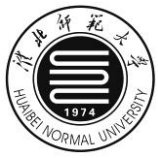
分类号：　　学校代码：10373

密　级：　　学　　号：10812081201



淮北師範大學

硕士学位论文

题目： 数字签名技术在电子商务中的应用

论 文 作 者 陈 月 荣

指 导 教 师 魏 仕 民

专 业 名 称 计算机软件与理论

研 究 方 向 网络与信息安全

申请学位类别 工　学

淮北师范大学研究生处

2011 年 6 月 10 日

学位论文独创性声明

本学位论文是作者在导师的指导下进行的研究工作及取得的研究成果。据我们所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。学位论文作者和导师均承担本声明的法律责任。

学位论文作者签名：_____日期：_____

导　师　签　名：_____日期：_____

学位论文版权使用授权书

本学位论文作者完全了解 淮北师范大学 有关保留、使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属 淮北师范大学 。学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权 淮北师范大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编本学位论文。保密的学位论文在解密后适用本授权书。

学位论文作者签名：_____　日期：_____

导　师　签　名：_____日期：_____

数字签名技术在电子商务中的应用

摘要：Internet 的快速发展使电子商务成为商务活动的新模式，电子商务从产生至今虽然时间不长，但发展十分迅速。电子商务的发展前景及其带来的影响，已经引起世界各国政府和企业的广泛关注和积极参与。由于电子商务交易平台的虚拟性和匿名性，其安全问题也变得越来越突出，电子签名技术的应用及其立法为电子商务安全运行提供了重要保障。

数字签名是目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。所谓"数字签名"就是通过某种密码运算生成一系列符号及代码组成电子密码进行签名，来代替手书签名或印章。它采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证出文件的原文在传输过程中有无变动，确保传输电子文件的完整性、真实性和不可抵赖性。在电子商务的发展热潮中，电子商务的安全性已成为制约电子商务发展的重要瓶颈。随着电子商务的发展，网络上资金的电子交换日益频繁，如何防止信息的伪造和欺骗成为非常重要的问题。在计算机通信系统中，维护电子文档的安全也成为至关重要和非常敏感的问题。为保护信息的安全，数字签名应运而生，它是现代密码学主要研究的内容之一。目前关于数字签名的研究主要集中点是基于公钥密码体制的数字签名。改进数字签名在内的安全技术措施，确定 CA 认证权的归属问题是解决电子商务安全问题的关键。而数字签名(Digital Signatures)技术是保证信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性的一种有效的解决方案，是电子商务安全性的重要部分。

本文首先分析了数字签名的研究现状与发展趋势。其次是探讨了数字签名的相关技术，包括数字签名的数学基础与数字签名的相关概念。第三，分析了基于大整数因式分解的 RSA 签名方案和基于离散对数的 ElGamal 签名方案。其签名方案是在公共密钥体制基础上建立的，实现公钥密码体制思想的主要是数字签名方案和 DSA 数字签名方案。最后，在基于这两个数学难题的基础上提出新的数学方法，即基于不同的数学难题提出一种安全性同时基于离散对数问题和素因子分解问题的数字签名方案。

关键词：数字签名，RSA 签名，ElGamal 签名，DSA 签名

The Application of E-commerce in Digital Signature

Abstract: The rapid development of Internet makes Electronic Commerce into a new business model.E-commerce from generation to up now.

Although it is not a long time, its development is growing very rapidly. Prospects for the development of e-commerce and its impact has attracted world wide attention from government and business and active participation because of E-commerce trading platform and the virtual anonymity. The security issues become more prominent which electronic signature technology and the safe operation of E-commerce legislation provides important protection.

Digital signature which is the most common, most mature technology and operational is the E-commerce and E-government. That is to say. It is the most strongest electronic signature method. The so-called "digital signature" is generated by a cryptographic code composed of a series of symbols and signatures electronic password to replace the written signature or seal. It uses standardized procedures and scientific methods used to identify the signer's identity and the contents of an electronic data recognition. It also proved that the original document whether changes in the transmission process in order to ensure the integrity of electronic document transmission, authenticity and non-repudiation. Development boom in E-commerce, E-commerce security has become a major bottleneck restricting the development of E-commerce. With the development of electronic commerce and network. Electronic exchange of funds have become increasingly frequent. Information on how to prevent forgery and deception become a very important issue. In computer communication systems, maintenance of the security of electronic documents has become a critical and very sensitive issue. For the protection of information security, digital signatures came into being which is one of the main he study of modern cryptography, Current research on the digital signature focal point is based on the digital signature public key cryptosystem. Improve the security of digital signatures, including technical measures, to determine the ownership of the right CA certificate is the key to solving

E-commerce security issues. The digital signature (Digital Signatures) technology is to ensure the confidentiality of information transmission, data exchange integrity, non-repudiation of sending messages, trading the certainty of the identity of an effective solution for the importance of e-commerce security section.

This dissertation analyzes the digital signature of the situation and development trend. Followed by a digital signature of related technologies, including digital signatures and digital signatures based on mathematical concepts. Thirdly, the analysis of large integer factorization of RSA-based signature scheme and the ElGamal discrete logarithm based signature scheme. Its signature program is based on public key system, the realization of the main public key cryptosystem thought DSA signature scheme and digital signature scheme. Finally, in the two math problems on the basis of the number of proposed new method is proposed based on different mathematical problem while a security problem and based on discrete logarithm problem of prime factorization digital signature scheme.

Key words: digital signature，RSA signature，ElGamal signature，DSA signature

目 录

第一章 绪论

1.1 课题的研究与背景和意义

随着 Internet 的不断革新和发展，这样会给整个的全球经济带来了新的革命，也会改变着整个的商业社会的竞争格局。Internet 的迅猛发展使电子商务成为商务活动的新模式，电子商务的优势在于可以增加贸易的机会、降低贸易的成本、简化贸易的流程和提高贸易的效率。利用 Internet 开展电子商务，依然是企业走向成功或飞跃发展的必要途径。而利用电子商务进行商业交易，首先需要拥有电子商务网站。其中企业建立电子商务网站需要考虑到以下的因素：例如企业想要入住商场时，就必须要考虑方位、客户流量和商业信誉等因素，一些中小企业者建设电子商务网站时也需要考虑如下因素：如访问量，商家数量以及质量和商业信誉等因素。除此之外，它们还要考虑到电子商务网站开展电子商务的实力，例如渠道其中包括物流、支付方式和配送方式等等；另外还有硬件的设施及维护服务和商务推广支持的以及是否具备开展电子商务的丰富经验，这些因素都可供入住企业借鉴等等。优秀的电子商务网站所必须具备的这些因素。电子商务包括电子数据交换 EDI、电子订货系统 EOS、管理信息系统 MIS 和商业增值网 VAN 等，其中电子数据交换 EDI 成为电子商务的核心部分。

网络的开放性与共享性也导致了网络的安全性受到严重影响，在开放的 Internet 平台上，社会生活中传统的犯和不道德行为将变得更加隐蔽和难以控制。人们从面对面的交易和作业，变成网上互不见面的操作、没有国界和没有时间罪限制，就产生了更大的安全隐患。因此，在电子商务的发展热潮中，电子商务的安全性已成为制约电子商务发展的重要瓶颈。改进数字签名在内的安全技术措施和确定 CA（Certificate Authority）认证权的归属问题是解决电子商务安全问题的关键。数字签名技术的应用范围也是十分广泛的，在保障 EDI（Electronic Data Interchange）电子数据交换的安全性方面起着一个突破性的进展。

在电子商务安全方面，数字签名技术也有着特别重要的地位，数字签名(Digital Signatures)技术是保证信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性的一种有效的解决方案，是电子商务安全性的重要部分。

实现数字签名有很多种方法，但是目前数字签名采用较多的技术还是公钥加密技术，例如 RSA 算法、基于离散对数算法和 Hash 函数算法等等。数字签名在理论研究和应用方面都有很大的空间，所以仍然有很多问值得研究和需要解决。因此本文设计一个同时基于两个难解决问题的数字签名方案在电子商务中的应用。其中离散对数问题和素因子分解问题是密码学中两个著名的难解决问题，基于这两个签名方案，提出一种安全性同时基于离散对数问题和素因子分解问题的数字签名方案的研究有着重要的理论和现实意义。

1.2 课题的发展和研究现状

信息安全是一门综合的、交叉的学科领域，它主要包括数学、通信、微电子学和计算机科学等多学科的一个综合研究体系。密码学是一门与信息安全有密切相关的数学科学，是信息安全的核心技术。与其他学科进行相比，信息安全的研究更强调创新性和自主性，创新性可以抵抗各种攻击，适应技术发展的需求；而自主性可以避免“陷门”，这样体现了国家主权。

自从 1976 年 W.Diffie 和 M.Hellman 提出公开密钥密码以来，在密码学领域中爆发了一场深刻的革命，密码学的理论与技术不再是仅为少数人掌握服务于政府、外交及军事的神秘科学。尤其是商业和银行业越来越国际化，密码学的理论与技术在经济领域获得了广泛的应用。国际上已经提出了许多种公钥密码体制，但是广泛应用的主要有两类：一类是基于大整数因子分解问题的公钥密码体制，其中 RSA 公钥密码体制是最典型的代表；另一类是基于离散对数问题的公钥密码体制，其中 ElGamal 公钥密码体制和 ECC 椭圆曲线公钥密码是最典型的代表。

公钥密码主要是用于数字签名和密钥分配。数字签名在信息安全中有着重要的应用，包括身份认证、数据的完整性、匿名性及不可否认性等等。但是特别在大型网络安全通信中的密钥分配、认证及电子商务系统中具有重要的作用。目前数字签名的内容研究是非常之多的，其中包括的有普通签名和特殊签名。普通签名又包括 RSA、、Rabin、ElGamal、Schnorr 等等签名，其特殊签名又包括不可否认签名、防失败签名、盲签名、群签名和门限签名等等，它们是与具体应用环境密切相关联的。这样，数字签名的应用将会会涉及到了法律问题，美国联邦政府制定了自己的 DSS 数字签名标准，该签名是基于有限域上的离散对数问题上，

部分州也已制定了数字签名法。像法国和德国等的一些国家也已经制定了数字签名法，其中法国是第一个制定数字签名法的国家。2004 年 8 月，第十届全国人大常委会通过了我国《电子签名法》。这部法律规定，可靠的电子签名与手写签名或者盖章具有一样的法律效力。该法在 2005 年 4 月起施行，它将对我国的电子商务和电子政务的发展起到极其重要的作用。虽然目前有许多数字签名的方案被提出，但是基于大整数因式分解和离散对数数学问题的数字签名的安全性工作做的还不多，许多方面的安全性还没有正式证明公布。

1.3 本文的课题内容

本文的主要内容是数字签名技术在电子商务中的应用的研究。

第一章：介绍课题的研究背景与意义，以及课题的研究现状。

第二章：网络安全基础理论，主要介绍密码学及其概念，与密码学相关的数论知识。

第三章：数字签名技术在电子商务中的应用，主要介绍了数字签名的相关概念，以及分析了 RSA 加密和数字签名算法。

第四章：基于离散对数问题的数字签名，主要分析了 ElGamal 数字签名方案和 DSA 数字签名方案。

第五章：改进的数字签名，在第二章和第三章的基础上提出了新的方案。

第六章：结束语，对本文进行了总结，并对课题发展方向进行了展望。

第二章 网络安全基础理论

2.1 密码学及其基本概念

密码学(Cryptology)是一门古老的科学。在密码学形成和发展的历程中，科学技术的发展和战争的刺激都起了积极的推动作用。电子计算机一出现便被用于密码破译，使密码进入电子时代。1949 年商农（C.D.Shannon）发表了《保密系统的通信理论》的著名论文，把密码学置于坚实的数学基础之上，标志着密码学作为一门科学的形成。1976 年 W.Diffie 和 M.Hellman 提出公开密钥密码，从此开创了一个密码的新时代。1977 年美国联邦政府颁布数据加密标准（DES），这是密码史上的一个创举。1994 年美国联邦政府颁布密钥托管加密标准（EES）,1994 年美国联邦政府颁布数字签名标准（DSS），2001 年美国联邦政府颁布高级加密标准（AES）。这些都是密码发展史上的一个个重要的里程碑。

密码学是研究信息及信息系统安全传统的科学，它起源于保密同性计算。也是作为数学的一个分支，其包括密码编码学（Cryptogtaphy）和密码分析学（Cryptanalytics）两部分。密码编码学(Cryptography)主要是研究对信息进行编码，实现对信息的隐蔽；而密码分析学(Cryptanalytics)主要是研究加密消息的破译或消息的伪造。两者相互对立，而又相互促进的向前发展。

尚未隐藏或未加密的信息称为明文(Plaintext)或消息（Message），用 P 或 M 表示。明文是发送者准备发送的原文信息，明文的集合称为明文信息空间，用 SP 表示。而用某种方法去伪装消息并且要隐藏它的内容的过程则称为加密(Encrtption)，其中被加密的消息则称为密文(Ciphertext)，用 C 表示。所以的密文构成密文信息空间，用 SC 表示。而把密文转换为明文的过程则称为解密(Decryption)。对明文进行加密操作的人员称为密码员（Cryptogtapher）。密码算法(Cryptography Algorithm)是用于加密和解密的数学函数。密钥（Key）是加密或解密所需要的除密码算法之外的关键信息，密码员对明文进行加密时所采用的一组规则称为加密算法（Encyption Algorithm）。所传送消息的预定对象称为接收者(Receiver)，接收者对密文解密所采用的一组规则称为解密算法(Decryption Algorithm)。加密和解密算法的操作通常都是在一组密钥（Key）的控制下进行的，则分别称为加密密钥(Encryption Key)和解密密钥(Decryption Key)。下面介绍

加密和解密的过程，如图 2-1 所示：

：

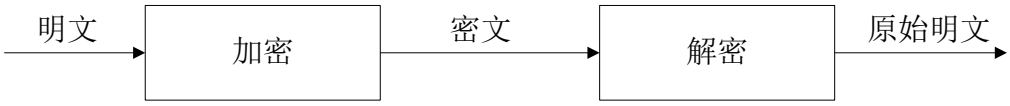


图 2-1 加密与解密过程

加密函数 E 作用于明文 M 得到密文 C，用数学公式表示为：E（M）=C。解密函数 D 作用于密文 C 产生明文 M，用数据公式表示为：D（C）=M。先加密后再解密消息，原始的明文将恢复出来，D（E（M））=M 必须成立。

信息安全的目的就是要保障网络环境下数字信息的有效性。所以密码学除了提供机密性外，还需要提供三方面的功能：完整性、抗抵赖性和可用性。

机密性：事对抗敌手被动攻击，保证信息不泄露给未经授权的主体。

完整性：对抗敌手主动攻击，防止信息被未经授权的主体篡改，也就是说入侵者是不可能用假消息代替合法消息。

抗抵赖性：主体无法在事后否认曾经对信息进行发生和接收等操作。

可用性：是保证信息及信息系统确实可随时为经授权的主体所用而不受到干扰或阻碍。

现代密码学用密钥解决了这个问题，密钥用字母 K 表示，密钥是由用户事先选定的较短的字符或数字序列叫，其作用是近似于打开保险箱的钥匙。所以密钥的集合构成了密钥空间，用 SK 表示的。密钥空间中含有不同的密钥的个数称为密码量，密钥量是衡量一个密码体制安全性的重要的指标。加密和解密运算都密钥 K 控制下操作的，即运算都依赖于密钥，并用 K 作为下标表示，加解密函数表达为：

E_K（M）=C；D_K（C）=M；D_K（E_K（M））=M 如图 2-2 所示：

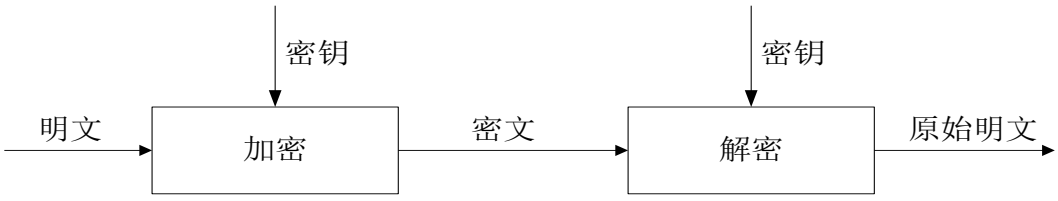


图 2-2 在 K 下加密与解密过程

有些算法在加密和解密过程中使用的不同的密钥，即加密密钥 K_1 与相应的解密密钥 K_2 是不同的，在这种情况下，加密和解密的函数表达式为：$E_{K_1}(M)=C$；$D_{K_2}(C)=M$。函数必须具有的特性是，$D_{K_2}(E_{K_1}(M))=M$，如图 2-3 所示：

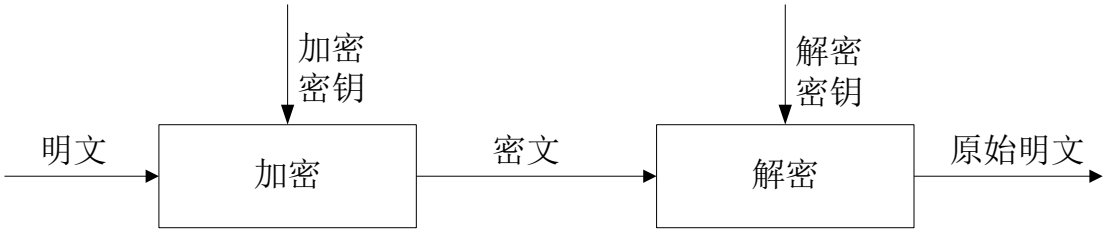


图 2-3 在密钥不同下加密与解密过程

2.2 密码算法分类

根据密钥类型的不同我们可以将密码技术分为两类：一类是对称密码算法又称为单钥体制；另一类是非对称密码算法又称双钥体制。

2.2.1 对称密码算法(Symmetric Cipher Algorithm)

秘密密钥算法通常称为对称密码算法或传统密码算法，也称单钥算法。它是应用较早的加密算法，技术成熟。对称密码算法基本原理是数据的发送方可以将明文或消息和加密密钥一起经过特殊加密运算处理后，使其将变成复杂的加密密文发送出去。接收方收到密文后，如果想解读原文，那么在解密过程中需要使用加密用过的密钥，也就是加密和解密过程中使用的是同一个密钥，以及具有相同算法的逆算法对密文进行解密，这样才能够使其恢复成我们想要读的明文。对明文加密有两种方式：一种是明文消息按字符逐位地进行加密称为流密码（Stream Cipher）；另一种是将明文消息分组即含有多个字符逐组的 进行加密。称为分组密码（Block Cipher）。对称加密算法缺点是在进行保密通信之前，双方都必须要通过安全信道传送所用密钥，这对于相距较远的用户可能是要付出很大的代价，甚至难以实现。另外，在有众多的网络用户在通信下，为了要使 n 个用户之间相互进行保密通信，将需要 n（n-1）/2 个密钥；当 n 很大时，代价也是很大。需要使用其他人不知道的惟一的密钥，这样会使得发收双方所拥有的密钥数量成几

何级数增长，密钥管理就成为了用户的负担。在分布式网络系统中，对称密码算法使用较为困难，主要原因是密钥管理非常地困难，使用成本也较高。对称加密算法有 DES、IDEA 和 AES 在计算机专网系统中广泛地被使用。

DES（Data Encryption Standard）数据加密标准是一种对称加密算法，是 IBM 公司在 70 年代发展出的一个加密算法。它主要应用在保护金融数据的安全中起到了重要的作用，在最初开发的 DES 是可以嵌入在硬件中的。例如 ATM(Automated Teller Machine)机即自动取款机就是用 DES 加密的。DES 加密原理是使用密钥长度为 64 位，其中 8 位是奇偶校验码位。其剩余的 56 位是真正密钥所使用的，这是一个迭代的分组密码，使用的技术称为 Feistel 网络，其中将加密的文本块分成两半。使用子密钥对其中一半应用循环功能，然后将输出的结果与另一半进行“异或”运算，接着再交换这两半，这一过程会继续下去，到了最后一个循环时就不需要交换了。DES 使用 16 个循环，采用了四种基本运算分别是异或、置换、代换和移位操作。DES 的常见变体是三重 DES，采用的是 168 位比特的密钥对明文进行三次加密的一种机制，要比 56 位比特密钥 DES 安全性强大的多。由于 DES 的整个体制是公开的，系统的安全性全靠密钥的保密。 目前，DES 使用是越来越少，原因在于其使用了 56 位密钥，则密钥比较容易地被破解，近些年来 AES 逐渐替代了 DES， AES 可以使用 128 位比特、192 位比特和 256 位比特密钥，并且可以用 128 位分组加密和解密数据。

AES（Advanced Encryption Standard）高级加密标准又称 Rijndael 加密算法是美国联邦政府采用的商业及政府数据加密标准。AES 的基本要求是采用了对称分组密码算法，分组密码算法通常是由密钥扩展算法和加密或解密算法两部分组的，密钥长度可以支持 128 位比特、192 位比特和 256 位比特，分组长度是 128 位比特，该算法易用于各种硬件和软件中。在应用方面，通过前面的分析得知，DES 的密钥比较容易地被破解，所以 DES 在安全上是很薄弱的，因为密钥容易被破解，但由于 DES 芯片的还在快速地大量生产，使得 DES 仍能暂时继续使用，为了提高算法安全强度，通常我们使用三级 DES，但是 AES 迟早是要替代 DES。

在对称密码算法中，数据加密和解密过程中所采用的密钥都是同一个密钥 K，因而其安全性是主要是依赖于所拥有密钥的安全性。对称密码算法的主要优点是加密和解密速度都很快，加密强度高，并且算法是公开的。该对称密码算法

最大的缺点是实现密钥的秘密分发困难，在大量用户的情况下，密钥管理非常地复杂，而且无法完成身份认证等功能，这样就不便于应用在目前的网络开放的环境中。DES（Data Encryption Standard）数据加密标准和 IDEA(International Data Encryption Algorithm)国际数据加密标准是目前最著名的对称密码算法，AES（Advanced Encryption Standard）高级加密标准是加密强度最高的对称密码算法。

2.2.2 非对称密码算法(Asymmetric Cipher Algorithm)

非对称密码算法又称公钥密码算法是用一个密钥进行加密， 而用另一个密钥进行解密。其中加密密钥是可以公开的，又称公开密钥（Public Key)，简称公钥。解密密钥必须保密又称私人密钥（Private Key)，简称私钥。

公钥密码算法的主要特点是密钥在加密和解密过程中是不同的，因此它可以实现多个用户加密的消息但只能由一个用户解读明文或者说只能由一个用户加密消息但多个用户可以解读。前者是用于公共网络中实现的保密通信，而后者是可用于认证系统中对消息进行数字签名。在加密文件中使用公钥密码算法时，只有使用匹配的一对公钥和私钥时，才能够完成对明文的加密和密文的解密过程。加密明文时采用的是公钥加密，解密密文时采用的是私钥才能完成解密，这样便可以阅读明文，而且在发送方即加密者知道收信方的公钥，只有收信方即解密者才是唯一知道自己私钥的人。

非对称密码算法的基本原理是：找到一种体制，从加密函数 E_k 计算解密函数 D_k 在计算上是不可行的，这样加密函数 E_k 可以公布，使任何人用之加密，而只有一个人知道解密函数 D_k，并能用于解密。由于公钥密码算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。广泛应用的公开密钥算法有 RSA 算法和美国国家标准局提出的 DSA。双钥体制的出现是密码学研究中的一项重大的突破，已是现代密码学诞生的标志。所以以公开密钥算法为基础的加密技术应用非常的广泛。

公钥密码算法的优点：扩展性好，当增加新用户时，只需要生产一对新密钥；当删除用户时，密钥可以很容易地从公钥密码算法删除；因为只需发布公钥，所以密钥的发布十分简单，安全和 Hash 函数配合可以提供信息的完整性鉴别和信息的抗否认性。

公钥密码算法的缺点：是加解密的速度慢，例 RSA 要比 DES 的速度慢一千到五千倍左右。其常用于共享密钥，数字签名等小数据量信息的加解密，而不用于大数据量文件的加解密。

2.3 相关的数论基础知识

定义 1 若一个大于 1 的正整数 p 除了 1 和 p 之外没有其它正因子，则称 p 是一个质数或素数。一个既不是质数也不是 1 的正整数称为合数。

定义 2 给定正整数 m，若 m | (a-b)，则称 a 与 b 对模 m 同余，记为 $a \equiv b \bmod m$。

定义 3 若 $ab \equiv 1 \bmod m$，则称 b 是 a 的对模 m 的乘法逆元素，或对模 m 的逆元素，在不引起混乱的情况下，记为 $a^{-1} (\bmod m)$ 或 a^{-1}。

定理 1 （算术基本定理）对任意正整数 n>1，有 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，其中 p_i 是素数，a_i 是正整数，($1 \le i \le k$)，若不计较因式的次序，这个表示式是唯一的，称为 n 标准的分解因式，或素因数分解式。

定理 2 在数论中，欧拉定理（也称费马-欧拉定理）是一个关于同余的性质。欧拉定理表明，若 n，a 为正整数，且 n，a 互素，(a，n) = 1，则 a^φ(n) ≡ 1 (mod n) 。

2.4 本章小结

本章主要介绍了密码学的概念、加密与解密运算、密钥体制即对称密钥体制和非对称密钥体制，并叙述了两类密钥体制的优缺点。以及与密码学相关的数论的知识。

第三章 数字签名技术在电子商务中的应用

加密的作用是对文件传送信息的进行保密，如果要防止他人对传输的文件的信息进行破坏，以及要确定发送方的身份，则我们需要用数字签名技术。在电子商务安全保密系统中，数字签名有着非常重要的地位，因为数字签名可以保证电子商务中数据的源鉴别、完整性和不可否认性。

目前数字签名使用较多的技术是双钥体制技术即，例如美国 RSA 数据安全公司的 PKCS(Public Key Cryptography Standards)、DSA（Digital Signature Algorithm）、国际电联电信委员会（ITU-T）制定的 X.509 认证和 PGP(Pretty Good Privacy) 基于 RSA 公匙加密体系的邮件加密软件。公钥加密系统采用的是非对称加密算法，1994 年美国国家标准协会（ANSI）公布了 DSS 数字签名标准，从而使公钥加密技术应用十分地的广泛。

3.1 数字签名的定义

数字签名是一种类似于写在纸上的普通的签名，数字签名通常定义两种互补的运算：一种运算是用于签名，另一种运算是用于验证。数字签名有两种：一种是对整体消息的签字，也就是消息经过密码变化的被签消息整体；另一种是对压缩消息的签字，是附加在被签字消息之后或在某一特定位置上的一段签字图样。而这种数据或变换是允许接收者用以确认的数据单元的来源和完整性，目的是为了保护数据，以防止他人伪造。数字签名主要是基于公钥密码体制的数字签名。

类似于手书签字，数字签名也应满足以下条件：(1)发方事后不能抵赖自己的签名；（2）任何其它人不能伪造签名；（3）收方对已收到的签字消息也不能否认；（4）如果当事人双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。

为了实现数字签名的目的，发送方必须向接收方提供非保密信息，以便后来能验证消息的签名；但是又不能泄露产生签名的机密信息，以防止他人伪造签名。所以，签名者和验证者可公用的信息不能太多。

3.2 电子商务中数据传输的安全性需求

如果电子商务系统的可靠性不高，那么可能被攻破而失窃，可靠性可能要求安全性来提供认证、完整性和不可否认性。可靠性并不等于安全性，服务器上的可靠协议对攻击者和授权用户都提供可靠的服务。匿名和安全保密性是彼此不同但又相互关联的特性。保密性是意味着信息的主人可以掌控信息，安全性要完全控制信息，匿名意味着找不到信息的主人，即身份与信息不关联，但匿名保证了个人的隐私。下面我们就讨论在电子商务中安全：

（1） 安全支付机构，以处理各种类型支付信息的传递和处理，例如借贷卡、信用卡和电子支票。另外还要提供三方保密数据分配。

（2）商业交易中数据的不可否认性，如果要保证交易双方否认，那么需要对各消息源的认证和数字签名技术来实现。

（3）保证经过 Internet 传递的数据的完整性，才能可靠地进行 Internet 商务，这是由数据完整性和保密性实现的。

（4）在 Internet 商务系统的基础设施中应包括一些的可信赖机构。例如 X.509 证书和数字签名认证。

这些要求的实现主要是借助数据的安全保密技术，其中最主要包括认证性、保密性、数据完整性、、不可否认性、安全协议和防火墙等等。

3.3 数字签名的过程

在传统的商业系统中，通常都是利用手书签字或者是印章来规定契约性的责任，以便在法律上能认证、核准和生效。如今，随着计算机通信网的发展，人们希望通过电子设备实现快递、远距离的交易，这样数字签名或电子签名就应运而生了，并开始用于商业通信系统中。例如在电子商务中，传送的文件是通过数据加密的方来保护电子签名的数据，但也只能防止第三方获得真实的数据。然而在交易过程中，对文件的否认、伪造、篡改和冒充等问题可以由电子签名来解决，则具体要求是消息的发送方首先要用一个 Hash 函数从报文文本中生成报文摘要即散列值，发送方用自己的私钥对这个散列值进行加密。其次，把加密后的消息摘要将作为附件和消息一起发送给消息接收方。最后，消息的接收方首先用与发

送方一样的 Hash 函数，从接收到的原始报文中计算出散列值，其次再用发送方的公钥来对消息附加的数字签名进行解密。在签名过程中，如果两个报文摘要相同，那么接受者能确定明文是发送方发的，满足了数字签名具有不可否认性。因为数字签名可以对原始的消息进行鉴别，这样接收者就不能对发送者发的消息进行篡改。

数字签名有两种功能：一种是能够确定报文确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名。另一种是数字签名能够确定消息的完整性。因为数字签名的特点是它能够代表了文件的特征，如果文件发生了改变，那么数字签名的值也将随着发生变化。也就是说不同的文件将会得到不同的数字签名。数字签名将会涉及到一个 Hash 函数、发送者的公钥和私钥。

3.4 数字签名的算法与 Hash 函数

Hash 函数又称为哈希函数、散列函数或杂凑函数，是密码体制中常用的一类公开函数。它是指将任意长度的消息映射成某一固定长度消息的一种函数。一般来说，Hash 函数主要是用于消息完整性检测和消息认证。例如，Hash 函数应用于数字签名系统有很多的好处：一方面可以提高签名的速度，当签名的消息 m 过长时，可用 Hash 函数对 m 进行压缩成某一固定范围内的数据 $m'=h(m)$，然后再计算签名 $s=Sign_k(m')$，其中 k 是签名密钥，$Sign_k$ 是签名函数。另一方面，可以不泄露要签名的消息，对消息 m 的签名是 $s=Sign_k(m')$，这里 Hash 函数 h 是公开的，$m'=h(m)$ 也一是公开的。根据 Hash 函数的性质，从 $m'=h(m)$ 恢复出 m 几乎是不可能，所以可以保密消息 m。

MD5（Message Digest Algorithm）消息摘要第五版函数是一种单向的散列函数，它是将任意长度的消息 M 压缩成 128 位固定长度的散列值 h 的消息摘要。MD5 散列函数要具有单向性，则必须要满足给定 M，很容易地计算 h，以便于软硬件的实现；当给定 h，根据 H(M)=h，反推 M 很难，说明函数具有单向性；当给定 M，找到另一个 M’满足 H(M)= H(M’)很难，说明函数具有弱抗攻击性，可以实现信息的完整性检验。在某些应用中，还需要满足抗碰撞的条件即找到两个随即的消息 M 和 M’，使 H(M)= H(M’)满足很难，即函数具有强抗攻击性。另

外 MD5 算法的运算包括位与、位或、位反和位异或，其均为基本运算，在计算机中是比较容易实现并且执行速度很快，是一种被广泛认可的单向散列算法。

3.5 RSA 加密算法和数字签名算法

1978 年，美国麻省理工学院（MIT）的 R.L.Rivest、A.Shami 和 L.Adleman 提出了基于数论构造的公钥的密码体制的方法，称作 MIT 体制，后来 RSA 取名来自开发他们三者的名字，又称为 RSA 体制。RSA 密码系统是较早提出的一种公开钥密码系统，RSA 算法的安全性是建立在“大整数的素因子分解的困难问题”基础上的，它是一种分组密码体制。

3.5.1 RSA 加密算法

RSA 算法是建立在数论中的可逆模幂运算上的，选取两个不同素数 p 和 q，n 是 p 和 q 的乘积，定义密钥空间 K={n，p，q，d，e}，算法描述：

（1）选择一对不同的、足够大的素数 p，q。

（2）计算 n=pq。

（3）计算 $\varphi(n)=(p-1)(q-1)$，同时对 p, q 严加保密，不让任何人知道。

（4）找一个与 $\varphi(n)$ 互质的数 e，且 1<e< $\varphi(n)$。

（5）计算 d，使得 de≡1 mod $\varphi(n)$ 即 $d \equiv e^{-1} \bmod \phi(n)$。

（6）公钥 KU={e，n}，私钥 KR={d，n}。

（7）加密时，先将明文变换成 0 至 n-1 的一个整数 M。若明文较长，可先分割成适当的组，然后再进行交换。设密文为 C，则加密过程为：$C \equiv M^e (\bmod n)$。

（8）解密过程为：$M \equiv C^d (\bmod n)$。

3.5.2 RSA 算法的速度

由于在运算中进行的都是大数计算，硬件实现的 RSA 的速度最快也只有

DES 的千分之一倍；软件实现的 RSA 的速度只有 DES 的百分之一倍。无论是在软件方面还是在硬件方面的实现，速度一直是 RSA 的缺陷，在速度上 RSA 无法与对称密钥体制相比，因此 RSA 体制多只用于密钥的交换和认证。所以 RSA 算法只能用于少量的数据加密。

3.5.3 RSA 数字签名算法

随着网络环境越复杂和网络用户越多，使用公开密钥密码算法越方便，其优点是特别适用于多用户的通信网，它大大减少了多用户之间通信所需要的密钥量，便于密钥的管理。公钥加密算法使用的是两个不同的密钥，其中一个密钥是公开的，另一个密钥是保密的。公开密钥可以保存在未加密的电子邮件信息中、系统目录内或公告牌里，网络用户都可以获得公开密钥。而私有密钥是用户专用的，由用户本人持有，它是用来对由公开密钥加密信息进行解密的。

RSA 算法中数字签名技术实际上是通过一个 Hash 函数来实现的。文件如果发生改变，数字签名的值也将随着发生变化。不同的文件将会得到不同的数字签名。一个最简单的 Hash 函数就是把文件的二进制码相累加，取最后的若干位。Hash 函数对发送数据的双方都是公开的。

数字签名 RSA 算法如下：用户 A 对消息 m 用解密变换 s $D_r(m)=m^d \bmod n$，其中 d，n 为用户 A 的私钥，只有用户 A 才知道它；用户 B 收到用户 A 的签名后，用户 A 用公钥和加密变换得到消息，因 $E_r(s)=E_r(D_r(m))=m^{de \bmod n}$,又 de≡1mod $\varphi(n)$ 即 de= $\varphi(n)$ +1，根据欧拉定理 $\varphi(n)$ =1 mod n，所以 $E_r(s)=m^{\varphi(n)+1}=m \bmod n$。如果明消息 m 和签名 s 一起发送给用户 B，用户 B 可以确定消息的确是用户 A 发送的，也就是说用户 A 和 B 不能否认消息的发送和接受，因为除了用户 A 外，其他任何人都不能由消息 m 产生 s。所以 RSA 签名方案是可行的。

但是 RSA 数字签名过程中存在着因计算方法和计算时间长的弱点，因此对消息 m 进行签名前，则需要对消息 m 作 MD5 变换。RSA 是较早开始使用的公钥密码体制，经受了多种攻击的检验，但没有一种对其产生致命的影响，因此 RSA 的安全性是较高的。RSA 被用于 SET 协议的 CA 证书当中，可用于手机签名。

RSA 的安全性是基于分解大整数的困难性假定，之所以为假定是因为至今还未能证明分解大整数就是 NP 问题，也许有尚未发现的多项式时间分解算法。如果 RSA 的模数 n 被成功分解为 p 和 q 的乘积，则立即获得 $\varphi(n)=(p-1)(q-1)$，从而能够确定 e 模 $\varphi(n)$的乘法逆元 d，即 $d \equiv e^{-1} \bmod \varphi(n)$，因此攻击成功。

3.5.4 RSA 算法的实现

RSA 算法的实现包括：密钥的生成、加密算法和解密算法。RSA 体制的安全性主要是依赖于大素数分解的困难性，为了保证 RSA 体制的安全，必须要认真地选择各参数，选择 p 和 q 必须为素数，且两个数要有足够的打，因为 n=pq，使得 n 分解在计算上是不可行的。所以在计算机中实现 RSA 算法时须要定义大数的数据结构。

```
typedef struct
{unsigned long int b [MAX_LENGTH];
unsigned int size;}BigNum;
```

RSA 算法的实现涉及到一些大数的基本运算，我们定义一个大数的基本运算库包括加法运算、减法运算、乘法运算、除法运算和取模运算等等，其中模乘运算和模幂运算是最重要的运算。

模幂算法是加密解密的核心算法，下面是 RSA 算法的 C 语言程序的实现：

```
#include <stdio.h>
int datamodul(int a, int b, int c)   /*该函数是实现幂的取余运算*/
{int r=1;
b=b+1;
while(b!=1)
   {r=r*a;
    r=r%c;
    b--;}
printf("%d\n",r);
return r;
}
```

```
int fun (int x, int y) /*该函数是判断 e 和 t 互素*/
{int t;
  while(y)
{t=x;
x=y;
y=t%y;
}
if(x==1)
return 0;     /*如果函数值返回为 0，则 x 与 y 互素*/
  else
return 1;   /*如果函数值返回为 1，则 x 与 y 不互素*/

}
void main()
{int p,q,e,d,m,n,t,c,r;
printf("请输入两个素数 p,q:");
scanf("%d,%d",&p,&q);
n=p*q;
printf("计算 n 为%d\n",n);
t=(p-1)*(q-1);                    /*求欧拉函数*/
printf("计算 t 为%d\n",t);
printf("请输入公钥 e:");
scanf("%d",&e);
if(e<1 || e>t || fun(e,t))      /*判断 e<1 或 e>t 或 e 与 t 不互素时，就重新输入*/
{    printf("e  不符合要求，请重新输入:");
        scanf("%d",&e);
        }
   d=1;
while(((e*d)%t!=1)    /*这段程序是求私钥 d*/
d++;
```

```
printf(“经过计算 d 为%d\n”,n);
printf(“加密请输入 1\n”);     /*加解密选择*/
printf(“解密请输入 2\n”);
scanf(“%d”,&r);
switch(r)
{case 1: printf(“请输入明文 m:”);   /*这段程序是加密求密文 c*/
        scanf(“%d”,&m);
        c=datamodul(m,e,n);
        printf(“则密文为%d\n” c);break;
case 2: printf(“请输入密文 c:”); /*这段程序是解密求明文 m*/
        scanf(“%d”,&c);
        m=datamodul(c,d,n);
        printf(“则明文为%d\n” m);break;
}
}
```

3.5.5 RSA 公钥和私钥的结构定义

解密模数和解密指数用到了 RSA 私钥。但是为了加快 RSA 解密计算的速度，采用了数论中的中国剩余定理又称为孙子定理对 RSA 算法进行计算。所以 RSA 私钥包含 p，q，d mod (q-1)，d mod (p-1)和 q-1 mod p，其中 p 和 q 为大素数，d mod (p-1)，d mod (q-1)，q-1 mod p 由计算过程中生成的。生成密钥步骤：

```
typedef struct {
unsigned int bits;
unsigned char modulus[MAX_RSA_LEN];     /*定义公钥 n 的最大长度  */
 unsigned char publicExp[MAX_RSA_ LEN];      /*定义公钥 e 的最大长度  */
unsigned char exp[MAX_RSA_LEN];                /*定义私钥 d 的最大长度*/
unsigned char prime[2][MAX_RSA_ LEN];              /*定义两个素数因子*/
 unsigned char primeExp[2][MAX_RSA_PRIME_LEN];
unsigned char coeffi[MAX_RSA_PRIME_LEN];
```

} RSA_PRIVATE_KEY; 下面是对生成 RSA 密钥的过程进行叙述：

第一步是 e 的值选择为 3 或者 25537；

第二步是随机地选择一个大素数 p，直到 gcd (e，p-1)=1，即表示 e，p-1 两个数的最大公约数为 1，简单的说就是两个数互质；

第三步是随机选择一个不同于 p 的大素数 q，直到 gcd (e,q-1)=1，即 e 与 q-1 互质；

第四步是计算 n=pq，根据欧拉定理得 $\varphi(n)=(p-1)(q-1)$；

第五步是计算 d，使得满足 de≡1 mod $\varphi(n)$ 式子；

第六步是计算 d mod (p-1)、d mod (q-1)和 q-1 mod p；

第七步是将 n，e 作为 RSA 公钥；将 n，e，d mod (p-1)，d mod (q-1) 和 q-1 mod p 作为 RSA 私钥。

3.5.6 随机数的产生

真正意义上的随机数或者随机事件是指在某次产生过程中是按照实验过程中表现的分布概率随机产生的，其结果是不可预测的和不可见的。而计算机中的随机函数是按照一定算法模拟产生的，其结果是确定的和可见的。所以用计算机随机函数所产生的“随机数”并不随机，是伪随机数。密钥的生成用到了随机数，而且公钥加密时的填充字符也用到了随机数。它必须具有足够的随机性，是因为防止破译者掌握密钥随机数规律性后，将会重新配制密钥。实现过程如下：第一步是对相邻两次敲击键盘的时间间隔进行记录，直到不再需要随机数；第二步是要计算 MD5（Message Digest Algorithm）消息摘要算法第五版，直到不再需要伪随机数。

3.6 RSA 的安全性分析

RSA 是较早开始使用的并应用比较广泛的公钥密码体制，已经受了多种攻击的检验，但是还没有一种对其产生致命的影响，因此 RSA 的安全性是较高的。RSA 可用在 SET 安全电子协议的 CA 证书当中，也可用于手机签名中。

3.7 本章小结

本章主要介绍数字签名的概念、原理和算法等，在这章节主要分析了 RSA 加密和数字签名的算法。RSA 数字签名算法包括签名算法和验证算法。首先是用了 MD5 算法对消息作散列进行计算，在签名的过程中我们则需要用用户的私钥，在验证过程中我们则需要用用户的公钥。如果用户 A 用签名算法将字符串形式的消息处理成签名，那么用户 B 用验证算法来验证签名是否是用户 A 对消息的签名，以便确认是用户 A 发送的消息，如果消息没有被篡改过，那么用户 A 一定发送过消息。

RSA 签名和 RSA 加密的异同点，其相同点都使用一对密钥即公钥和私钥，其不同点是 RSA 加密用公钥加密，用私钥解密；RSA 签名是用私钥签名，用公钥匙验证。

第四章 基于离散对数问题的数字签名

4.1 有限域上的离散对数

给定一个有限域F_q 和F_q^* 的一个生成元，对于F_q^* 的任意一个元素 h，求整数 a<q，使得$h=g^a$，称为有限域离散对数问题（Discrete Logarithm Problem Over Finite Field)。

4.2 椭圆曲线离散对数

椭圆曲线上所有的有理点外加一个无穷远点的特殊点构成的集合,按给定的加法运算构成一个 Abel 群。给定椭圆曲线 E 上一个阶 n 的基点 P,且点 Q 属于由 P 点生产的 n 阶循环群，求满足方程 Q=mP 的解 m，称为解椭圆曲线 E 上的离散对数问题(Discrete Logarithm Problem Over Elliptic Field)。

4.3 椭圆曲线的简介

椭圆曲线作为代数编码中的重要问题已有很长的研究历史，直到 1985 年，Neal.Koblitz 和 Victor.Miller 独立将其引入密码学中，提出了椭圆曲线密码算法即 ECC，ECC 既可以用于文件加密，又可以用于文件数字签名。利用有限域上椭圆曲线的点构成的群实现了离散对数密码算法。在《数字签名分析和实现》一文中详细地介绍了 DSA 算法，ECDSA（Elliptic Curve Digital Signature Algorithm）椭圆曲线数字签名算法被广泛应用在椭圆曲线上的变化，由 IEEE(Institute of Electrical and Electronics Engineers)美国电气电子工程师协会工作组和 ANSI（Amercian National Standards Institute）组织美国国家标准学会开发的。随即又展开了对 ECC 椭圆曲线密码学的研究，除了研究椭圆曲线外，还有人提出在其它类型的曲线例如超椭圆曲线上的实现 。

4.3.1 离散对数问题的分类

在密码学中，有三种群上的离散对数问题比较常用，它们是素数域的乘法群、有限域的椭圆曲线群和特征为 2 的有限域的乘法群。本文涉及到的是素数域乘法群的离散对数问题。可以表述以下：设 p 是一个素数，Z_p^*是的一个生成元。已知 a 为整数，求整数 b，使得等式 $g^b \equiv a(\mathrm{mod}p)$成立。如果 p 是一个适中的大整数，那么以上这个离散对数问题就可以被公认为困难问难，即不存在多项式时间算法来求解。

基于素数域上的离散对数问题的数字签名方案是一类常用的数字签名方案。其中包括著名的 ElGamal 数字签名方案、DSA 数字签名方案和 Okamoto 签名方案等等。

4.3.2 椭圆曲线密码算法优缺点

RSA 算法是既可以实现加密，又可以实现数字签名。其中 PGP 软件是基于 RSA 算法。RSA 算法的安全性是取决于模 n 的分解困难性，随着现代计算水平的提高，人们可以用计算机分解更大的数。因此 RSA 算法的密钥也要求越来越长。在电子商务中的 SET(Secure Electronic Transactions)安全电子协议中，规定了用户使用 1024 位比特长的 RSA 密钥，而认证中心 CA 使用了 2048 位比特长的 RSA 密钥。密钥长度加长会给我们带来两个问题：一个问题是运算速度会比较慢，另一个问题是密钥存储和管理问题。如果用 16 位比特长的 IC 卡实现电子钱包，那么就要用 1024 位比特的 RSA 算法，这样速度就会很慢，则要以秒进行计算。而 IC 卡或 32 位的 IC 卡里固化了 RSA 算法的芯片，则其价格较贵。椭圆曲线加密系统有很多是依赖于离散算法问题的加密系统组成，其中 DSA 就是一个很好的例子，DSA 是以离散对数为基础的算法。椭圆曲线数字签名系统已经被研究了很多年并创造了很多商业价值。由于其自身的优点，椭圆曲线密码学一出现便受到关注。现在密码学界普遍认为它将替代 RSA 成为通用的公钥密码算法，SET(Secure Electronic Transactions)电子安全协议的制定者已把 ECC 作为下一代 SET 协议中的非对称密码算法，目前 ECC 已成为研究的热点。另外，ECC 特别适用于计

算能力、集成空间受限和带宽受限例如在 Web 服务器上集中进行密码计算会形成瓶颈，这样 Web 服务器上的带宽有限使带宽费用高，采用 ECC 就可节省时间和带宽。

4.4 ElGamal 数字签名方案

ElGamal 密码体制是一种基于离散对数问题的双钥密码体制，既可用于数据加密，又可用于数字签名，其安全性主要是依赖于计算有限域上离散对数这一难题。密钥对产生办法。首先选择一个素数 p，两个随机数 g 和 x，其 g, x < p, 计算 y = g^x (mod p)，则其公钥为 y, g 和 p。私钥是 x。g 和 p 可由一组用户共享。

ElGamal 用于数字签名时。被签信息为 M，首先选择一个随机数 k,有 gcd(k,p-1) =1,即 k 与 p－1 互质，计算 a = g^k (mod p)，再用扩展 Euclidean 算法对下面方程求解 b：M = xa + kb (mod p - 1)，签名就是(a, b)。随机数 k 需要丢弃。验证时要验证下式：y^a * a^b (mod p) = g^M (mod p)，同时一定要检验是否满足 1<= a < p。否则签名容易伪造。ElGamal 用于加密时，被加密信息为 M，首先选择一个随机数 k，则 k 与 p－1 互质，然后计算 a = g^k (mod p) 和 b = y^k M (mod p)，即(a, b)为密文，是明文的两倍长。解密时计算 M = b / a^x (mod p) 。ElGamal 签名的安全性依赖于乘法群$(IF_p)^*$上的离散对数计算。素数 p 必须足够大，且 p-1 至少包含一个大素数。

ElGamal 用于数字签名时。被签信息为 M，首先选择一个随机数 k,有 gcd(k,p-1) =1,即 k 与 p－1 互质，计算 a = g^k (mod p)，再用扩展 Euclidean 算法对下面方程求解 b：M = xa + kb (mod p - 1)，签名就是(a, b)。随机数 k 需要丢弃。验证时要验证下式：y^a * a^b (mod p) = g^M (mod p)，同时一定要检验是否满足 1<= a < p。否则签名容易伪造。ElGamal 用于加密时，被加密信息为 M,首先选择一个随机数 k,k 与 p－1 互质,然后计算 a = g^k (mod p) 和 b = y^k M (mod p)，即(a, b)为密文，是明文的两倍长。解密时计算 M = b / a^x (mod p) 。ElGamal 签名的安全性依赖于乘法群$(IF_p)^*$上的离散对数计算。素数 p 必须足够大，且 p-1 至少包含一个大素数。

计算 a = gˆk (mod p)，再用扩展 Euclidean 算法对下面方程求解 b：M = xa + kb (mod p - 1)，签名就是(a, b)。随机数 k 需要丢弃。验证时要验证下式：yˆa * aˆb (mod p) = gˆM (mod p) ，同时一定要检验是否满足 1<= a < p。否则签名容易伪造。ElGamal 用于加密时，被加密信息为 M，首先选择一个随机数 k，k 与 p - 1 互质，然后计算 a = gˆk (mod p) 和 b = yˆk M (mod p) ，即(a, b)为密文，是明文的两倍长。解密时计算 M = b / aˆx (mod p) 。

计算 a = gˆk (mod p)，再用扩展 Euclidean 算法对下面方程求解 b：M = xa + kb (mod p - 1)，签名就是(a, b)。随机数 k 需要丢弃。验证时要验证下式：yˆa * aˆb (mod p) = gˆM (mod p) ，同时一定要检验是否满足 1<= a < p。否则签名容易伪造。ElGamal 用于加密时，被加密信息为 M，首先选择一个随机数 k，k 与 p - 1 互质，然后计算 a = gˆk (mod p) 和 b = yˆk M (mod p) ，即(a, b)为密文，是明文的两倍长。解密时计算 M = b / aˆx (mod p) 。

因子以抵抗 Pohlig-Hellman 算法的攻击。被签消息 M 一般都应采用信息的 Hash 值，例如 SHA（Secure Hash Algorithm）安全杂凑算法。ElGamal 的安全性主要是依赖于 p 和 g 的值，如果 p 和 q 选取不适当，那么签名容易被伪造，所以在签名过程中应保证 g 对于 p-1 的大素数因子不可约的。一般的 ElGamal 数字签名方案：在系统中有两个用户 A 和 B，A 要发送消息到 B，并对发送的消息进行签名。B 收到 A 发送的消息和签名后进行验证。

(1)系统初始化

选取一个大的素数 p，g 是 GF(p)的本原元。h：GF(p)→GF(p)，是一个单向 Hash 函数。系统将参数 p、g 和 h 存放于公用的文件中，在系统中的每一个用户都可以从公开的文件中获得上述参数。

(2)对发送的消息进行数字签名的过程

假定用户 A 要向 B 发送消息 m [1,p-1]，并对消息 m 签字。第一步：用户 A 选取一个 x [1,p-1]作为秘密密钥，计算 y= gˆk (mod p)作为公钥。将公钥 y 存放于公用的文件中。第二步：随机选取 k ，k 的取值范围在[1,p-1]之间且

gcd(k,(p-1))=1，计算 r=gˆk(modp)，对一般的 ElGamal 型数字签名方案有签名方程（Signature Equation)：ax=bk+c(mod(p-1))。

其中(a，b，c)是(h(m),r,s)数学组合的一个置换。由签名方程可以解出 s。那么(m,(r,s))就是 A 对消息 m 的数字签名。第三步：A 将(m,(r,s))发送到 B

(3)数字签名的验证过程

当 B 接收到 A 发送的消息(m,(r,s))，再从系统公开文件和 A 的公开文件中获得系统公用参数 p，g，h 和 A 的公钥 y。由(m,(r,s))计算出(a，b，c)验证等式： yˆa * aˆS (mod p) = gˆM (mod p)是否成立。

D.Bleichenbache“GeneratingElGamal Signatures Without Knowing the Secret Key”中提到了一些攻击方法和对策。ElGamal 的一个不足之处是它的密文成倍扩张。

美国的 DSS(Digital Signature Standard)的 DSA(Digital Signature Algorithm)算法是经 ElGamal 算法演变而来。

4.5 DSA 数字签名方案

DSA（Digital Signature Algorithm)数字签名算法是在 ElGamal 算法和 Schnorr 算法基础上设计的。它也是一种双钥密码体制，该算法只能用作对文件进行数字签名，而不能对文件进行加密，这也是与 ElGamal 算法不同之一。DSA 算法使用公开密钥目的是为了接受者验证数据的完整性和发送者的身份。其安全性是基于解离散对数问题的困难性。下面其介绍原理：

（1）参数产生阶段

L 是从 512 位到 1024 位比特长的素数并且可被 64 除尽的即可供使用，其中 p 是 L 位长的素数， q 是 160 位比特长且和 p-1 互素的因子(q | p-1)。选择 g = h(p-1)/q，其中 h 是小于 p-1 并且满足大于 1 的任意数（1<h<p-1)，每个用户选取私钥并计算他们的公钥选择 x 是小于 q 的数（0<x<q)。计算 $y = g^x \pmod p$。

（2）签名生成阶段

k 选取的是小于 q 的随机数或拟随机数（0<k<q)，计算 $r = (g^k \bmod p) \bmod q$ ，$s = [k^{-1} (h(M) + xr] \bmod q$，发送签名 (r，s)及消息 M，验证签名只需计算：$w = s^{-1} \pmod q$ ，$u_1 = (SHA(M).w) \pmod q$ ，$u_2 = rw \pmod q$ ，

$v=(g^{u_1}.y^{u_2}(\bmod p))(\bmod q)$，如果 v=r， 则签名有效。

4.6 ElGamal 和 DSA 两种方案的比较

则两种方案有以下缺陷：

（1）ElGamal 算法既可以用于签名又可以用于加密或解密，而 DSA 算法只能用于签名，不能用于加密或解密。

（2）方案的执行速度慢。由于上面两种方案算法涉及到乘法逆元的运算，影响了签名的速度。

（3）安全性有待于提高。散列函数和数字签名结合使用，能够增加其安全性,在 2005 年 2 月来自上东大学的王小云教授理论破解了散列函数 MD5 和 SHA 算法，这样会对数字签名安全性产生了影响。安全性有待于提高。散列函数和数字签名结合使用，能够增加其安全性，在 2005 年 2 月来自上东大学的王小云教授理论破解了散列函数 MD5 和 SHA 算法，这样会对数字签名安全性产生了影响。

4.7 本章小结

本章主要介绍了基于离散对数问题的数字签名方案，叙述了椭圆曲线发展的背景，分析了 ElGamal 数字签名方案和 DSA 数字签名方案。得出基于该问题的数学方面的方案存在缺陷。

第五章 改进的数字签名方案

5.1 改进的数字签名方案

随着科技的发展和密码学研究的不断进步，基于大整数因式分解或离散对数问题的数学难题随时可能被攻破。本文是建立在两个数学难题的签名方案，该方案包括三个阶段即参数和密钥生成阶段、签名生成阶段和签名验证阶段 ：

（1） 参数和密钥生成阶段

假设 p 是一个大素数，且 $p=4p_1q_1+1$，则 $p_1=2p_2+1$， $q_1=2q_2+1$，其中 p_1、p_2、q_1、q_2 是不同的大素数。让 $n=p_1q_1$，则 $g^n\equiv 1\bmod p$，$g^{p_1}\neq 1\bmod p$ 和 $g^{q_1}\neq 1\bmod p$，其 g 是公开的。然后选取一个单向杂凑函数 H（x，y），并将 p，n，H(x,y)都公开。随机选择一个数 x（1<x<n/2），并有 gcd(x，p-1)=1。计算 $y=g^{x^2}\bmod p$，$z=g^{x^{-2}}\bmod p$，其 $xx^{-1}=1\bmod n$；其中用户将 y，z，n 和 p 是签名公钥，x， p_1， q_1 是签名私钥。

（2）签名生成阶段

m 是被签名的消息，如果用户想对消息 m 进行签名，那么签名过程如下：第一步是要随机选择一个整数 k(1<k<n/2)，且有 gcd(k，n)=1；第二步是计算 $r=g^{k^2}\bmod p$；第三步是计算 $e=H(r,m)\bmod p$；第四步是计算 $s=(x+x^{-1})e\bmod p$；第五步是传送 $sig(m)=(e,s)$ 作为签名。

（3）签名验证阶段

（e，s）是消息 m 的签名，如果用户 B 想签名（e，s），那么验证过程如下：第一步是由 s，y，z，e 可以计算 $\bar{r}=g^{s^2}y^{-1}z^{e^{-2}}g^{-2e}\bmod p$；第二步是检测 $e=H(\bar{r},m)\bmod p$ 式子是否成立，如果等式成立，那么 sign(e，s)就是 m 的合法签名，要不然为不合法的签名。

定理 令 $p=4p_1q_1+1$，其 $p_1=2p_2+1$，$q_1=2q_2+1$，p_1，p_2，q_1，q_2都是素数，p 也可能是素数。

证明 若 p_1，q_1都是素数，则 p_2，q_2可以是下列形式：

$p_2=3m+2$；$q_2=3n+2$，其 m 和 n 是整数。

将 p_2 和 q_2 分别代入等式 $p_1=2p_2+1$ 和 $q_1=2q_2+1$ 有 $p_1=2p_2+2=2(3m+2)+1=6m+5$，$q_1=2q_2+1=2(3n+2)+1=6n+5$，代入 $p=4p_1q_1+1$，得 $p=4p_1q_1+1=4(6m+5)(6n+5)+1$=144mn+120m+120n+101，当 m=3，n=1 时，计算出 p=1013 是素数，只有当 m，n 取一定的值时，p 才有可能是素数。

定理如果用户 A 使用了上述签名算法进行签名，那么验证用户 B 一定得收签名。

证明 因为 $s=(x+x^{-1}e)k \bmod r$，所以有 $s^2=(x^2+2e+x^{-2}e^2)k^2 \bmod n$，又因为 g 是有限域 F(P)中 n 阶元，所以 $g^{s^2}=g^{x^2}g^{2e}g^{x^{-2}e^2}g^{k^2} \bmod p$ 又因为 $y=g^{x^2} \bmod p$，$z=g^{x^{-2}} \bmod p$，所以得 $g^{s^2}=yg^{2e}z^{e^2}g^{k^2}g^{s^2} \bmod p$，$g^{k^2}=y^{-1}g^{-2e}z^{-e^2} \bmod p$，又因为 $r=g^{k^2} \bmod p$，所以 $\bar{r}=r=y^{-1}g^{-2e}z^{-e^2}g^{s^2} \bmod p$，因此 $e=H(r,m)$即验证用户 B 一定得接受签名。从等式 $y=g^{x^2} \bmod p$ 中，我们得知，要计算出 x 就相当于计算分解因素 n 和离散对数。

5.2 该方案的安全性分析

第一种情况分析是对抗从公钥（p，n，g，y，z）中揭露出密钥 x 的攻击。攻击者只需要从方程 $y=g^{x^2} \bmod p$ 中求解 x，而计算 x 的难度也就相当于分解 n 和求解离散对数。

第二种情况分析是对抗从消息 m 的签名 sign（e，s）中导出密钥 x 的攻击。由于 H（x，y）是一个单向杂凑函数，所以攻击者几乎是不可能从 $e=H(r,m)$ 式子中求解出 r，即使攻击者求出 r，也需要从 $r=g^{k^2} \bmod p$ 式子

中求出 k，才能从 $s=(x+x^{-1}e)k \bmod n$ 式子中求出 x，但是解方程 $r=g^{k^2} \bmod p$ 相当于求解两个难题的困难性，所以在这种情况下，攻击者要想得到用户私钥要比求解两个难题的困难性还要大。

第三种情况分析是对抗具有计算因数分解能力或具有离散对数能力的攻击者。要想求解 x，就必须同时具有两个数学难题的计算能力，如果只具备一种数学难题能力仍然不能求出 x，而不知道 x 我们还是无法计算出 s，从而也不能伪造签名。

5.3 本章小结

在上述研究的方案中，得到 p，n，p_1，p_2，q_1，q_2 后就可以销毁，因为在以后的签名过程中和验证过程中都不会用到，另外所有的用户都可以共用 p 和 n，这样会比数字签名方案基于一个数学难题的要好，因为其改进的方案的安全性是基于两个问题的。

第六章 结束语

随着计算机网络和信息技术的发展，信息安全在各领域发挥着越来越重要的作用，其中密码学已成为信息安全技术的核心，而数字签名技术是电子商务的核心技术之一，数字签名技术可以提供防伪功能，其数字签名具有不可伪造的特性，所以在防止重放攻击的情况下，可以用于厂家给贵重商品提供防伪标识。随着计算机网络的发展，过去依赖于手书签名的各行各业中，现在都可用电子数字签名来代替，它是实现电子商务、电子支票、电子出版等系统安全的重要保障。

本文是主要研究数字签名的算法，在建立大整数因式分解和离散对数难题上提出的新的算法，同时基于这两个数学难题的基础上，其安全性要比基于一个数学难题的的安全性高的多。通过这三年对数字签名知识的学习和研究，在写本文之前，我做了以下的准备：首先是通过阅读大量的文献，主要是通过图书馆网站下载论文看国内在这方面研究的现状，发现国内的数字签名发展和国外相比较，还有一定的差距，不过这些年我国在这方面发展的很快。其次，在阅读文献的基础上，认识到密码学理论知识与计算机及数学学科有着密切的联系。最后，在这些充分的准备基础上，提出了改进的数字签名技术。

在生成和验证数字签名的过程中需要完善,只有在广泛使用 SSL（Secure Sockets Layer）安全套接层建立安全链接的 Web 浏览器,才有可能频繁地会用到数字签名技术。例如一个公司要对其员工在网络上的行为进行规范，需要建立广泛协作机制来支持数字签名的实现。支持数字签名技术是 Web 发展的目标,需要确保数据在传送过程中的保密性、完整性及不可否认性才能够保证在线商业的安全交易。其中安全问题是阻碍电子商务广泛应用的最大问题，需要改进数字签名在内的安全技术措施和确定 CA 认证权的归属问题是解决电子商务安全问题的关键。

电子商务的发展是有赖于电子商务服务的模式和领域的创新，数字签名技术的广泛使用和普及将会给电子商务带来了生机和活力。除了数字签名技术外，还有其他的密码技术，如加密在电子商务中也有着广泛的用途。

随着新一代基于 IC 卡和密码技术的身份验证的推广，电子商务和数字签名将会有着更加广泛的应用和综合的发展空间。

参考文献

[1] Shamir A.Identity-based cryptosystems and signature schemes.Advances in Cryptology-CRYPTO’84,LNCS196,Springer-Verlag,Berlin,1984, 47–53.

[2]Chayn D.Van Heijst E Group signatures,1991,50-90.

[3]Ohtak,Okamoto. E.Practical extension of Fiat-Shamir scheme Electr.Lett[J].1988,24(15):955-956.

[4] Chang C and Lin C. An ID-based signature scheme based upon Rabin's public keycryptosystem.Proceedins 25th Annual[J] IEEE International Carnahan Conference onSecurity Technology,October 1-3,1991, 139-141.

[5] Nishioka T,Hanaoka G,and Imai H. A new digital signature scheme on ID-based key-sharing infrastructures. Information Security and International Workshop[J] ISW'99,LNCS 1729,Springer-Verlag,Berlin,1999, 259-270.

[6] Joux A. A one round protocol for tripartite Diffie-Hellman.Algorithmic Number Theory Symposium[J] ANTS-IV,LNCS 1838,Springer-Verlag,Berlin,2000, 385–394.

[7] F.Zhang and K.Kim. ID-based signature and ring signature from pairings[J] ASIACRYPT 2002,533-547.

[8] Fiat A.Shamir A How to prove yourself:Practiacal solution to identification and signature problems,1987,28-80.

[9] J.Herranz and G.Saez.New dentity-based ring signature schemes[J].ICICS 2004,LNCS,Springer,2004,27-39.

[10]ElGamal T A public key cryptosystem and a signature scheme based on discrete logarithms,1985,20-115.

[11] Cha J and Cheon J. An identity-based signature from Gap Diffie-Hellman groups[J]. PKC 2003, 18-30.

[12] Libert B, Quisquater J. The exact security of an identity based signature andits applications[J].http://www.iacr.org/2004/102.

[13] R.Sakai,K.Ohgishi,M.Kasahara. Cryptosystems Based on Pairings[J].

in Symposium on Cryptography Information Security,2000.

[14] C.Cocks.An identity based encryption scheme based on quadratic residus[J]. in Cryptography and Coding,LNCS 2001,360-363.

[15] Hess F. Efficient identity based signature schemes based on pairings[J].SAC2002, LNCS 2595, 2003,310–324.

[16] Chien H,Jan J and Tseng Y. RSA-based partially blind signature with low computation[J] Proceedings of Eighth International Conference on Parallel and Distributed Systems,ICPADS 2001, 385-389.

[17] Schnorr C.P, Security of blind discrete log signatures against interactive attacks[J].ICICS2001, LNCS2229, ,Springer-Verlag,2001,l-12.

[18] Chaum D and Heyst E. Group signatures[J]. Advances in Cryptology—EUROCRYPT'91,LNCS 547,Springer-Verlag,Berlin,1992,57-265.

[19] 陈兵．信息安全与数字签名技术．北京邮电大学学报, 2003, 1 (24): 34-37.

[20] 王振武. 数字签名技术的研究. 辽宁大学学报, 2004, 6 (14): 245-250.

[21] 张先红. 数字签名原理及技术. 北京: 机械工业出版社, 2004（90-100）.

[22] 卢开登. 计算机密码学—计算机网络中的数据保密与安全[M]. 清华大学出版社，2007（200-220）.

[23] 杨千里，王育民等. 电子商务技术实务. 北京: 电子工业出版社，2001 (90-110) .

[24] 章照止. 现代密码学基础. 北京: 北京邮电大学出版社，2004 (82-96).

[25] 杨波. 现代密码学. 北京: 清华大学出版社，1999 (50-155).

致谢

首先由衷的感谢我的导师魏仕民教授，感谢魏老师为我提供了良好的学习条件，营造良好的学习氛围。在这种学习氛围中，我感受到了魏老师严谨治学的态度和做学术科研的精神．在攻读硕士的三年中，魏老师为我们提供了和谐自由的学习环境，他对科学敏锐的洞察力和极强的预见性，给我的研究以莫大的启发。三年来，不仅从魏老师身上学到了丰富的专业理论知识，更重要的是他那精益求精的科研态度和对工作高度负责的敬业精神。这对于我今后的学习和工作都是笔宝贵的财富

我还要感谢计算机科学与技术的诸位老师和陈国龙教授、洪留荣教授和张明新在学习上给予的指导和帮助，此一并致以深深的谢意！感谢朝夕相处的同窗好友以及师弟师妹们！

最后，我要感谢出席论文答辩会的专家们，在百忙之中给予我的指导！

攻读硕士学位期间出版或公开发表的论著、论文

（1）陈月荣.基于 Internet 上电子商务系统的安全[J].现代交际（学术版）.2010（3）:108-109