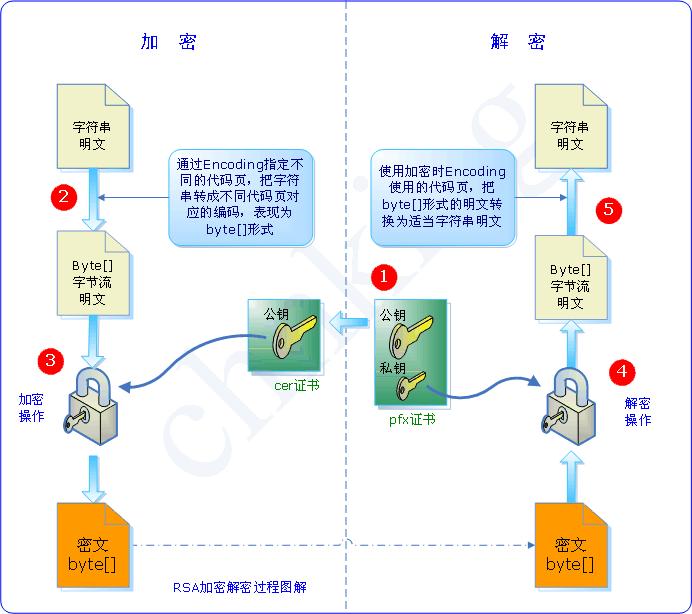


图 rsa加密算法图解

1. 公开密钥加密技术的优缺点

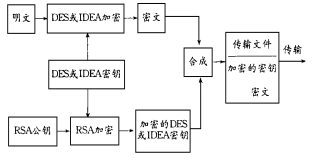
公开密钥加密技术的优点是：

1. 密钥少便于管理，网络中的每一用户只需保存自己的解密密钥，则 N个用户仅需产生N对密钥。
2. 密钥分配简单，加密密钥分发给用户，而解密密钥则由用户自己保管。
3. 不需要秘密的通道和复杂的协议来传送密钥。
4. 可以实现数字签名和数字鉴别。

公开密钥加密技术的缺点是加、解密速度慢。

### 对称密钥和公开密钥相结合的加密技术

鉴于对称密钥和公开密钥加密技术的特点，在实际应用中将两种加密技术相结合，即结合使用DES / IDEARSA，对于网络中传输的数据用DES或IDEA加密，而加密用的密钥则用RSA加密传送，此方法既保证了数据安全又提高了加密和解密的速度。DES /IDEA和RSA结合使用如图2所示。



首先发信者使用DES /IDEA算法用对称钥将明文原信息加密获得密文，然后使用接收者的RSA公开钥将对称钥加密获得加密的DES或IDEA密钥，将密文和加密的密钥一起通过网络传送给接收者。接收方接收到密文信息后，首先用自己的密钥解密而获得DES或IDEA密钥，再用这个密钥将密文解密而最后获得明文原信息。由此，起到了对明文信息保密的作用。

著名的PGP( Pretty Good Privacy )软件就是使用RSA和IDEA相结合进行数据加密。另外，保密增强邮件( PRM )将RSA和DES结合起来，成为一种保密的 E- mail通信标准。常用到的 SSL( Secure Sockets Layer，安全套层 )安全措施也是利用两种加密技术对客户机和服务器之间所传输的信息进行加密的。

## 主要应用

加密技术的应用是多方面的，但最为广泛的还是在电子商务和VPN上的应用，下面就分别讲述一下。

### 加密技术在电子商务方面的应用

电子商务(E—business)要求顾客可以在网上进行各种商务活动，不必担心自己的信用卡会被人盗用。人们开始用RSA的加密技术，提高信用卡交易的安全性，从而使电子商务走向实用成为可能。 NETSCAPE公司是Intemet商业中领先技术的提供者，该公司提供了一种基于RSA和保密密钥的应用于因特网的技术，被称为安全插座层(SecureSocketsLayer，SSL)。SsL3．O用一种电子证书(electriccertificate)来实行身份进行验证后，双方就可以用保密密钥进行安全的会话了。它同时使用“对称”和“非对称”加密方法，在客户与电子商务的服务器进行沟通的过程中，客户会产生一个SessionKey，然后客户用服务器端的公钥将SessionKey进行加密，再传给服务器端，在双方都知道SessionKey后，传输的数据都是以SessionKey进行加密与解密的，但服务器端发给用户的公钥必需先向有关发证机关申请，以得到公证。

基于SSL3．0提供的安全保障，用户就可以自由订购商品并且给出信用卡号了，也可以在网上和合作伙伴交流商业信息并且让供应商把订单和收货单从网上发过来，即安全又方便。

### 加密技术在VPN中的应用

现在，越多越多的公司走向国际化，一个公司可能在多个国家都有办事机构或销售中心，每一个机构都有自己的局域网LAN(LOCalArea Network)，但在当今的网络社会人们的要求不仅如此，用户希望将这些LAN连结在一起组成一个公司的广域网，这个在现在巳不是什么难事了。 现在已经有了加密／解密功能的路由器，这就使人们通过互联网连接这些局域网成为可能，这就是我们通常所说的虚拟专用网(VirtIlalPrivateNetwork，VPN)。当数据离开发送者所在的局域网时，该数据首先被用户端连接到互联网上的路由器进行硬件加密，数据在互联网上是以加密的形式传送的。当达到目的LAN的路由器时，该路由器就会对数据进行解密，这样目的LAN中的用户就可以看到真正的信息了。

## 加密性能优劣

### 对称加密算法

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。此外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的惟一钥匙，这会使得发收信双方所拥有的钥匙数量成几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难，主要是因为密钥管理困难，使用成本较高。而与公开密钥加密算法比起来，对称加密算法能够提供加密和认证却缺乏了签名功能，使得使用范围有所缩小。在计算机专网系统中广泛使用的对称加密算法有DES和IDEA等。美国国家标准局倡导的AES即将作为新标准取代DES。

### 非对称加密算法

非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要。 特点是算法强度复杂、安全性依赖于算法与密钥但是由于其算法复杂，而使得加密解密速度没有对称加密解密的速度快。对称密码体制中只有一种密钥，并且是非公开的，如果要解密就得让对方知道密钥。所以保证其安全性就是保证密钥的安全，而非对称密钥体制有两种密钥，其中一个是公开的，这样就可以不需要像对称密码那样传输对方的密钥了。这样安全性就大了很多。

### 对称加密算法和非对称加密算法的比较

RSA并不能替代DES，它们的优缺点正好互补。 RSA的密钥很长，加密速度慢，而采用DES，正好弥补了RSA的缺点。即DES用于明文加密，RSA用于DES密钥的加密。由于DES加密速度快，适合加密较长的报文；而RSA可解决DES密钥分配的问题。美国的保密增强邮件（PEM）就是采用了RSA 和DES结合的方法，目前已成为E-MAIL保密通信标准。

# 未来发展趋势

正是由于不同的加密算法各有所长，所以在今后相当长的一段时期内，各类加密体制将会共同发展。近年来，混沌学理论的研究给在这一方向产生突破带来了曙光。此外，充满生气的量子密码被认为是一个潜在的发展方向，因为它是基于光学和量子力学理论的。该理论对于在光纤通信中加强信息安全、对付拥有量子计算能力的破译无疑是一种理想的解决方法。由于电子商务等民用系统的应用需求，认证加密算法也将有较大发展。此外，在传统密码体制中，还将会产生类似于IDEA这样的新成员，新成员的一个主要特征就是在算法上有创新和突破，而不仅仅是对传统算法进行修正或改进。密码学是一个正在不断发展的年轻学科，任何未被认识的加/解密机制都有可能在其中占有一席之地。 数据加密技术今后的研究重点将集中在三个方向：第一，继续完善非对称密钥加密算法；第二，综合使用对称密钥加密算法和非对称密钥加密算法，利用它们自身的优点来弥补对方的缺点；第三，随着笔记本电脑、移动硬盘、数码相机等数码产品的流行，如何利用加密技术保护数码产品中信息的安全性与私密性、降低因丢失这些数码产品带来的经济损失也将成为数据加密技术的研究热点。

**参考文献：**

1. 黄志清**.**网络安全中的数据加密技术研究**.**研究与设计**.**6卷第5期
2. 刘宇平**.**数据加密技术在计算机安全中的应用分析**.**信息通信**.**2012年第2期
3. 柯海清,冯启明**.**数据加密技术及网络应用**.**武汉理工大学学报交通科学与工程版
4. 卢开澄**.**计算机密码学**.**第二版.清华大学出版社.1998
5. 马明明**.**数据加密技术的发展历史**.**河西学院
6. 张玉秀**.**浅谈数据加密技术的发展**.**电脑学习**.**2008年4月第2期