致谢

本文是在导师李善庆教授的悉心指导下完成的。李老师学识渊博、治学严谨、诲人不倦，使我受益非浅。多年来，无论在学习上还是生活上，李老师都给了我很大的帮助和鼓励，使我在如何应用数学知识分析解决实际问题方面收获良多。在此，谨向李老师表示由衷的感谢。

此外，还要向其他所有帮助和鼓励我的老师和同学们，对一直关心和鼓励我的亲人朋友们致以深深的谢意！

摘要

在当今计算机网络迅速普及发展的信息时代，信息安全成为被普遍关注的重大问题，使用密码是有效可行的方法。本文首先介绍计算机密码学的发展史、现状和趋势。并通过对现有的主要的加密解密算法，特别是椭圆曲线密码体制的分析，揭示加密解密算法的特点与技术关键。在深入研究椭圆函数的及其他数学理论的基础上，提出了一套更有效，安全性更好的基于椭圆函数的加密解密算法。之后，用基于椭圆函数的加密解密算法结合现有的密码机制设计了一个新的密码系统。最后对算法的可行性，计算复杂度，安全性进行了分析，并给出了该算法的软件实现。

关键字： 密码学、椭圆函数、椭圆曲线密码体制。

Abstract

With the development of computers and the population of network, the security of the information has become the more important matter. Cryptology is the most effective method. First, this paper introduces the phylogeny, present situation and direction of the cryptology. According to the analysis of the existing cryptological algorithm, especially the cryptosystem based on ellipse curve, it discloses the characteristic and key technique of the cryptology. Through deep researching of ellipse function and other mathematical theory, it puts forward a new cryptographic function based on the ellipse function, which has better security and availability. Then it designed a new cryptosystem combined with this function and existing cryptological principle. Finally, it analyses the availability, complexity and security of the cryptology based on the ellipse function. Also it provides software implementation of the cryptosystem.

Key words: cryptology, ellipse function, cryptosystem based on ellipse curve

第一章 绪论

§1.1 引论

在当今计算机飞速发展的信息时代，信息作为一种重要的资源，在社会生产、生活中的作用日益显著。特别是计算机网络的深入普及，打破了传统的行业、地域和发展空间的概念，把地球上的人们笼罩在一张密密麻麻的信息大网中。围绕信息与信息技术，国家与国家之间，集团和集团之间，甚至个人和个人之间展开着尖锐激烈的斗争，这种斗争的最高形式可以用“信息战”来概括。美国著名的未来学家阿尔温·托夫勒声称：“电脑网络的建立与普及将彻底改变人类生存及生活的模式，而控制与掌握网络的人就是人类未来命运的主宰。谁掌握了信息，控制了网络，谁就将拥有整个世界。”美国前任总统克林顿声称：“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”“当21世纪即将降临的时候，美国的敌人已将战场从物理空间扩展到虚拟空间。”美国前陆军参谋长沙利文上将称：“信息时代的出现将从根本上改变战争进行的方式，”“信息是取得胜利的本钱”。信息战的实质是，运用精确制导武器、干扰器、计算机病毒等各种进攻性信息手段，攻击敌方的信息和信息系统，使其指挥与控制体系瘫痪，达到不战而胜的目的；运用己方的信息和信息系统，使部队全面了解战场情况，对敌实施有效打击，夺取战争的胜利。信息战核心是获取“信息控制权”。海湾战争中，美国将带有计算机病毒的微机芯片装入伊拉克从法国购买的用于防空系统的新型打印机中，达到了使伊拉克军事指挥中心计算机失灵的目的，充分显示了现代技术条件下“信息控制权”的关键作用。信息战突破了传统的地缘概念，无法用领土、领空、领海来划分，其特点也更加隐蔽，被称为是一场“无硝烟”的战争。由此可见，建立安全的“信息边疆”，将是确保国家安全的时代主题。

信息领域的严峻斗争，使我们认识到，只讲信息应用是不行的，必须同时考虑信息安全问题。由于信息网络国际化、社会化、开放化、个人化的特点，使它在提供人们“技术共享”、“信息共享”的同时，也带来了不安全的阴影。信息社会并不安宁，网上信息的被泄露、篡改和假冒，黑客入侵，计算机犯罪，计算

机病毒传播等，对网络信息形成重大威胁。因而，人们对网络处理的安全性提出了一些要求：

（1） 通信线路最明显的一个不安全的因素是他人可以很容易地窃听电话而获得有价值的信息。用卫星微波接力传递信息，对于凡是愿意架设天线的人们，这些信都可以认为是公开的。所以要设法保护通信的信息不被窃听或篡改破坏。

（2） 人们希望对于自己拥有的资源具有特权。担心他人通过网络非法“入侵”自己的资源，所以希望网络能够提供对访问者的合法性检查。

（3） 人们更担心“入侵”者可能访问信息资源中存在的隐含通道，这使得进入者可能窃取高度机密的信息亦可能设置病毒而使信息系统崩溃。

（4） 人们在心理上要求一种互相信任感。反映在网络技术上，不仅要求网络有能力确认用户的合法性，而且网络亦不可能对用户进行欺骗。用户希望对自己拥有的信息在网络中的流向或存留有一个完全确切的了解和掌握。

这些担忧提出了网络的安全性问题，同时也反映了信息安全的应该实现的几多方面，信息安全包括：

信息的保密性：保证信息不泄漏给未经授权的人。

信息的完整性：防止信息被未经授权者篡改。

信息的可用性：保证信息和信息系统确实为授权者所用，防止由于计算机病毒或其它人为因素造成系统的拒绝服务，或者为非法者所用。

信息的可控性：对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。

信息的不可否认性：保证信息行为人不能过后否认自己的行动。

保护信息安全涉及面很宽，它包括着技术、管理、制度、人员和法律的诸多方面。仅就技术而言，有防病毒、防电磁泄漏、物理安全防护、系统安全防护、密码保护等。解决信息安全的基本策略是综合治理。信息安全决不是单靠某一项措施或某一项技术所能奏效的。

密码是实现一种变换，利用密码变换保护信息秘密是密码最原始、最基本的功能；然而，随着信息和信息技术发展起来的现代密码学，不仅用于解决信息的保密性，而且也用于解决信息的完整性、可用性、可控性和不可抵赖性。可以说，密码是保护信息安全的最有效的手段，也是保护信息安全的关键技术。

密码作为运用于军事和政治斗争的一种技术，历史悠久。过去密码的研制、生产、使用和管理都是在封闭的环境下进行的。七十年代以来，随着计算机、通信和信息技术的发展，密码领域发生了新的变化，这个变化是：密码应用范围日益扩大，社会对密码的需求更加迫切，密码研究领域不断拓宽，密码科研也从专用机构走向社会和民间，密码技术得到了空前发展。

当前，密码学不仅在保护党政领导机关的秘密信息中具有重要的、不可代替的作用，同时，在保护经济、金融、贸易等系统的信息安全，以及在保护商业领域如网上购物、数字银行、收费电视、电子钱包的正常运行中也具有重要的应用。有人把密码技术看作信息高速公路的保护神。随着信息和信息技术的发展，电子数据交换逐步成为人们交换的主要形式，密码在信息安全中的应用将会不断拓宽，信息安全对密码的依赖会越来越大。

§1.2 密码学的发展历史，现状和趋势

§1.2.1 什么是密码

要研究密码学首先就要知道什么是密码。一般来说，任何一种密码体制包括5个要素：需要采用某种方法来掩盖其要传送的信息或字符串称为明文；采用某种方法将明文变为另一种不能被非授权者所理解的信息或字符串的过程称为加密变换；经加密过程将明文变成的信息或字符串称为密文；用于具体加密编码的参数称为密钥，将密文还原为明文的过程称为解密变换。

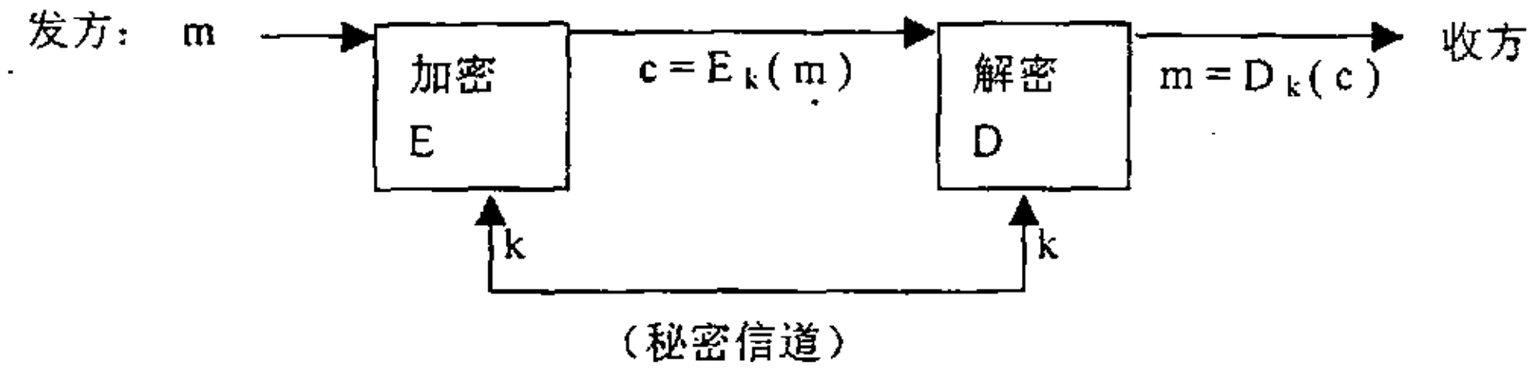
那么，什么是密码？简单地说它就是一组含有参数k的变换E 。设已知信息m，通过变换E_k得密文 ，即

$$c = E_k(m) \quad m = D_k(c)$$

这个过程称之为加密，参数 k 称之为密钥。加密算法 E 确定之后，由于密钥 k 不同，密文c也不同。

当然不是所有含参数 k 的变换都可以作为密码，它要求计算 $E_k(m)$不困难，而且若第三者不掌握密钥 k，即使截获了密文 c，他也无法从 c 恢复信息 m，也就是反过来从 c 求 m 极为困难的。以后称 m 为明文。

通信双方一为发言方，或简称为发方，另一方为收信方或简称收方。传统的保密机制可用图 1.1 表示。



从密文 c 恢复明文的过程称之为解密。解密算法 D 是加密算法 E 的逆运算，解密算法也是含参数 k 的变换。传统密码加密用的密钥 k 与解密用的密钥 k 是相同的，所以有时也叫对称密码。通信双方用的密钥 k 是通过秘密方式出双方私下约定产生的，只能由通信双方秘密掌握。如果丢失了密钥，则密码系统不攻自破。密钥的重要性可想而知。

密码加密算法的对立面就是密码分析，也就是密码的破译技术研究。加密与破译是一对矛盾，了解破译对研究加密是非常必要的。总的说来密码分析学是研究在不知密钥的情况下，利用密码体制的弱点来恢复明文的一门学科。对密码的攻击主要可分为以下几种：

（1）唯密文攻击。即密码分析者仅仅掌握若干密文。不言而喻，这些密文都用同一加密算法和密钥加密的。密码分析者的任务是尽可能多地恢复明文或者推算出密钥。找出密钥就可以一劳永逸地解出其它被加密的信息。即已知 $c_i=E_k(m_i)$，i=1,2...,l. 推出 $m_1,m_2,...,m_l$ 或推出 l。或从 $c_{l+1}=E_k(m_{l+1})$推出 m_{l+1}。

（2）已知明文攻击。密码分析者不仅掌握若干的密文，还知道对应的明文本身。密码分析者利用它推出用来加密的密钥，或导出加密算法。即已知 $c_i=E_k(m_i)$ 及 m_i，i=1,2,...,l，推出 k，或从 $c_{l+1}=E_k(m_{l+1})$推出 m_{l+1}。显然已知明文攻击较之唯密文攻击有更强的攻击力，掌握的关于该密码的信息也更多。

（3）选择明文攻击。密码分析者不仅获得若干明文机器相应的明文，而且掌握的明文还加以挑选。不消说，比已知明文攻击条件更苛刻。明文是经过选择的，必然提供了更多可供破译的信息，攻击力更强了。密

码分析者利用来推出加密的密钥或加密算法，或由用同一加密算法及密钥加密的新密文推出对应的明文。

一般说来，好的加密算法是可以公开的，也是不怕公开的。公开了不会从根本上有利于攻击者。只要敌方不掌握密钥，谁也没有有效的办法从密文恢复明文。（请注意这里指的是有效的算法。）数据加密标准 DES 就是这样。不过新拟议中的美国加密标准还是打算将算法隐蔽起来，这样会给攻击者增加麻烦。但目的不是全靠算法保密来达到安全。

实际上所有的加密算法都是可以破译的。所以实际上不存在不可破译的密码。如果破译所需的计算能力和时间是现实所不能实现的，则称这样的密码是安全，或计算上安全的。比如破译所需时间要几十个世纪，事实上不可能作到。退一步讲，若保密有效时间为一年，破译要 5 年，即使破译了也没意义了。破译一密码需要的计算时间和计算能力的综合（实际上也就是破译算法的时间复杂度和空间复杂度）成为工作因子。

§1.2.2 密码学的发展历史，现状和趋势

密码通信的历史极为久远，其起源可以追溯到几千年前的埃及，巴比伦，古罗马和古希腊。古典密码术虽然不是起源于战争，但其发展成果却首先被用于战争。交战双方都为了保护自己的通信安全，窃取对方情报而研究各种方法。世界上最早的一种密码产生于公元前两世纪，是由一位希腊人提出的，人们称之为棋盘密码，原因为该密码将 26 个字母放在 5×5 的方格里，i,j 放在一个格子里，具体情况如下表所示

	1	2	3	4	5
1	A	b	c	d	e
2	F	g	h	ij	k
3	L	m	n	o	p
4	Q	r	s	t	u
5	V	w	x	y	z

这样，每个字母就对应了由两个数构成的字符 α β，α 是该字母所在行的标号，β 是列标号。如 c 对应 13，s 对应 43 等。如果接收到密文为

43 15 13 45 42 15 32 15 43 43 11 22 15

则对应的明文即为 secure message。

另一种具有代表性的密码是凯撒密码。凯撒加密变换实际就是一个同余式

$c \equiv m+k \mod 26$

其中 m 是明文字母对应的数，c 是与明文对应的密文的数。随后，为了提高凯撒密码的安全性，人们对凯撒密码进行了改进。选取 k,b 作为两个参数，其中要求 k 与 26 互素，明文与密文的对应规则为

$c \equiv km+b \mod 26$

可以看出，k=1 就是前面提到的凯撒密码。于是这种加密变换是凯撒加密变换的推广，并且其保密程度也比凯撒密码高。

以上介绍的密码体制都属于单表置换。意思是一个明文字母所对应的密文字母是确定的。根据这个特点，利用频率分析可以对这样的密码体制进行有效的攻击。鉴于单表置换密码体制具有这样的攻击弱点，人们自然就会想办法对其进行改进，来弥补这个弱点，增加抗攻击能力。法国密码学家维吉尼亚(Vigenere)于 1586 年提出一个种多表式密码，即一个明文字母可以表示成多个密文字母。该密码曾被认为是三百年内破译不了的密码，因而这种密码在今天仍被使用着。

1881 年世界上的第一个电话保密专利出现。电报、无线电的发明使密码学成为通信领域中不可回避的研究课题。前面已经讲过，密码技术的成果首先被用于战争。1914 年第一次世界大战爆发，德俄相互宣战。在交战过程中，德军破译了俄军第一军给第二军的电文，从中得知，第一军的给养已经中断。根据这一重要情报，德军在这次战役中取得了全胜。这说明当时交战双方已开展了密码战，又说明战争刺激了密码的发展。

1920 年，美国电报电话公司的弗纳姆发明了弗纳姆密码，其原理是利用电传打字机的五单位码与密钥字母进行模 2 相加。如若信息码（明文）为 11010，密钥码为 11101，则模 2 相加得 00111 即为密文码。接收时，将密文码再与密钥码模 2 相加得信息码（明文）11010。

这种密码结构在今天看起来非常简单，但由于这种密码体制第一次使加密由原来的手工操作进入到由电子电路来实现，而且加密和解密可以直接由机器来实现，因而在近代密码学发展史上占有重要地位。随后，美国人摩波卡金在这种密码基础上设计出一种一次一密体制。该体制当通信业务很大时，所需的密钥量太

过庞大，给实际应用带来很多困难。之后，这种一次一密制又有了进一步改进，但历史事实证明，这种密码体制是不安全的，在太平洋战争中，日本使用的九七式机械密码就属于这一种。1940 年，美国陆军通信机关破译了这种密码。在中途岛海战中，日本海军大将山本五十六因密码电报被美国截获破译而被击毙在飞机上。

前面介绍了古典密码和近代密码，它们的研究还称不上是一门科学。直到1949 年香农(Shannon)发表了一篇题为“保密系统的通信理论”的著名论文，该文首先将信息论引入了密码，从而把已有数千年历史的密码学推向了科学的轨道，奠定了密码学的理论基础。该文利用数学方法对信息源、密钥源、接收和截获的密文进行了数学描述和定量分析，提出了通用的秘密钥密码体制模型。由于受历史的局限，七十年代中期以前的密码学研究基本上是秘密地进行，而且主要应用于军事和政府部门。密码学的真正蓬勃发展和广泛的应用是从七十年代中期开始的。

1977 年美国国家标准局颁布了数据加密标准 DES 用于非国家保密机关。该系统完全公开了加密、解密算法。此举突破了早期密码学的信息保密的单一目的，使得密码学得以在商业等民用领域的广泛应用。此外，在密码学发展的进程中的另一件值得注意的事件是，在 1976 年，美国密码学家迪菲(Diffie)和赫尔曼(Hellman)在一篇题为“密码学的新方向”一文中提出了一个崭新的思想[8]，不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。1978 年，由美国麻省理工学院的里维斯特(Rivest)，沙米尔(Shamir)和阿德曼(Adleman)提出了 RSA 公钥密码体制[7]，它是第一个成熟的、迄今为止理论上最成功的公钥密码体制。它的安全性是基于数论中的大整数因子分解。该问题是数论中的一个困难问题，至今没有有效的算法，这使得该体制具有较高的保密性。

自从 DES 算法颁布以来，世界各地相继出现了多种密码算法。但是它们都可以分为私钥密码体制（比如 DES 密码）和公钥密码（比如公开密钥密码）。有关对称密钥的密码算法有：DES 算法，LUCIFER 算法，Madryga 算法，NewDES 算法，FEAL-N 算法，REDOC 算法， LOKI 算法，KHUFU 算法， KHAFRE 算法，RC2 及 RC4 算法，IDEA 算法， MMB 算法，CA-1.1 算法，SKIPJACK 算法，Karn 算法以及 MDC 算法等。有关非对称密钥的密码算法有：RSA 算法，DSS 算法，背包体制，

POHLIG-Hellman 算法，Rabin 算法，ElGamal 算法，SCHNORR 算法，ESIGN 算法，McEliece 算法，OKAMOTO 算法，还可以在有限域上的椭圆曲线上建立 RSA，ElGamal 算法等。

此外，除了以上密码体制外，近些年来国内外都在研究的多种新型密码，如量子密码(Quantum Cryptography)、热流密码（Heat Flow Cryptography)、混沌密码（Chaos Cryptography）和图视密码(Visual Cryptography)。这些都还处于预研阶段，特别是其安全性和可靠性需要研究，离实用尚有距离。

§1.3 我国信息安全及其技术研究迫在眉睫

信息安全保障能力是 21 世纪综合国力和生存能力的重要组成部分，关系到信息革命的成败。面对信息超级大国的垄断和未来信息战的威胁，我们必须发展独立的信息安全系统。

§1.3.1 重视我国信息安全及其技术的战略意义

正在经历信息化高速发展的我国，同样面临信息发达国家所曾经发生或正在发生的种种问题。黑客入侵、计算机犯罪、计算机病毒泛滥、金融部门业务人员违法等事件正在呈现高速增长的趋势。

同时，信息网络的国际化、社会化、开放化、个人化，使国家的“信息边疆”不断延伸。信息系统的许多应用业务要与国际接轨，诸如电信、电子商务、电子支付等信息空间跨越国境。国际上围绕信息的获取、使用和控制的斗争愈演愈烈。“控制信息权”成为综合国力和竞争能力的重要体现。特别是我国信息基础设施的主要设备和技术大多是从国外引进，这正是影响国家全局和长远利益的重大关键问题。例如目前美国英特尔公司在奔腾 III 处理器内部设置序列号功能，宣称是为了更加提高保密性能，从而提高电子商务的安全性。实际上对于在号称世界上保密措施最严密的美国国防部的电脑上都能任意浏览的网上“黑客”，正好能够通过唯一识别 CPU 个体的序列号，主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先设定来收集敏感信息或进行定向破坏。因此，如果类似引进与自主的问题及网络信息安全的相关问题能够处理得好，不但能保证信息系统的高效运转，而且将建立起对抗霸权、抵御信息侵略的屏障。如果上述问题解决不好，必将全方位危及我国的经济、政治、军事、文化、社会生活的各个方面，置国家和人民于高风险的经济金融和信息战的威胁之中。

信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组

成部分，是世纪之交世界各国奋力攀登的制高点。特别是面对某些妄图以信息能力称霸的超级大国的信息战的威胁，我们必须高度重视维护国家的主权独立和安全，高度重视在信息安全的基础上发展我国的经济竞争实力。

§1.3.2 我国信息安全技术发展的概况和当前亟需解决的问题

1. 我国信息安全技术发展的概况

我国的信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。安全体系的构建和评估，通过学习、吸收、消化的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制出了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是，这些产品安全技术的完善性、规范化实用性还存在许多不足，特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面存在很大差距，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络信息安全研究起步晚，投入少，研究力量分散，与技术先进国家有差距，特别是在系统安全和安全协议方面的工作与国外差距更大，在我国研究和建立创新性安全理论和系列算法，仍是一项艰巨的任务。然而我国的网络信息安全研究毕竟已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好。我国建国后历来具有保密工作的优良传统，我国也拥有在代数编码方面具有特点和实力的一批著名数学专家。因此，在密码学理论研究领域，我国拥有具有自己特点的研究基础和理论成果，其中许多成果达到国际先进的水平。青年密码学家来学嘉与美国密码学家 Massey 一起提出引起国际密码学界重视与好评的分组密码算法 IDEA 就是一个证明。但是如何把我们拥有的理论基础用于我国的信息安全需求，正经历着一个从面向政府应用到关注社会应用的认识、组织、协调、推动的过程。中国科学院信息安全国家重点实验室正在大力深化密码理论研究，密码算法研究和算法集成化研究。实验室和企业合作，完成了物理噪声源集成芯片的研制投产，动态口令保护卡（DID）的投产，开展了网络银行的应用。山东大学网络信息安全研究所推出了利用 RSA 公开密钥密码算法认证身份的应用系统。我国首套拥有自主知识产权的电子商务安全认证系统，已由湖南省邮电管理局和信息产业部电信研究院联合开发成功，1999 年 8 月 2 日通过了国家密码管理委员会和信息产业部组织的技术鉴定。

在计算机系统安全的许多方面，我国也开展了相应的研究：中软公司开发了具有我国自主知识产权的达到 B2 安全级 COSLXV2.1 的安全操作系统；华中理工大学研制了多级安全保密管理信息系统模拟原型，并与天融信公司推出安全数

据库系统；天融信公司推出了自主品牌的系列防火墙产品；中国科学院信息安全技术工程研究中心研制了防火墙、内联网安全集成系统、智能卡安全集成系统；原电子部 30 所和原邮电部数据所都推出了系列化的网络保密产品。清华大学、北京大学等一些单位开发成功了安全路由器、保密网关等安全产品。

2. 当前亟需解决的问题

我们必须清醒地认识到，我们的工作尚处于起步阶段。我们的研究队伍力量分散，研究开发的经费投入不足，研究项目缺乏宏观规划的有力导向，防护机制多处于在系统外围补充，产品规范不够，适应多平台、多协议的能力有限，产业运作机制尚待理顺，产品还没有形成集成、配套、规模的能力。

信息安全领域是一个综合、交叉的学科领域，它需要综合利用数学、物理、生化信息技术和计算机技术的诸多学科的长期知识积累和最新发展成果，需要提出系统的（而不是个别的）、完整的（而不是零碎的）、协同的（而不是孤立的）解决信息安全的方案。同时，它的研究和发展又将刺激、推动和促进相关学科的研究和发展。

沈昌祥院士认为：我国当前应从安全体系结构、安全协议、现代密码理论、信息分析和监控以及信息安全系统五个方面开展研究，各部分都提供应用的功能，相互间协同工作形成有机整体。在安全体系结构研究方面，要创建科学的能综合满足需要的安全模型。

信息安全问题本身就是个错综复杂的难题。比如商业机密的保密问题，牵扯面比较广，任何国家在信息的安全和机密保密方面，都有自己的要求。我们国家在信息安全保密体制上究竟谁来管理？怎么管理？有没有一套有序的管理办法？一系列相关问题接踵而来。

总之，我们要有我们自己的密码算法，来抵制国外加密产品的限制以及威胁。

第二章　加密解密算法的特点及技术关键

在这一章节中，首先我来看几个重要的密码体制。通过下面的介绍，我们可以看出它们各自的优缺点，从而揭示出加密与解密算法的特点与技术关键。

§2.1　传统的密码体制

传统的密码体制是相对于近代的密码体制而言的。在早期的常规密钥密码体制中，典型的有代替密码，其原理可以用一个例子来说明：

将字母 a，b，c，d，…，w，x，y，z 的自然顺序保持不变，但使之与 D，E，F，G，…，Z，A，B，C 分别对应（即 c=m+3）。若明文为 student，则对应的密文为 VWXGHQW（此时密钥为 3）。

前面提到过的棋盘密码，还有凯撒密码都属于传统的密码体制。由于这两种密码体制的安全很底，人们对它们进行了相应的改进，但总的来说都没有跳出单表置换的圈圈。即一个明文字母对应的密文字母是确定的。根据这个特点，利用频率分析可以对这样的密码体制进行有效的攻击。破译者通过对密文中各字母出现频率的分析，结合自然语言的字母频率特征，就可以将该密码体制破译。

后来，法国密码学家维吉尼亚于 1586 年提出一个种多表式密码。其原理是这样的：给出密钥 K=k[1]k[2]…k[n]，若明文为 M=m[1]m[2]…m[n]，则对应的密文为 C=c[1]c[2]…c[n]。其中 C[i]=(m[i]+k[i]) mod 26。

从中可以看出，当 K 为一个字母时，就是凯撒密码。而且容易看出，K 越长，保密程度就越高。显然这样的密码体制比单表置换密码体制具有更强的抗攻击能力，而且其加密、解密均可用所谓的维吉尼亚方阵来进行，从而在操作上简单易行。该密码可用所谓的维吉尼亚方阵来进行，从而在操作上简单易行。

§2.2　对称密钥密码技术

对称（传统）密码体制是从传统的简单换位，代替密码发展而来的，自 1977 年美国颁布 DES 密码算法作为美国数据加密标准以来，对称密钥密码体制得到了迅猛地发展，在世界各国得到了关注和使用。对称密钥密码体制从加密模式上可分为序列密码和分组密码两大类。

§2.1.1 序列密码

序列密码一直是作为军事和外交场合使用的主要密码技术之一，它的主要原理是，通过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流，（逐比特加密）得到密文序列。所以，序列密码算法的安全强度完全决定于它所产生的伪随机序列的好坏。衡量一个伪随机序列好坏的标准有多种，比较通用的有著名的 Golomb 的三个随机性公设。

密钥流是 0——1 序列，例如 00110111。这序列前两个数字是 00，称为 0 的 2 游程；接着是 11，是 1 的 2 游程；继之是 0 的 1 游程和 1 的 3 游程。

假定 $s_1s_2s_3\cdots$是 0——1 序列，用$\{s_i\}$表示。r 是对于所有的正整数 m，满足 $s_{m+r}=s_m$ 的最小正整数。若存在这样的 r，则称序列$\{s_i\}$为以 r 为周期。若有下列两个子序列：$s_1,s_2,\cdots,s_r;s_{1+\tau},s_{2+\tau},\cdots,s_{r+\tau}$。从前一序列后移 τ 位便得到后一序列。若 $s_i=s_{i+\tau}$，则称对应于第 i 位是相同的。这两个子序列中相同的位的数目用 n_τ 表示，不同的位的数目用 $d_\tau=r-n_\tau$ 表示。定义

$$R(\tau)=\frac{n_r-d_r}{r}$$

为自相关数。

τ =0 时，显然有 $n_\tau=r, d_\tau=0, R(0)=1$

τ ≠0，R(τ)为异相自相关函数。

则 Golomb 的随机性公设可以表述如下：

（1） 若 r 是奇数，则 0——1$\{s_i\}$的一个周期内 0 的个数比 1 的个数多一个或少一个；若 r 是偶数，则 0 的个数与 1 的个数相等。

（2） 在长度为 r 的周期内，1 游程的个数为游程总数的 1/2，2 游程的个数占游程总数 $1/2^2$，…，c 游程的个数占游程总数的 $1/2^c$。而且任意长度 0 的游程个数和 1 的游程个数相等。

（3） 异相自相关函数是一个常数。

衡量一个伪随机序列好坏的标准除了 Golomb 公设外，还有序列 Rueppel 的线性复杂度随机走动条件，线性逼近以及产生该序列的布尔函数满足的相关免疫条件等。

产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列， 典型方法有：

反馈移位寄存器：采用 n 阶非线性反馈函数产生大周期的非线性序列，例如 M 序列，具有较好的密码学性质，只是反馈函数的选择有难度，如何产生全部的 M 序列至今仍是世界难题。

利用线性移位寄存器序列加非线性前馈函数，产生前馈序列，如何控制序列相位及非线性前馈函数也是相当困难的问题，Bent 序列就是其中一类好的序列。

钟控序列，利用一个寄存器序列作为时钟控制另一寄存器序列（或自己控制自己）来产生钟控序列，这种序列具有大的线性复杂度。

组合网络及其他序列，通过组合运用以上方法，产生更复杂的网络，来实现复杂的序列，这种序列的密码性质理论上比较难控制。

利用混沌理论，细胞自动机等方法产生的伪随机序列。

对序列密码攻击的主要手段有代数方法和概率统计方法，两者结合可以达到较好的效果。目前要求寄存器的阶数大于 100 阶，才能保证必要的安全。

序列密码的优点是错误扩展小，速度快，利于同步，安全程度高。

§2.1.2 分组密码

分组密码的工作方式是将明文分成固定长度的组（块），如 64 比特一组，用同一密钥和算法对每一块加密，输出也是固定长度的密文。比较著名的分组密码算法是 IDEA(International Data Encryption Algorithm)[21]和 DES。例如 DES(Data Encryption Standard)密码算法的输入为 64 比特明文，密钥长度 56 比特，密文长度 64 比特。

设计分组密码算法的核心技术是：在复杂函数可以通过简单函数迭代若干圈得到的原则下，利用简单函数及对合等运算，充分利用非线性运算。以 DES 算法为例，它采用美国国家安全局精心设计的 8 个 S-Box 和 P-置换，经过 16 圈迭代，最终产生 64 比特密文，每圈迭代使用的 48 比特子密钥是由原始的 56 比特产生的。

DES 算法加密时把明文以 64bit 为单位分成块，而后用密钥把每一块明文转化成同样 64bit 的密文块。DES 可提供 72，000，000，000，000，000 个密钥，用每微秒可进行一次 DES 加密的机器来破译密码需两千年。采用 DES 的一个著名的网络安全系统是 Kerberos，由 MIT 开发，是网络通信中身份认证的工业上的事实标准。

DES（或其他分组密码）算法的使用方式有 4 种，电子密本（ECB），密码分组链接(CBC)，输出反馈(OFB)和密文反馈(CFB)。

DES 的密钥存在弱密钥，半弱密钥和互补密钥，选择密钥时要注意这些问题。DES 受到的最大攻击是它的密钥长度仅有 56 比特，强力攻击的代价低于 1000 万美元，1990 年以色列学者 S.Biham 和 A.Shamir 提出了差分分析攻击的方法[42][43][44]，采用选择明文 247 攻击，最终找到可能的密钥。日本学者 M.Matsui 提出的线性分析方法[45][46][47]，利用 243 个已知明文，成功地破译了 16 圈 DES 算法，到目前为止，这是最有效的破译方法。

基于以上弱点，人们将 DES 算法作了多种变形，三重 DES 方式，独立子密钥方法，可变的 S-Box 及其使用次序以及推广的 GDES 等。这些改变有些是增

强了密码算法的安全性，有些作用不大，有些还削弱了 DES 的安全性。

另外一个影响比较大的时 IDEA 算法（国际数据加密算法），它是由中国学者来学嘉(Xuejia Lai)与著名密码学家 James Massay 于 1990 年联合提出的[48]，在 Biham 和 Shamir 演示了差分密码分析后，为了抗此攻击，增加了密码算法的强度，最后于 1992 年最后完成[21]。它的明文与密文块都是 64 比特，但密钥长 128 比特。加密与解密也相同，只是密钥各异。IDEA 加密算法可以描述如下：

64 比特的数据块分成 4 个子块，每一子块 16 比特，令这 4 个子块为 X_1，X_2，X_3 和 X_4，作为迭代第 1 轮的输入，全部共 8 轮迭代。每轮迭代都是 4 个彼此间以及 16 比特的子密钥进行异或运算，mod 2^{16} 做加法运算，mod $(2^{16}+1)$做乘法运算。任何一轮迭代的第 3 和第 4 子块互换。子密钥的产生过程是，子密钥块每轮 6 个最后输出变换 4 个，共 52 个。首先将 128 比特的密钥分成 8 个子密钥，每个子密钥 16 比特。这 8 个子密钥正好是第 1 轮的 6 个及第 2 轮的前两个。再将密钥左旋转 25 比特，再将它分成 8 个子密钥。前 4 个是第 2 轮的子密钥，后 4 个是第 3 轮的子密钥。将密钥再左旋转 25 比特，产生后 8 个子密钥。依次类推，直到算法结束。 IDEA 有比 DES 更强的抗攻击性，直到目前为止还没有有关 IDEA 被破译的报道。

自从 DES 算法颁布以来，世界各地相继出现了多种密码算法。之所以出现这些算法，有政治原因和技术原因。各国在商用方面都需要自己设计的密码算法，不能依靠外国的算法。又因为 DES 算法的弱点和软件实现中面临的位操作及大量的置换，设计寿命仅有 5 年，所以必须设计出更高强度的密码算法，以代替 DES。例如 TH 加密算法，它是由我国清华大学设计的，它保持了 DES 的优点，但抗攻击能力确大大提高了。除此之外还有：

LUCIFER 算法[9][10][11][12]，Madryga 算法，NewDES 算法[13][49]，FEAL-N 算法[14][15][50]，REDOC 算法[16][17][51]，LOKI 算法[18]，KHUFU 算法[19][20]，KHAFRE 算法[19][20]，RC2 及 RC4 算法，IDEA 算法，MMB 算法[22][23]，CA-1.1 算法[24][25][26]，SKIPJACK 算法[27]，Karn 算法以及 MDC 算法[28]等。其中多数算法为专利算法。

以上这些算法有些已经遭到了破译，有些安全强度不如 DES，有些强度高于 DES，有些强度不明，还有待于进一步分析。其中安全强度高于 DES 算法的如 RC2 及 RC4 算法，IDEA 算法， SKIPJACK 算法等。

清华大学研制开发了 TUC 系列密码算法，已申请国家专利。

总之，因为对称密钥密码系统具有加解密速度快，安全强度高等优点，在军事，外交以及商业应用中使用越来越普遍。

§2.3 非对称密钥密码技术

随着计算机网络的发展，传统的对称密码体制远远不能满足实际的需要。因为在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。1976 年美国密码学家 Diffie 和 Hellman 在一篇题为“密码学的新方向”[8]一文中提出了公开密钥密码体制（也称公钥密码体制）的思想，这不同于传统的对称密钥密码体制，它要求密钥成对出现，一个为加密密钥(e)，另一个为解密密钥(d)，且不可能从其中一个推导出另一个。自 1976 年以来，已经提出了多种公开密钥密码算法，其中许多是不安全的， 一些认为是安全的算法又有许多是不实用的，它们要么是密钥太大，要么密文扩展十分严重。多数密码算法的安全基础是基于一些数学难题， 这些难题专家们认为在短期内不可能得到解决。因为一些问题(如因子分解问题)至今已有数千年的历史了。

公钥加密算法也称非对称密钥算法，用两对密钥：一个公钥和一个专用密钥。用户要保障专用密钥的安全；公共密钥则可以发布出去。公钥与专用密钥是有紧密关系的，用公共密钥加密的信息只能用专用密钥解密，反之亦然。由于公钥算法不需要联机密钥服务器，密钥分配协议简单，所以极大简化了密钥管理。除加密功能外，公钥系统还可以提供数字签名。在 Diffie 和 Hellman 思想的刺激下，各种公钥密码体制开始涌现。公共密钥加密算法主要有:RSA(Rivest、Shamir、Adleman)[7][29][30][31]， Fertezza，ElGamal 算法等，其中以 RSA 算法的影响为最大，它是第一个成熟的、迄今为止理论上最成功的公钥密码体制。

DSS(Digital Signature Standard)、Diffie-Hellman 公钥加密方法支持彼此互不相识的两个实体间的安全通信，如信用卡交易，但缺乏对资源访问的授权能力(存取控制)。公钥加密算法中使用最广的是 RSA。RSA 使用两个密钥，一个公共密钥，一个专用密钥。如用其中一个加密，则可用另一个解密，密钥长度从 40 到 2048bit 可变，加密时也把明文分成块，块的大小可变，但不能超过密钥的长度，RSA 算法把每一块明文转化为与密钥长度相同的密文块。密钥越长，加密效果越好，但加密解密的开销也大，所以要在安全与性能之间折衷考虑，一般 64 位是较合适的。

公用密钥的优点就在于，也许你并不认识某一实体，但只要你的服务器认为该实体的 CA（证书授权）是可靠的，就可以进行安全通信，而这正是 Web 商务这样的业务所要求的。例如信用卡购物。服务方对自己的资源可根据客户 CA 的发行机构的可靠程度来授权。目前国内外尚没有可以被广泛信赖的 CA。美国 Netscape 公司的产品支持公用密钥，但把 Netscape 公司作为 CA。由外国公司充当 CA 在我国是一件不可能的事情。

公共密钥方案较保密密钥方案处理速度慢，因此，通常把公共密钥与专用

密钥技术结合起来实现最佳性能。即用公共密钥技术在通信双方之间传送专用密钥，而用专用密钥来对实际传输的数据加密解密。另外，公钥加密也用来对专用密钥进行加密。

在这些安全实用的算法中，有些适用于密钥分配，有些可作为加密算法，还有些仅用于数字签名。多数算法需要大数运算，所以实现速度很慢 ，不能用于快的数据加密。

在这种体制中，PK 是公开信息，用作加密密钥，而 SK 需要由用户自己保密，用作解密密钥。加密算法 E 和解密算法 D 也都是公开的。虽然 SK 与 PK 是成对出现，但却不能根据 PK 计算出 SK。公开密钥算法的特点如下：

1、用加密密钥 PK 对明文 X 加密后，再用解密密钥 SK 解密，即可恢复出明文，或写为：D(SK,E(PK,X))=X

2、加密密钥不能用来解密，即 D(PK,E(PK,X))≠X

3、在计算机上可以容易地产生成对的 PK 和 SK。

4、从已知的 PK 实际上不可能推导出 SK。

5、加密和解密的运算可以对调，即：E(PK,D(SK,X))=X

在公开密钥密码体制中，RSA 体制已被 ISO/TC97 的数据加密技术分委员会 SC20 推荐为公开密钥数据加密标准。

除了上面提到的一些公钥密码体制之外还有好多的公钥密码体制。人们一直努力在其他困难问题上建立公开密钥密码体制，不至于一旦一些数学难题被解决以后，没有可用的密码算法，所以出现了大量的公开密钥密码算法，包括：背包体制，Pohlig-Hellman 算法[32][33]，Rabin 算法[34]，ElGamal 算法[35][36]，SCHNORR 算法，ESIGN 算法，McEliece 算法[37]，OKAMOTO 算法，还可以在有限域上的椭圆曲线上建立 RSA，ElGamal 算法等。

我们认为 RSA 算法是目前最好的密码算法，它不仅可以作为加密算法使用，而且可以用作数字签名和密钥分配与管理，而 DSS 只适合作签名，且安全强度和速度都不如 RSA，椭圆曲线上的公开密钥密码系统安全强度依赖于曲线的选择和体制，相信它会有更高的安全强度。主要可以从以下两个方面来考虑：

（1） 它在传输过程中用到了大数因子分解，这也是 RSA 安全性的主要的体现。

（2） 它还在映射过程中加进了一定难度，把明文按照一定规则映射到曲线上，在不知道映射规则的情况下是很难得到相应的明文的。这就给攻击带来了更大的难度，从而安全性得到了提高。

目前 200 比特长的椭圆曲线密码体制已经有相当高的安全强度。

在几乎所有的实用公开密钥密码系统中，都涉及到大数运算和素数选择 ，模幂运算采用反复平方取模算法，素数测试一般采用 Rabin-Miller 算 法，还有

其他素性测试算法用来选择大素数，如 Solovag-Strassen 测试法，Lehmann 测试法等。

虽然说，在网络上全都用公开密钥密码体制来传送机密信息是没有必要的，也是不现实的。但是公钥密码系统在网络传输中的应用是不容忽视的，而且对它的发展提出了许多新的要求。

§2.4 公钥算法分析

我们主要的目的是要设计一个安全性较高，而且计算速度又快的算法来满足现实的需求。以下，我们将通过介绍一些典型的公开密钥密码算法来揭开算法设计的特点及关键。

§2.4.1 RSA 公开密钥密码算法

公开密钥： n，e；n=pq，(p，q 分别为两个互异的大素数，p，q 必须保密)e
与(p-1)(q-1) 互素

秘密密钥：d；de=1 (mod (p-1)(q-1))

加密：$c= m^e \pmod n$， 其中 m 为明文，c 为密文

解密： $m= c^d \pmod n$

一般要求 p，q 为安全素数，n 的长度大于 512bit ，这主要是因为 RSA 算法的安全性依赖于因子分解大数问题。

较之于对称密码算法，公钥算法的速度要慢的多了。硬件实现时，RSA 比 DES 慢大约 1000 倍。软件实现时，DES 大约比 RSA 快 100 倍。下表给出了 RSA 软件速度的实例[52]。

具有 8-位公开密钥的 RSA 对于不同长度模数的加密速度（在 SPARC II 中）

	512 位	768 位	1024 位
加密	0.03 秒	0.05 秒	0.08 秒
解密	0.16 秒	0.48 秒	0.93 秒
签名	0.16 秒	0.52 秒	0.97 秒
验证	0.02 秒	0.07 秒	0.08 秒

我们前面的讨论中已经提到过，RSA 的安全性完全依赖于分解大数的难度。但是我们注意到，如果有另外的方法让密码分析者推算出 d，它也可作为分解大数的一种新的方法。这就将值得我们担忧。密码分析者也可通过猜测(p-1)(q-1)的值来攻击 RSA，同时，也可以尝试每一种可能的 d。但以上的种种方法实际上并没有比分解 n 来的快。此外，还有些专门针对 RSA 的算法攻击，譬如对 RSA

的选择密文攻击，对 RSA 的公共模数攻击，对 RSA 的低加密指数攻击等[53]。有一些成功地实现了攻击。这是我们不愿意看到的。

§2.4.2 Diffie-Hellman 密钥交换协议

设 p 为 512 比特以上大素数，g<p，p，g 公开，A 与 B 通过对称密钥密码体制进行保密通信，以下是 A，B 通过公开密钥算法协商通信密钥的协议。

(1) A 随机选择 x<p，发送 $g^x \pmod p$ 给 B;

(2) B 随机选择 y<p，发送 $g^y \pmod p$ 给 A;

(3) A 通过自己的 x 秘密计算 $(g^y)^x \pmod p = g^{xy} \pmod p$;

(4) B 通过自己的 y 秘密计算 $(g^x)^y \pmod p = g^{xy} \pmod p$;

A 与 B 拥有相同的数据 $g^{xy} \pmod p$ 作为共同的秘密密钥进行保密通信。g 和 n 的选择对系统的安全性影响很大。最重要的是 n 应该很大：因为系统的安全性取决于与 n 同样长度的数的因子分解的难度。而且要进行算法的攻击，就要涉及到离散对数的计算。因而，算法安全性同样依赖于有限域上的离散对数问题。

§2.4.3 背包公钥密码系统

所谓背包问题是：已知一长度为 b 的背包，及长度分别为 a_1，a_2，…，a_n 的 n 个物品。假定这些物品的半径和背包相同，若从这 n 个物品中选出若干个正好装满这个背包。现在反过来问，究竟是哪些物品？这个问题导致求 x_i=0，或 1，i=1，2，…，n，使满足

$$\sum_{i=1}^{n} a_i x_i = b$$

其中 a_1，a_2，…，a_n 和 b 都是整数。

背包密码系统是选取一组正整数 $a_1, a_2, \cdots, a_n$ 作为公钥予以公布，$m=m_1m_2\cdots m_n$ 是 n 位 0，1 明文符号串。利用公钥加密如下：

$$c = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n$$

从密文 c 求明文 m_1，m_2，…，m_n 等价于解背包问题。

背包问题是著名的 NP 完备类困难问题，至今还没有好的求解方法，只能对所有的可能进行穷尽搜索。从而，我们也可以看出，低密度（n 过小）的背包公钥系统的安全性不是很高。

§2.4.4 椭圆曲线上的密码系统

椭圆曲线密码体制是一种基于代数曲线的公钥密码体制。椭圆曲线已经研究了很多年了，关于这方面有大量的文献。1985 年，Neal Kobilitz 和 V.S. Milller 分别提出将它用于公开密钥密码体制[55][56]。他们没有发明有限域上使用椭圆曲

线的新的密码算法，但他们用椭圆曲线实现了已存在的公开密钥密码算法，如Diffie-Hellman 算法。椭圆曲线的吸引人之处在于提供了“元素”和“组合规则”来组成群的构造方式。用这些来构造密码算法具有完全相似的特性，但它们并没有减少密码分析的分析量。此外，以其良好的安全性，曲线选取范围广，在同等长度的密钥下具有比 RSA 体制更快的加密，解密速度及更高的密码强度而倍受青睐。有关椭圆曲线上的公钥密码系统有，Diffie-Hellman 公钥密码系统，Massey-Omura 公钥密码系统，ElGamal 公钥密码系统等，下面仅以 Massey-Omura 公钥密码系统为例作以介绍。

已知有限域 GF(q)，用户 A 选一加密密钥 e_A，$0 \le e_A \le N$，满足（e_A，q-1）=1，通过欧几里德算法求得 d_A 满足：

$e_A d_A \equiv 1 \bmod (q-1)$

根据类似的理由，若用户 B 有 $e_B d_B \equiv 1 \bmod (q-1)$而且（$e_B$，q-1）=1，若 A 欲向 B 发送信息 m，则 A 送去 m^{e_A}，B 无法获得 m，因他既不知道 e_A，也不知道 d_A，B 退还 A 以 $m^{e_A e_B}$。A 收到 $m^{e_A e_B}=c$ 后，作 $c^{d_A}=m^{e_B}$并送给 B，B 对此结果做 $m^{e_B d_B} = m \bmod(q)$，从而获得明文 m。

Massey-Omura 密码体系在椭圆曲线上的实现过程如下：

假定 m 嵌入到 E 上的 P_m 点。设 E 上的点数 N 为已知的大素数，每一个用户随机选择一数 e，1<e<N，（e,N）=1，d 是 e 的逆，即 ed=1(mod N)。假如 A 要送 B 信息 m。

（1） A 首先送去 $e_A P_m$，这里 e_A 表示属于用户 A 的 e；

（2） B 退还给 A 以 $e_B e_A P_m$；

（3） A 再送去 $d_A e_B e_A P_m = e_B P_m$；

（4） B 乘以 d_B 得到 $d_B e_B P_m = P_m$。

通过分析上面的算法，我们可以知道，椭圆曲线密码系统之所以比 RSA 有更好的安全性和更快计算速度，是因为：

（1） 在信息发送之前，我们把信息 m 嵌入到了椭圆曲线上。这样即使攻击者有效地解得了发送的信息，在不知道映射规则的前提下是很难确切地取得明文的。而往往这个映射规则的复杂度并不比大素数分解来的容易，同时也是不能通过一般的离散对数来进行破译。

（2） 在发送的过程仍然保有大素数分解的难度。而且不涉及到指数运算，从而提高了算法的计算速度。

§2.5 与公钥有关的数学理论基础

从前面的算法中可以看到，大数分解定理在公钥密码体系中起到了相当重要的作用。其他一些公钥密码体系的安全性也是基于一定的数学理论基础的。下面就有关的数学理论加以说明（其中的大部分证明可以见[1]）。

§2.5.1 欧拉定理

若整数 a 和 m 互素，则

$$a^{\phi(m)} = 1 \bmod(\quad m\ )$$

其中 Φ(m)是比 m 小但与 m 互素的正整数个数。

（证明略）

§2.5.2 中国剩余定理

设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，则同余方程组

$$x \equiv b_i (\bmod\ \ m_i) \quad i=1,\ 2,\ \cdots,\ k$$

模 $m_1 m_2 \cdots m_k$ 有唯一解。（证明略）

§2.5.3 威尔逊定理

n 是素数的充要条件是

$$(n-1)! \equiv -1 \pmod n$$

（证明略）

§2.5.4 平方剩余定理

若 p 是奇素数，则整数 1，2，…，p-1 中正好有(p-1)/2 个是模 p 的平方剩余，其余的(p-1)/2 个是非平方剩余。

（证明略）

除了以上所列举的定理之外，还有许多其他的数学理论来支持加密算法。下面将简述一些典型的算法。

§2.5.5 分解的欧几里德算法

S1.求 q 及 r，使 $n_1 = qn_2 + r$

S2.若 r=0，则作

{ g←n_2，输出 g，结束}

否则转 S3

S3. $n_1 \leftarrow n_2$, $n_2 \leftarrow r$，输 S1

§2.5.6 mod m 的逆元素算法

S1. $n_1 \leftarrow m$, $n_2 \leftarrow u$, $b_1 \leftarrow 0$, $b_2 \leftarrow 1$

S2.求 q,r，使 $n_1=qn_2+r$

S3.若 $r \neq 0$，则作

{ $n_1 \leftarrow n_2$, $n_2 \leftarrow r$，$t \leftarrow b_2$, $b_2 \leftarrow b_1-q\ b_2$, $b_1 \leftarrow t$ 转 S2

S4.若 $n_2 \neq 1$ 则给出不存在的信息，然后结束

S5.若 $b_2 < 0$ 则作

$b_2 \leftarrow b_2+m$, b_2 是逆而结束

§2.5.7 素数测试

S1.从{1，2，…，n}中随机且均匀地产生一数 a

S2.计算 gcd{a,n}

S3. 若 gcd{a,n}≠1，则 n 非素数

S4.计算(a/n)及 $a^{(n-1)/2} \bmod n$

S5.若$(a/n) \equiv a^{(n-1)/2} \bmod n$，则 n 可能是素数，否则 n 是合数

其中，gcd{a,n}是指两数的最大公因式，$(a/n) \equiv a^{(n-1)/2}$ 是 Legendre 符号

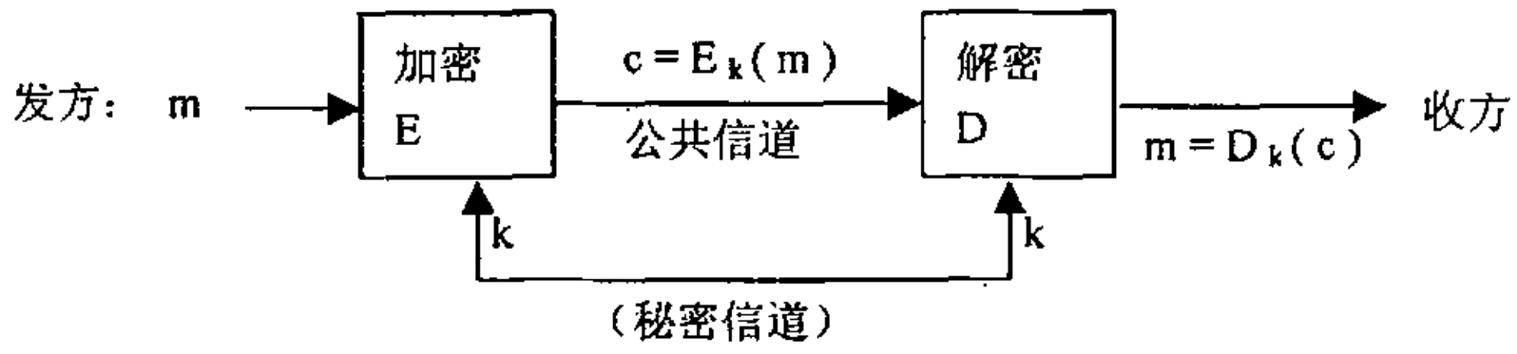
§2.5.8 其它算法

此外还有很多算法，如 Fermat 因数分解法，连分式因数分解法，Pollard 整数分解法，大数模幂乘快速算法，离散对数算法等等。其中离散对数算法有 Pohlig-Hellman 求法和 Shank 法等，它在 RSA 加密算法中起到很大的作用。上面所提到的各种算法的具体实现及算法复杂度分析，在有关密码学的书中都有详细的综述，在这儿就不再赘述了。

§2.6 密码技术的特点与关键

密码技术是保护信息安全的主要手段之一。密码技术自古有之，到目前为止，已经从外交和军事领域走向公开。它是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，不仅具有保证信息机密性的信息加密功能， 而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确证性，防止信息被篡改、伪造和假冒。

从前面的讨论中，我门可以看到密码的机制，如图：



用数学语言来说，加密，解密本质上就是要找一个函数对，即函数和反函数。而其中密钥则是函数中一个参数。加密的过程是，我们可以在发送方取得密钥(也即是参数）和明文（函数的原象），通过函数变换得到密文（函数的象）。我们将函数的象在公共信道上进行传送。解密的过程是，接受方通过秘密信道取得参数和函数象，通过函数的逆变换，我们可以重新得到函数的原象，从而实现加密和解密的过程。一个加密与解密算法的安全性的主要关键是在未知密钥的情况下，只知道密文应该是很难解得原文的。因而，加密算法不能太简单。同时，在选取密钥的时候，密钥的长度直接关系到算法的计算复杂度，在能够满足安全性要求的情况下，密钥的长度还不能过长。

为了保证系统有很好的安全性能，选择一个健壮的加密算法是至关重要的。此外，安全系统的结构和算法的实现以及通信协议也会影响到系统的安全性。

为了防止密码分析，应采取以下机制：

健壮的加密算法。一个好的加密算法往往只有用穷举法才能得到密钥，所以只要密钥足够长就会很安全。建议至少为 64 位。

动态会话密钥。每次会话的密钥不同，即使一次会话通信被破解，不会因本次密钥被破解而殃及其它通信。

保护关键密钥(Key Encryption Key，KEK)，定期变换加密会话密钥的密钥。因为这些密钥是用来加密会话密钥的，泄漏会引起灾难性后果。

密码学包括密码编码学和密码分析学，密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容，密码编码技术和密码分析技术是相互依存，互相支持，密不可分的两个方面。

从密码体制方面而言，密码体制有对称密钥密码技术和非对称密钥密码技术，对称密钥密码技术要求加密解密双方拥有相同的密钥；而非对称密钥密码技术是加密解密双方拥有不相同的密钥，在不知道陷门信息的情况下，加密密钥和解密密钥在计算上是不能相互算出的。

密码学不仅仅是编码与破译的学问，而且包括安全管理、安全协议设计、秘密分存、散列函数等内容。到目前为止，密码学中出现了大量的新技术和新概念，例如零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术、混沌密码等。

在下面的章节中，将通过对椭圆函数的研究，来构造一种有效的加密算法。

第三章 基于椭圆函数的加密解密算法设计

§3.1 基本概念

定义 1　命 M 是一个数集，如果其中任意二数的和差都在这集中，这集称为数模。

例1　所有的自然数成一模。同样对任意的 $\omega \in M$

$n\omega$，n=0,±1, ±2,…也成一模

例2　所有的复数也成一模。

例3　所有形如

a+bi, a,b=0,±1, ±2,…

的数也成一模。

定义 2　如果模 M 中有 n 个数 $\omega_1, \omega_2, \cdots, \omega_n$，使数模中任一数 ω 可以唯一地表示成为

$P_1\omega_1+P_2\omega_2+\cdots+P_n\omega_n$，（P 是整数）

形式，则 ω_1，ω_2，…，ω_n 称为M的底，n 称为数模秩数。

例 1 的底是 $\dot{\omega}$，其秩是一。

例 3 的底是 1，i，其秩是二。

如果模M有另一底 $m=n$，ω_2'，…，ω_m'，则由定义可知

$$\omega_i = \sum_{j=1}^{m} a_{ij}\omega'_j, \omega'_j = \sum_{k=1}^{n} b_{jk}\omega_k$$

所以

$$\omega_i = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{ij}b_{jk}\omega_k$$

由定义可知表示是唯一的。因此

$$\sum_{j=1}^{m}\sum_{k=1}^{n} a_{ij}b_{jk} = \begin{cases} 1, 若\ i=k \\ 0, 若\ i\neq k \end{cases}$$

因此（a_{ij}），（b_{jk}）是二个可求逆的矩阵，且 $m=n$。

定理 1　如果模M还有一底 ω_1'，…，ω_m'，则 $m=n$，而且其间的关系

$$\omega_i = \sum_{j=1}^{n} a_{ij}\omega'_j, i=1, \cdots, n$$

可以一个列式等于±1的方阵（a_{ij}）表之。

定理 2　没有有限聚点的复数模的秩数只能是一或二。（证明略见[2],pp.234）

定义 3　椭圆函数：

命 ω_1,ω_2 是任意二复数，其比非实数，适合于

$$f(z+2\omega_1)=f(z),\quad f(z+2\omega_2)=f(z)$$

的函数称为双周期函数。以 $2\omega_1$，$2\omega_2$ 为周期，双周期的亚纯函数称为椭圆函数。（在全平面上（不包括∞）除去孤立极点外，无处不解析的函数称为亚纯函数。）

如果亚纯函数的周期有一聚点，则它是常数。因为如果有聚点 z_0，则在 z_0 附近有无穷多个点 z_k 都使 $f(z_k)=f(z_0)$，$k=1$，2，…，由 Vitali 定理，可知其为常数。注意，此处两个周期其比是复数。

定义 4　考虑由变形

$$z'=z+m\omega+m'\omega',\quad m,m'=0,\pm1,\pm2,\cdots \qquad (1)$$

所成的群。如果有变形（1）把 z_0 变为 z，这两点称为相合。

定义 5　在平面上的一个域称为一个基域，如果它适合以下的条件

I　任何一点一定相合于这基域中的一点；

II　基域中任何一点都不相合。

§3.2　椭圆函数的一般性质

假设 $f(z)$ 是任一椭圆函数，即双周期的亚纯函数。具有周期 2ω 和 $2\omega'$。假定比 ω/ω' 非实数。并且不防假定 $\mathrm{Im}(\omega/\omega')>0$。因此由四点 0，$2\omega$，$2\omega'$，$2\omega+2\omega'$ 所形成的非蜕化的周期平行四边形称为基域。

定理 1　如果双周期函数是整函数，则它一定是常数。（证明略,见[2],pp236）

定理 2　椭圆函数 $f(z)$ 在基域内所有的极点的留数之和等于 0。（证明略见[2],pp237）

定理 3　不存在一阶的椭圆函数。

证明：由定理 2 可以立即推导。因为若存在一阶椭圆函数，则在基域内的某 a 点上有将仅有一个一阶极点，在该点处函数展开式的无限部分为 $B(u-a)^{-1}$，$B\neq0$，即留数不等于零。这显然与定理 2 式矛盾的。即椭圆函数的阶至少等于二。

定理 4　椭圆函数在基域内取一复数值 a 的次数等于阶数，因此零点数等于阶数。

证明：在基域中 $f(z)=a$ 的解数与极点数之差等于

$$\frac{1}{2\pi i}\int_c \frac{f'(z)}{f(z)-a}dz$$

被积函数是椭圆函数。因此，此数是 0。即得所证。

定理 5　在一基域内，$f(z)=a$ 的解是 $a_1,a_2,\cdots,a_n$，而 $f(z)=\infty$ 的解是 $p_1,p_2,\cdots,p_n$，则

$$\sum_{i=1}^{n} a_i,\ \sum_{i=1}^{n} p_i$$

相合。

前面已经讲过，没有一阶的椭圆函数存在。因而我们从两阶的椭圆函数入手，希望从这些基本的椭圆函数构造出所有的椭圆函数来。两阶的椭圆函数显然有两种：

(1)　只有一个两阶极点的椭圆函数；

(2)　有两个不同的一阶极点的椭圆函数。

这就是 Weierstrass 理论与 Jacobi 理论各自不同的出发点。

特殊情况：

在定义椭圆函数的时候，我们注意到了，两个周期 ω,ω'，它们的比值是非实数的。对于这一点，我们可以从以下几种情况来考虑：

① 当 ω,ω' 中有一个为零时，很显然 $f(z)$ 就变为单周期的函数。

不妨设 $\omega\neq 0$，则有

$$f(z+m\omega)=f(z),\ m\in Z$$

② 当 ω,ω' 的比值为实数时，有

$$\omega'=k\omega+\theta\omega,\ k\in Z,\ \theta\in(0,1)$$

因而有

$$\begin{cases} f(z+\omega)=f(z) \\ f(z+\omega')=f(z+\theta\omega)=f(z) \end{cases}$$

从而有

$$f(z+(1-\theta)\omega)=f(z)$$

因为函数是双周期的函数，我们可以得出

$$1-\theta=\theta \quad 或 \quad 1-\theta=1$$

有 $\theta=0$ 或 $\theta=1/2$，因为 θ 不可能为零，所以 $\theta=1/2$。

很显然 $f(z)$ 的周期为 $\omega/2$。从而 $f(z)$ 就变为单周期的函数。

一旦 $f(z)$ 变为单周期的函数。由于我们现在要考虑的是加密解密算法，我们可以把 $f(z)$ 直接放到实数域上进行考虑。对于有极点的函数，再讨论也就显得无意义了。因而，最终变成了普通以 ω 为周期的整函数的讨论。

对于普通以 ω 为周期的整函数，即适合于 $f(z+m\omega)=f(z), m\in Z$ 的整函数，命 $z=\omega w/2\pi$，及

$$f(z)=\phi(w)$$

则 $\phi(w+2\pi)=f(z+\omega)=f(z)=\phi(w)$

即 $\phi(w)$ 是以 2π 为周期的函数。要讨论 $\phi(w)$ 在全平面的性质，只要研究 $\phi(w)$ 在长条 $0\le w<2\pi$ 中的性质即可。

把 $\phi(z)$ 展开为 Fourier 级数得，

$$\phi(z)=\sum_{n=-\infty}^{\infty} c_n(y)\, e^{inx}$$

这儿

$$c_n(y)=\frac{1}{2\pi}\int_0^{2\pi}\phi(z)\, e^{inx}\,dx$$

因此对于该类函数，我们可以用快速 Fourier 变换来实现。这不在本文的讨论范围之内。

§3.3 几个重要的函数

§3.3.1 $\gamma(z)$ 函数

我们把原点放在基本平行四边形的中心，研究那种 z=0 为二重极点的椭圆函数。由于周期性，所以 $z=2m\omega+2m'\omega'$ 也都是极点，因此我们考虑级数

$$\sum_{m,m'}\frac{1}{(z-2m\omega+2m'\omega')^2}$$

记 T=$2m\omega+2m'\omega'$（以下同）

级数

$$f(z)=\sum_{m,m'=-\infty}^{\infty}\frac{1}{(z-T)^3} \qquad (1)$$

是绝对收敛的（但 z 不等于$2m\omega+2m'\omega'$之一）。在任何一个圆 R 内，除有在此圆内有极点的诸项外，这级数是一致收敛的。因而可以证明（1）代表一亚纯函数，而且它以$2\omega,2\omega'$为周期，是一个椭圆函数。

对（1）求积，得

$$\phi(z)=c+\int_{z_0}^{z}f(z)dz$$

$$=c-\tfrac{1}{2}\sum[\frac{1}{(z-T)^2}-\frac{1}{(z_0-T)^2}]$$

把$m=m'=0$的项提出，

$$\phi(z)+\frac{1}{2z^2}=c+\frac{1}{2z_0^2}-\tfrac{1}{2}\sum{}'[\frac{1}{(z-T)^2}-\frac{1}{(z_0-T)^2}]$$

其中$\sum'$表示由$\sum$中除去$m=m'=0$的一项。

右端的函数在 z=0 处有则，所以可选 c 使其在 z=0 处的值为零，即

$$0=c+\frac{1}{2z_0^2}-\tfrac{1}{2}\sum{}'[\frac{1}{(z-T)^2}-\frac{1}{(z_0-T)^2}]$$

$$\therefore\phi(z)=-\frac{1}{2}\{\frac{1}{z^2}+\sum{}'[\frac{1}{(z-T)^2}-\frac{1}{(z_0-T)^2}]\}$$

记$\varphi(z)=-\frac{1}{2}\gamma(z)$

$$\gamma(z)=\frac{1}{z^2}+\sum{}'[\frac{1}{(z-T)^2}-\frac{1}{(z_0-T)^2}]$$

易证：

(1) $\gamma(z)$是偶函数

$$\gamma(z)=\gamma(-z)$$

(2) $\gamma'(z)=-2f(z)$是椭圆函数

$$\gamma'(z)=-\frac{1}{z^3}-2\sum{}'\frac{1}{(z-T)^3}=-2\sum\frac{1}{(z-T)^3}=-2f(z)$$

(3) $\gamma'(z)$是椭圆函数

$$\gamma'(z+2\omega)-\gamma'(z)=0$$

$$\gamma'(z+2\omega')-\gamma'(z)=0$$

即

$$\gamma(z+2\omega)-\gamma'(z)=c$$

$$\gamma(z+2\omega')-\gamma'(z)=c'$$

取 $z=-\omega, z=-\omega'$ 时，可得 $c=c'=0$。

$\gamma(z)$ 也是椭圆函数。

(4) $\gamma'(z)$ 是三阶的椭圆函数。在半周期处，$\omega,\omega',\omega+\omega'$ 为零点。因此这些点都是 $\gamma(z)$ 的二重点，即

$$\gamma(\omega)=e_1,\gamma(\omega')=e_2,\gamma(\omega+\omega')=e_3$$

§3.3.2 $\gamma(z)$ 与 $\gamma'(z)$ 的代数关系

先求 $\gamma(z)$ 在 z=0 处的 Laurent 展开式。由于

$$\frac{1}{(z-T)^2}-\frac{1}{T^2}=\frac{1}{T^2}[(1-\frac{z}{T})^{-2}-1]$$

$$=\sum_{n=1}^{\infty}\frac{n+1}{T^{n+2}}z^n$$

而 $\gamma(z)$ 是偶函数，可知

$$\gamma(z)=\frac{1}{z^2}+\frac{g_2}{20}z^2+\frac{g_3}{28}z^4+\cdots \qquad (1)$$

$$g_2=60\sum'\frac{1}{T^4},g_3=140\sum'\frac{1}{T^6}$$

对（1）微分得

$$\gamma'(z)=\frac{1}{z^2}+\frac{g_2}{10}z+\frac{g_3}{7}z^3+\cdots \qquad (2)$$

由（1），（2）可知

$$\gamma'^2(z)=\frac{4}{z^6}(1-\frac{g_2}{10}z^4-\frac{g_3}{7}z^6+\cdots)$$

$$\gamma^3(z)=\frac{1}{z^6}(1+\frac{2g_2}{20}z^4+\frac{3g_3}{28}z^6+\cdots)$$

因此

$$(\gamma'(z))^2-4(\gamma(z))^3+g_2\gamma(z)=-g_3+c_2z^2+c_3z^4+\cdots$$

右边是一处处有则的双周期函数，所以是常数。即$\gamma(z)$和$\gamma'(z)$有代数关系，即关于$\gamma(z)$得微分方程

$$(\gamma'(z))^2=4(\gamma(z))^3-g_2\gamma(z)-g_3$$

$\gamma'(z)$的三个零点已经知道$z=\omega,\omega',\omega+\omega'$。因此得出

$$(\gamma'(z))^2=4(\gamma(z)-e_1)(\gamma(z)-e_2)(\gamma(z)-e_3)$$

这儿$e_1+e_2+e_3=0,e_1e_2+e_2e_3+e_3e_1=-\frac{g_2}{4},e_1e_2e_3=\frac{g_3}{4}$，判别式$\frac{1}{16}(g_2^3-27g_3^2)$必须非零。

命$\gamma(z)=W$，则得微分方程

$$\frac{dz}{dW}=\frac{1}{\sqrt{4W^3-g_2W-g_3}}$$

$$z-z_0=\int_{\zeta_0}^{\zeta}\frac{dW}{\sqrt{4W^3-g_2W-g_3}}$$

其中$\zeta=\gamma(z),\zeta_0=\gamma(z_0)$

命$z_0\to 0$，则$W_0\to\infty$，因此得出

$$z=\int_{\infty}^{\zeta}\frac{dW}{\sqrt{4W^3-g_2W-g_3}} \tag{3}$$

在此我们可以得出函数变换对

$$\gamma(z)\text{和}z=\int_{\infty}^{\zeta}\frac{dW}{\sqrt{4W^3-g_2W-g_3}}$$

但是此处$\gamma(z)$表达式收敛速度都是缓慢的，在计算数值时很不方便。这一点可由 Jacobi 的 Theta 函数来弥补。它们有迅速的收敛表达式，而且它们可以表示出椭圆函数。

§3.3.3 ϑ 函数

我们现在用符号

$$q = e^{\pi i \tau}, \mathrm{Im}(\tau) > 0$$

因此 $|q|<1$

定义

$$\vartheta(z,q) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2niz}$$

当 $|z|<A$ 时

$$|q^{n^2} e^{2niz}| \le |q|^{n^2} e^{2nA}$$

由于当 $n \to \infty$ 时

$$|q|^{n^2} e^{2nA} / |q|^{(n-1)^2} e^{2(n-1)A} = |q|^{2n+1} A^2 \to 0$$

故级数

$$\sum_{n=-\infty}^{\infty} |q|^{n^2} e^{2nA}$$

是收敛的。因此（1）在任何一个有限区域内一致收敛。所以 $\vartheta(z,q)$ 是 z 的整函数。

显然有

$$\vartheta(z+\pi,q) = 1 + 2\sum_{n=1}^{\infty} (-1)^n q^{n^2} \cos 2nz$$

可推得：

$$\vartheta(z+\pi,q) = \vartheta(z,q)$$

$$\vartheta(z+\pi\tau,q) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2niz}$$

$$= -q^{-1} e^{-2iz} \sum_{n=-\infty}^{\infty} (-1)^{n+1} q^{(n+1)^2} e^{2(n+1)iz}$$

我们定义因子 $-q^{-1}e^{-2iz}$ 为周期 $\pi\tau$ 的乘子。因此 $\vartheta(z,q)$ 是以 1，$-q^{-1}e^{-2iz}$ 为乘子，以 π，$\pi\tau$ 为周期的函数。

按照通常的惯例，用 $\vartheta_4(z,q)$ 表这 $\vartheta(z,q)$，其他三个 ϑ 函数的定义如下：

$$\vartheta_3(z,q) = \vartheta_4(z+\frac{1}{2}\pi,q) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \cos 2nz$$

$$\vartheta_1(z,q)=ie^{iz+\frac{1}{4}\pi i\tau}\vartheta_4(z+\frac{1}{2}\pi,q)$$

$$=-i\sum_{n=-\infty}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}e^{(2n+1)iz}$$

$$=2\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\sin 2(n+1)z$$

$$\vartheta_2(z,q)=\vartheta_1(z+\frac{1}{2}\pi,q)$$

$$=2\sum_{n=0}^{\infty}q^{(n+\frac{1}{2})^2}\cos 2(n+1)z$$

易证明，ϑ 函数的乘子如下表

	$\vartheta_1(z)$	$\vartheta_2(z)$	$\vartheta_3(z)$	$\vartheta_4(z)$
π	-1	-1	1	1
π τ	-N	N	N	-N

这儿 N= $q^{-1}e^{-2iz}$，而且易知 $\vartheta_1(z)$，$\vartheta_2(z)$，$\vartheta_3(z)$，$\vartheta_4(z)$ 各有 $0,\frac{1}{2}\pi,\frac{1}{2}\pi+\frac{1}{2}\pi\tau,\frac{1}{2}\pi\tau$ 极其相合的点为零点。

同时，我们易得 ϑ 的一些性质

(1) $$\frac{\vartheta'(z+\pi)}{\vartheta(z+\pi)}=\frac{\vartheta'(z)}{\vartheta(z)}$$

$$\frac{\vartheta'(z+\pi\tau)}{\vartheta(z+\pi\tau)}=-2i+\frac{\vartheta'(z)}{\vartheta(z)}$$

(2) $$\vartheta_3(z,q)=\vartheta_3(2z,q^4)+\vartheta_2(2z,q^4)$$

$$\vartheta_4(z,q)=\vartheta_3(2z,q^4)-\vartheta_2(2z,q^4)$$

等等。

§3.3.4 用 ϑ 函数表示椭圆函数

假定 $f(z)$ 是以 $2\omega,2\omega'$ 为周期的椭圆函数，命 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 为基本零点，$\beta_1,\beta_2,\cdots,\beta_n$ 为基本极点，并假设已经使

$$\sum_{r=1}^{n}\alpha_r=\sum_{r=1}^{n}\beta_r$$

我们可以证明函数

$$\prod_{r=1}^{n}\frac{\vartheta_1(\frac{\pi(z-\alpha_r)}{z\omega}|\tau)}{\vartheta_1(\frac{\pi(z-\beta_r)}{z\omega}|\tau)}$$

就是一个与 $f(z)$ 有相同零点，相同的极点及相同的周期 $2\omega,2\omega'$ 的函数。因此任一个椭圆函数 $f(z)$ 可以表成为（$\omega'/\omega=\tau,\mathrm{Im}(\omega'/\omega)>0$）

$$f(z)=A\prod_{r=1}^{n}\frac{\vartheta_1(\frac{\pi(z-\alpha_r)}{z\omega}|\tau)}{\vartheta_1(\frac{\pi(z-\beta_r)}{z\omega}|\tau)}$$

在此，我们也可用 ϑ 函数来表示 $\gamma(z)$，有表达式

$$\gamma(z)=-\frac{\pi^2}{16\omega^2}\frac{\vartheta_1''}{\vartheta_1'}+(\frac{\pi}{2\omega})^2\csc^2(\frac{\pi z}{2\omega})+(\frac{\pi}{2\omega})^2[\frac{\phi''(v)}{\phi(v)}-\{\frac{\phi'(v)}{\phi(v)}\}^2]$$

这儿 $v=\frac{1}{2}\pi z/\omega$，而 $\phi(z)=\vartheta_1(z)/\sin z$，$\vartheta_1'=\vartheta_1'(0),\vartheta_1''=\vartheta_1''(0)$

我们可以看出用 ϑ 来表示 $\gamma(z)$，显然计算变的简单。但我们同时看到了，在表达式中，有 $\vartheta(z)$ 的导数，这使得计算又变得复杂化，从而我们不得不寻找其他的途径来简化数值计算。

§3.4 椭圆函数和椭圆积分

在实际问题中，椭圆函数往往由椭圆积分而来。椭圆积分的普遍形式是

$$\int R(x,y)dx \qquad (1)$$

其中 $R(x,y)$ 为 x 和 y 的有理函数，而

$$y^2=P(x)=bx^3+cx^2+dx+e$$

而 $R(x,y)$ 通常可以表示为

$$R(x,y)=R_1(x)+\frac{R_2(x)}{y}$$

式中 $R_1(x)$、$R_2(x)$ 为 x 的有理函数。积分 $\int R_1(x)dx$ 可用初等函数表示，而

$\int R_2(x)/y dx$ 是椭圆积分， $R_2(x)$ 可以表示为

$$R_2(x)=\sum_{m=0}^{n} a_m x^m+\sum_{p=1}^{q}\sum_{k=1}^{n_p}\frac{b_{pq}}{(x-h_p)^k}$$

式中 a_m, b_{pq}, h_p 由此可见，椭圆积分可以归结为下面的两种类型

$$I_m=\int\frac{x^m}{y}dx\ ,\quad J_k=\int\frac{dx}{(x-h)^k y}$$

可以证明（P(x)是三次多项式下）I_m，J_k能用三个基本的椭圆积分I_0，I_1和J_1表示。下面给出证明。求下列微分

$$\frac{d}{dx}(x^m\sqrt{P(x)})=m x^{m-1}\sqrt{P(x)}+\frac{x^m}{2}\frac{P'(x)}{\sqrt{P(x)}}$$

$$=\frac{1}{y}\left\{m x^{m-1}(a x^4+b x^3+c x^2+dx+e)+\frac{1}{2}x^m(4a x^3+3b x^2+2cx+d)\right\}$$

$$=\frac{1}{y}\left\{(m+2)a x^{m+3}+(m+\frac{3}{2})b x^{m+2}+(m+1)c x^{m+1}+(m+\frac{1}{2})d x^m+me x^{m-1}\right.$$

求积得

$$(m+2)a I_{m+3}+(m+\frac{3}{2})b I_{m+2}+(m+1)c I_{m+1}+(m+\frac{1}{2})d I_m+me I_{m-1}=x^m\sqrt{P(x)}+c \quad (2)$$

其中c为积分常数。

当P(x)为三次多项式时，$a=0$，公式（2）在依次令m=0,1,…时，得出I_m可用两个基本的椭圆积分 I_0, I_1 表达，同样有（设P(x)为三次多项式）

$$\frac{d\sqrt{P(x)}}{dx(x-h)^k}=\frac{1}{(x-h)^{k+1}y}\left\{\frac{x-h}{2}P'(x)-kP(x)\right\}$$

$$=\frac{1}{y}\left\{-\frac{kP(h)}{(x-h)^{k+1}}+(\frac{1}{2}-k)\frac{P'(h)}{(x-h)^k}+\frac{(1-k)P''(h)}{2(x-h)^{k-1}}+(\frac{1}{4}-\frac{k}{6})\frac{P'''(h)}{(x-h)^{k-2}}\right\}$$

利用Taylor公式

$$P(x)=P(h)+(x-h)P'(h)+\frac{(x-h)^2}{2}P''(h)+\frac{(x-h)^3}{6}P'''(h)$$

$$P'(x)=P'(h)+(x-h)P''(h)+\frac{(x-h)^2}{2}P'''(h)$$

可得以上结果。

求积得

$$-kP(h)J_{k+1}+(\frac{1}{2}-k)P'(h)J_k+\frac{1-k}{2}P''(h)J_{k-1}+(\frac{1}{4}-\frac{k}{6})P'''(h)J_{k-2}=\frac{\sqrt{P(x)}}{(x-h)^k}+c$$

很显然有 $J_0=I_0$， $J_{-1}=I_1-hI_0$。

在上式中依次令k=1,2,… ，我们求出 J_k 可由 J_1,I_0,I_1 表达。三个基本的椭圆积分 J_1,I_0,I_1 分别叫做第三种椭圆积分，第一种椭圆积分和第二种椭圆积分。

§3.5 Sn 函数

§3.5.1 ϑ 函数的一些性质

定理1 关于 ϑ 函数有下列无穷乘积表达式

$$\vartheta_1(z)=2Gq^{\frac{1}{4}}\sin z\prod_{n=1}^{\infty}(1-2q^{2n}\cos 2z+q^{4n})=2\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\sin(2n+1)z$$

$$\vartheta_2(z)=2Gq^{\frac{1}{4}}\cos z\prod_{n=1}^{\infty}(1+2q^{2n}\cos 2z+q^{4n})=2\sum_{n=0}^{\infty}q^{(n+\frac{1}{2})^2}\cos(2n+1)z$$

$$\vartheta_3(z)=G\prod_{n=1}^{\infty}(1+2q^{2n-1}\cos 2z+q^{4n-2})=1+2\sum_{n=1}^{\infty}q^{n^2}\cos 2nz$$

$$\vartheta_4(z)=G\prod_{n=1}^{\infty}(1-2q^{2n-1}\cos 2z+q^{4n-2})=1+2\sum_{n=1}^{\infty}(-1)^n q^{n^2}\cos 2nz$$

这儿 $G=\prod_{n=1}^{\infty}(1-q^{2n})$。

从而，我们又易知：

$$\vartheta_1'(z)=\phi(0)=2Gq^{\frac{1}{4}}\prod_{n=1}^{\infty}(1-q^{2n})^2$$

$$\vartheta_2(z)=2Gq^{\frac{1}{4}}\prod_{n=1}^{\infty}(1+q^{2n})^2 \qquad (1)$$

$$\vartheta_3(z)=G\prod_{n=1}^{\infty}(1+q^{2n-1})^2 \qquad (2)$$

$$\vartheta_4(z)=G\prod_{n=1}^{\infty}(1-q^{2n-1})^2 \qquad (3)$$

定理2

$$\vartheta_1^2(z)\vartheta_3^2=\vartheta_4^2(z)\vartheta_2^2-\vartheta_2^2(z)\vartheta_4^2$$

$$\vartheta_1^2(z)\vartheta_2^2=\vartheta_4^2(z)\vartheta_3^2-\vartheta_3^2(z)\vartheta_4^2$$

$$\vartheta_1^2(z)\vartheta_4^2 = \vartheta_3^2(z)\vartheta_2^2 - \vartheta_2^2(z)\vartheta_3^2$$

$$\vartheta_4^2(z)\vartheta_4^2 = \vartheta_3^2(z)\vartheta_3^2 - \vartheta_2^2(z)\vartheta_2^2$$

§ 3.5.2 ϑ 函数的商所适合的微分方程

函数 $\vartheta_1(z)/\vartheta_4(z)$ 是以-1，+1为乘子，π 、$\pi\tau$ 为周期的函数。因此它的微商

$$\{\vartheta_1'(z)\vartheta_4(z) - \vartheta_4'(z)\vartheta_1(z)\}/\vartheta_4^2(z)$$

也有些性质。又函数

$$\vartheta_2(z)\vartheta_3(z)/\vartheta_4^2(z)$$

也是以-1，1为乘子，π，$\pi\tau$ 为周期的函数，因此

$$\varphi(z) = \frac{\vartheta_1'(z)\vartheta_4(z) - \vartheta_4'(z)\vartheta_1(z)}{\vartheta_2(z)\vartheta_3(z)}$$

是以，π，$\pi\tau$ 为周期的函数，当且仅当

$$z = \frac{1}{2}\pi,\ \frac{1}{2}\pi + \frac{1}{2}\pi\tau$$

及相合点时，$\varphi(z)$ 才有可能有单极点。而且我们易验证 $\varphi(z)$ 是以 π 及 $\frac{1}{2}\pi\tau$ 为周期的椭圆函数，在基域内只有一单极点 $\frac{1}{2}\pi$。因此，它是一常数。命 $z \to 0$，可得常数是

$$\vartheta_1'\vartheta_4 / \vartheta_2\vartheta_3 = \vartheta_4^2$$

因此得出重要的微分方程

$$\frac{d}{dz}\{\frac{\vartheta_1(z)}{\vartheta_4(z)}\} = \vartheta_4^2\frac{\vartheta_2(z)\vartheta_3(z)}{\vartheta_4(z)\vartheta_4(z)} \tag{1}$$

与(1)相仿，我们还有

$$\frac{d}{dz}\{\frac{\vartheta_2(z)}{\vartheta_4(z)}\} = -\vartheta_3^2\frac{\vartheta_1(z)\vartheta_3(z)}{\vartheta_4(z)\vartheta_4(z)} \tag{2}$$

$$\frac{d}{dz}\{\frac{\vartheta_3(z)}{\vartheta_4(z)}\} = -\vartheta_2^2\frac{\vartheta_1(z)\vartheta_2(z)}{\vartheta_4(z)\vartheta_4(z)} \tag{3}$$

§ 3.5.3 Jocobi的三个重要的椭圆函数

定义

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})} \tag{4}$$

$$cn\mu = \frac{\vartheta_4}{\vartheta_2}\frac{\vartheta_2(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})} \tag{5}$$

$$dn\mu = \frac{\vartheta_4}{\vartheta_3}\frac{\vartheta_3(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})} \tag{6}$$

由§3.5.2中的定理2可知

$$sn^2\mu + cn^2\mu = 1 \tag{7}$$

$$\kappa^2 sn^2\mu + dn^2\mu = 1 \tag{8}$$

这儿

$$\kappa^{\frac{1}{2}} = \frac{\vartheta_2}{\vartheta_3}$$

由(1)，(2)，(3)，(4)，(5)，(6)可得

$$\frac{dsn\mu}{d\mu} = cn\mu dn\mu$$

$$\frac{dcn\mu}{d\mu} = -sn\mu dn\mu$$

$$\frac{ddn\mu}{d\mu} = -\kappa^2 sn\mu cn\mu$$

再由(7)，(8)可知 $y = sn\mu$ 适合于微分方程

$$(\frac{dy}{d\mu})^2 = (1-y^2)(1-\kappa^2 y^2) \tag{9}$$

同样 $y = cn\mu$ 适合于

$$(\frac{dy}{d\mu})^2 = (1-y^2)(\kappa'^2+\kappa^2 y^2) \tag{10}$$

这儿 $\kappa'^2 = 1-\kappa^2$， $y = dn\mu$ 适合于

$$(\frac{dy}{d\mu})^2 = (1-y^2)(y^2-\kappa'^2)$$

由(9)我们可得

$$\frac{d\mu}{dy} = \frac{1}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$$

求微分方程，我们可得（$sn0 = 0$）

$$\mu = \int_0^{sn\mu} \frac{dy}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$$

§3.5.4 算法对

通过以上的分析，我们可以容易地得到一个简洁的算法对

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})}$$

$$\mu = \int_0^{sn\mu} \frac{dy}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$$

在下面的章节中，我们将讨论该算法对如何用计算机来实现，以及用该算法对来实现的密码系统的安全性等。

第四章 加密解密算法的实现与分析

§4.1 基于椭圆函数的密码体制实现

我们在第二章的讨论中已经提到过，一个好的密码系统的关键是要有一个高强度的算法。通过第三节的分析，我们已经找到了一个高强度的算法。本节将引用前面所讨论出来的算法，设计一个新的而且安全性较高的密码系统，然后研究该算法的可行性，安全性，复杂度等。最后通过与其他算法作比较，对该系统的优、缺点进行分析。

§4.1.1 基于椭圆函数的密码体制

我们知道，现有的密码系统除了椭圆曲线密码体制外都涉及到大数的指数运算。而大数的指数运算有相当高的计算复杂度，这在工程计算中一般都要尽量避免的。因而我们这儿尽量的用类似于椭圆曲线密码体制的协议来设计我们的密码系统。当然，这也不能随便取的。在后面将分析，我们的系统是能够达到实际应用的安全需求的，而且计算复杂度也较之于现有的密码系统更简单。

在这儿，我们利用前面所讨论出来的算法对：

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})}$$

$$\mu = \int_0^{sn\mu}\frac{dy}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$$

及类似于Massey-Omura的椭圆曲线公钥密码体制来设计一个新的密码系统。其

中 $\vartheta_1(z) = 2Gq^{\frac{1}{4}}\sin z\prod_{n=1}^{\infty}(1-2q^{2n}\cos 2z+q^{4n}) = 2\sum_{n=0}^{\infty}(-1)^n q^{(n+\frac{1}{2})^2}\sin(2n+1)z$

$\vartheta_2(z) = 2Gq^{\frac{1}{4}}\cos z\prod_{n=1}^{\infty}(1+2q^{2n}\cos 2z+q^{4n}) = 2\sum_{n=0}^{\infty}q^{(n+\frac{1}{2})^2}\cos(2n+1)z$

$\vartheta_3(z) = G\prod_{n=1}^{\infty}(1+2q^{2n-1}\cos 2z+q^{4n-2}) = 1+2\sum_{n=1}^{\infty}q^{n^2}\cos 2nz$

$\vartheta_4(z) = G\prod_{n=1}^{\infty}(1-2q^{2n-1}\cos 2z+q^{4n-2}) = 1+2\sum_{n=1}^{\infty}(-1)^n q^{n^2}\cos 2nz$

$q = e^{\pi i\tau}, \mathrm{Im}(\tau) > 0$

假设用户 A 欲向用户 B 发送信息 m，则该系统基本思想如下：

（1）选取适当的 q（保密），从而确定 $sn\mu$；

（2）我们用算法 $sn\mu$ 将消息 m 变换成 P_m，将 P_m 进行编码使之变换为消息空间上的点 Q_m；

（3）取一个整数 N，其为大于消息空间点数的大素数；

(4)用户 A 任意选择一数 e_A（保密且 1<e_A<N），求得 d_A，有 $e_A d_A = 1 \bmod N$；

（5）用户 A 先将 $e_A Q_m$ 送给用户 B；

(6)用户 B 任意选择一数 e_B（保密且 1<e_B<N），求得 d_B，有 $e_B d_B = 1 \bmod N$；

（7）用户 B 将 $e_B e_A Q_m$ 退还给用户 A；

（8）用户 A 再将 $d_A e_B e_A Q_m = e_B Q_m$ 送给用户 B；

（9）用户 B 将得到的数乘以 d_B 得 $d_B e_B Q_m = Q_m$；

（10）将 Q_m 进行反编码得 P_m；

（11）利用算法对中的积分公式求得 m。

§4.2.2 基本算法分析

上面的密码系统主要涉及到以下的基本算法：

（1） 有限域上的模逆算法

（2） 有限域上的大数模乘法

（3） 素数测试

（4） 指数运算

（5） 大数模运算

（6） 积分计算

其中（1）、(2)、(3)、(6）这几种基本运算可以用现有的成熟算法来计算，(1)、(3）在 §2.5 中已经讨论过了，这儿就不再赘述了。

（1） 大数模乘算法

设模数 P 位长为 n，用 A*B（mod P）表示模乘，其中 A，B∈[1，P-1]，均为 n 位长的二进制数。首先计算 A*B，得到一个 2n 位长的积，然后对积求模。若处理器的寄存器字长为 b，则把 A，B 按字长各分为 K 块。实际处理时，先计算 A 的有效字块数 K_A，B 的有效字块数 K_B，通过部分记结果移位求和得

结果 C，可比一般方法提高速度 2~4 倍。

（2） 求模算法设计

本算法的基本思想是预计算，将预计算的结果造表待用，以空间换取时间，因而不再需要在调用时临时计算。

本算法由建表、初步模和同阶模三步完成。

第一步：建表，即构造 M 的 d+1 阶和 d 阶模表，可采用递推法，效率很高。建表必须在任何一次取模之前完成。

第二步：初步取模。设 A 为 N 位 B 进制数，M 为 D 位 B 进制数，则初步取模之后的结果为一个 D 位的 B 进制数，可能大于 M，也可能小于 M。最终取模的结果在 A 中，为一个 d 位的 B 进制数。

第三步：求同阶模，即对上一步的结果进一步求模。

对于 A*B≡C mod P，A 和 B 均为 n 位的二进制数，C 为 2n 位的二进制数，采用本算法求模，只需做 n/8 次的二进制加法，这里 B=256。

（3） 指数运算

在计算 $sn(m)$ 的时候，主要要解决的是 ϑ_i 计算。在计算 ϑ_i 的时候，我们可以看到有一个主要的计算项目是幂运算 q^{n^2}。我们可以通过以下的递推算法来简化计算：

$$q^{(n+1)^2} = q^{n^2} * q^{2n} * q$$

（4） 积分计算

基于椭圆函数的密码体制，最后一个步骤是要用一个积分公式来实现解密的。但是，我们知道积分

$$\mu = \int_0^{sn\mu} \frac{dy}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$$

是无法用有理函数的形式表示的。在计算的时候我们可以用数值积分来实现。

（5） 其他的关键技术

1. 超越数：在计算 ϑ_i 的过程中，涉及到超越数 e，为了减少误差，我们现在直接用 q 来进行计算。因为 τ 的选取，主要的目的是要计算 q。直接用 q 来作为算法的参数可以减少很多的计算量，而且也简化了算法。

2. 误差：在计算 ϑ_i 时，由于 ϑ_i 是一个无穷级数，这是没有办法用于数值计算的，为了能够用于计算就要对它进行截断。但是，在后面的积分计算过程中，要用到该计算的结果。同时我们看到

$\mu = \int_0^{sn\mu} \frac{dy}{\sqrt{(1-y^2)(1-\kappa^2 y^2)}}$ 中的被积函数是一个递增的函数，为了使结果的更可靠，在选取截断误差的时候，可以先估计被积函数的最大值来选取。q 的选取也是要用到一定的近似值来实现的。由于 q 是小于 1 的数，因而在计算过程中，误差是不会扩大的。

§4.2 基于椭圆函数密码系统的分析

§ 4.2.1 可行性分析

基于椭圆函数的密码系统的可行性，主要的关键是在进行信息传送之前的变换和在最后解密时的积分计算。对于函数

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})}$$

级数

$$\sum_{n=-\infty}^{\infty} |q|^{n^2} e^{2nA}$$

有快速的收敛速度。因而

$$\vartheta(z,q) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} e^{2niz}$$

$$q = e^{\pi i \tau}, \mathrm{Im}(\tau) > 0$$

也有快速收敛的性质，我们在数值计算的时候可以对无穷级数进行适当的截断。截断误差可以按照需要来设定。

积分计算。前面提到过，最后的积分计算不能表示成有理函数的表示形式，那我们这儿可以用数值积分来实现计算。在计算的过程中，我们可以用逐渐加大划分密度的办法来简化积分的计算，并通过对前后两次的积分结果的比较来判断积分误差的大小，从而终止积分计算，得到我们需要的结果。

此外，是算法的浮点数的解决。因为信息空间是整数空间，在作密文传送的过程中，我们可以看到主要也是对整数信息流的操作。而通过函数

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})}$$

变换的结果将是一个位数较大的浮点数。为了实现整数操作的结果，我们可以将计算结果进行移位，将它变为整数形式后再进行后面计算。之后的操作则是一个

逆移位操作。

从以上的分析可以看出，其他方面的算法已经研究的比较成熟，当然也是可行的，因而我们的密码系统也是可行的。

§4.2.2 系统的安全性分析

什么是系统的安全性？密码系统的安全性是算法强度和密钥长度的函数。基于椭圆函数的密码算法，具有比现有一般算法较高的安全性，主要可以从以下几个方面来考虑。

第一、算法具有足够的强度。

通过第三章的讨论，我们可以看到，要对函数

$$sn\mu = \frac{\vartheta_3}{\vartheta_2}\frac{\vartheta_1(\mu\vartheta_3^{-2})}{\vartheta_4(\mu\vartheta_3^{-2})}$$

进行破译，必须要知道椭圆函数的周期或者 q。但是椭圆函数的周期或者 q 是我们保密的内容。为了防止，密码分析者进行穷举攻击，我们可以取 q 有足够的位数。在这儿我们可以取到 64 位二进制数，已经达到国际的安全的标准 40 位。同时我们可看到，该算法变换的唯一取决要素是 q，它对明文的变换也是没有一定的规律可寻。所以，基于椭圆函数的密码算法是可以抗一般对称密钥的的密码分析。同时，也可以看到基于椭圆函数的密码算法是可抗现在主要的密码攻击法：差分密码分析，概率统计等。此外基于椭圆函数的密码算法还有大数分解难度。所以说，基于椭圆函数的算法具有足够的安全性。

第二、密钥的长度。

密钥的长度的选择，取决于算法的强度。基于椭圆函数的算法是足够强的，因而，密钥长度只要达到国际的安全标准 40 位即可。但是为了便于计算，我们这儿也可以取密钥的长度为 64 位标准可以取 64 位二进制数，但是公钥 N 必须选择位数较大的数。如果算法的安全性只是基于大数的分解，那么，我们的密钥要求将是很大的，因为 128 位以上的大数已经有成功地被分解的例子。

§4.2.3 加密解密算法的计算复杂度

一、基于椭圆函数的算法的计算复杂度

该算法主要要解决的椭圆函数的计算。而我们从前面的讨论过程中可以看到，函数 $\vartheta(z,q)=\sum_{n=-\infty}^{\infty}(-1)^n q^{n^2} e^{2niz}$ 有很强的收敛性，我们涉及到的只是指数的运

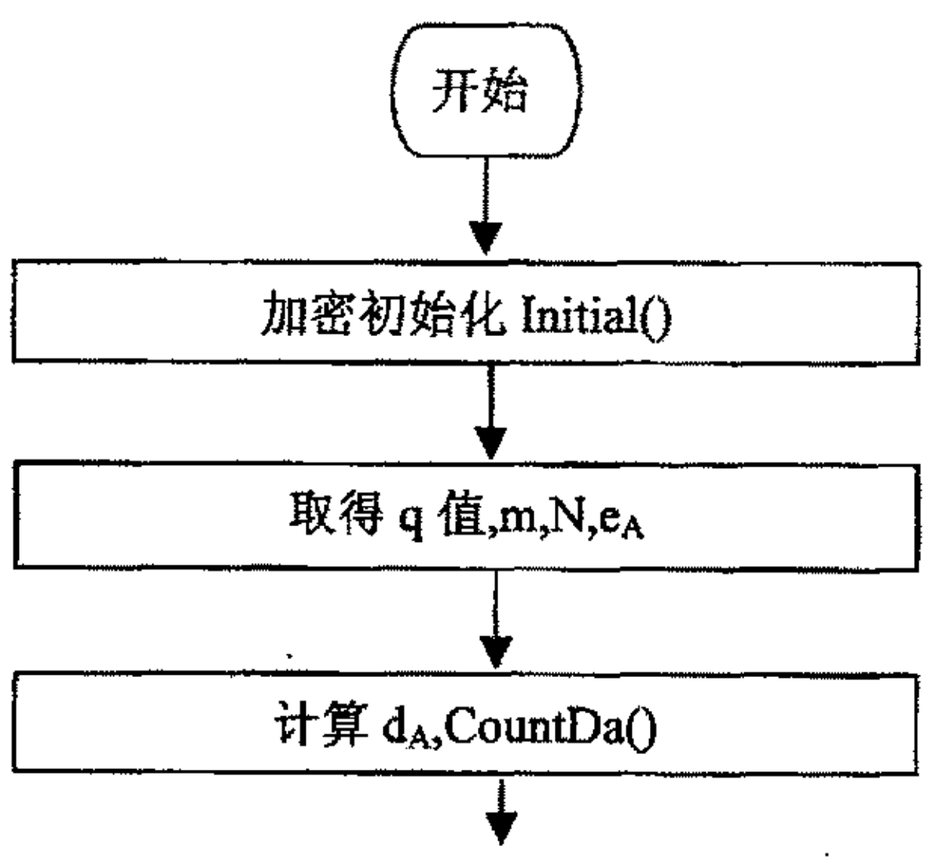
算。这在普通的公钥密码系统中都有。而我们的指数运算用 § 4.2.2 中的幂计算方法进行简化计算，总体的运算要比一般的算法快。当取定 N 时，我们可以看到主要涉及到的是乘法次数为 5N，加法次数为 N。因而在计算 sn 的过程最多达到的时间复杂度为 O(N)。对于空间复杂度，是由于以前的计算机的存取空间很少而要进行的，现在计算机硬件技术的飞速发展，使得我们在计算方法的空间复杂度上不用花费较多的精力。但是对于计算机的存取位数在实现算法的时候很重要。因为对于大数操作的时候直接影响到运算的精确度。基于椭圆函数的算法要求有 64 位的计算机存取位数。

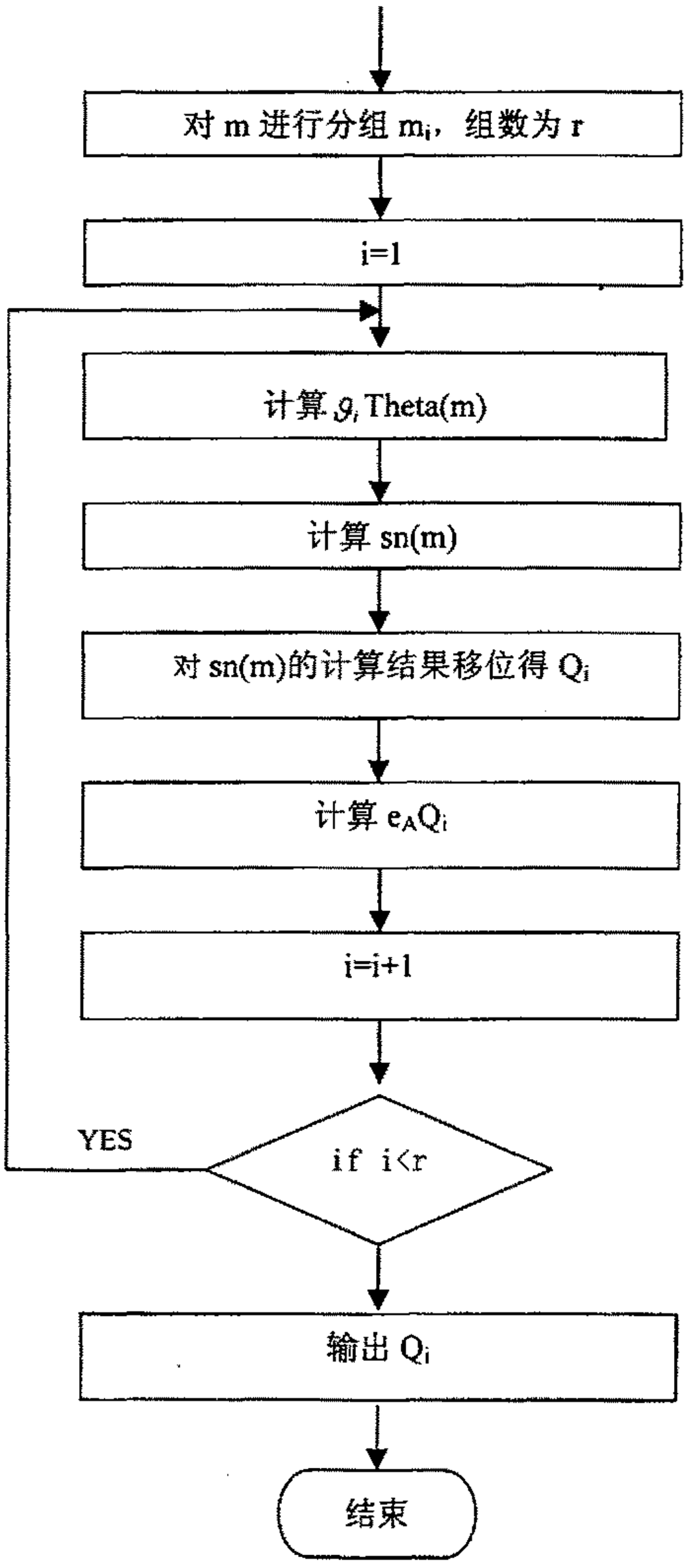
二、与其他算法的比较

在前面的讨论过程中，已经提到过，一般公钥密码体制的安全性是基于大数的分解难度之上的，但是随着计算机的发展和数论的研究，已经有好多成功分解高位大数的例子。为了提高算法的安全因素，人们又引进了指数的运算。这样就把离散对数的难度加到了公钥密码体制当中，如 RSA 等。但是，这无形之中就又涉及到了大数的高次运算。因为，如果底太小的话，密码分析者还是可以根据最原始也是最有效的穷举法进行分析。基于椭圆函数的密码系统与一般的椭圆曲线密码体制相比，少了曲线上的点加运算和复杂的平方剩余计算，同时把计算大数指数运算的复杂度简化到了计算椭圆函数的计算。因而，基于椭圆函数的密码算法具有比一般算法更快的速度。

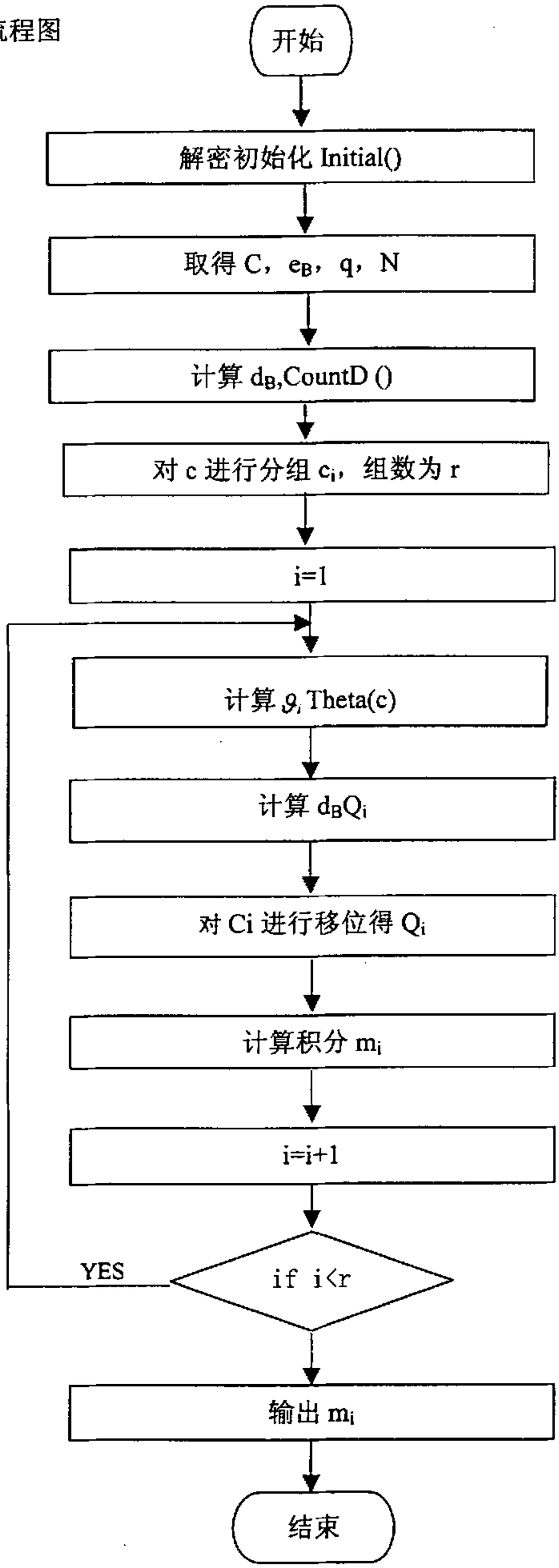
§ 4.3　程序流程图

§ 4.3.1 加密主程序流程图




对 m 进行分组 m_i，组数为 r
i=1
计算 g_i Theta(m)
计算 sn(m)
对 sn(m)的计算结果移位得 Q_i
计算 $e_A Q_i$
i=i+1
if i<r
YES
输出 Q_i
结束

§4.3.2 解密程序流程图


开始
解密初始化 Initial()
取得 C，e_B，q，N
计算 d_B,CountD ()
对 c 进行分组 c_i，组数为 r
i=1
计算 ϑ_i Theta(c)
计算 d_BQ_i
对 Ci 进行移位得 Q_i
计算积分 m_i
i=i+1
if i<r
YES
输出 m_i
结束

§4.4 实验数据

§4.4.1 测试的数据

N=299999999

ea1=25367　　ea2=76383

q=1111000011110000

m=0000111100001l　　00111100001111　　00110011001100　　0011

e(m)=998316060384003l　　99941035349061 28　　999399518965659 7

999399409515 0649

(1) eaqm=375865162130888502042432951637519271767454671398714782124624 6592046793

(2) neaqm=128357843210066701204243295163751927176745467189036801764664 30186521228

m=0000000000001　　00001111001111　　00001111001110　　0000111100110 10011

e(m)=998305006855592 5　　998316060394947 2　　998316060394937 5

998316060394847 8　　999399409515 0649

(1) eaqm=

25310691725815527112835784317252078112835784328379595837586516261041 7592124624651865212

(2) neaqm=

10030194125815527112835784328625655712835784328379595812835784326104 17591746643018 6521

q=0000000000000001

m=0000111100001l　　00111100001111　　00110011001100　　0011

e(m)=998345220964051 2　　999439609943361 7　　999428774681 52

9999428665007 9585

(1) eaqm=

26031934450868719219522126237992627136799337363499211359591242289538 05

(2) neaqm=

20232801550868719278441770232570846250969309363499212506902721688369 29

m=0000000000001　　00001111001111　　00001111001110　　0000111100110 10011

e(m)=998334166468291 5　　998345220974996 1　　998345220974986 3

998345220974896 8　　999428665007 9585

(1) eaqm=

1758397461115102742023280151272615112023280151247755452023280151020720802506902721688 36

(2) neaqm=

1742721131115102742023280151272615112023280151247755452023280151020720802506902721688 36

q=9999999999999999

m=0000111100001 1 00111100001111 00110011001100 0011

e(m)=9981004944115107 99919407882448 84 9991832513238518 9991831419442157

(1) eaqm=

1815214226792299925560581789970406144391512148722560603702502830 81

(2) neaqm=

1815214226792299925560581720797988922815872312148722522787968628919826 2

m=0000000000001 0000111100111 1 0000111100111 0 0000111100110 1 0011

e(m)=9980894480337682 9981004944224477 9981004944224377 9981004944223482 9991831419442157

(1) eaqm=

1065949642331846601909981792982379501909981791397750981815214221170716336060370228919 82

(2) neaqm=

1534908872598608718152142214231179818152142213977509818152142211707163322787968628919 82

q=0011001100110011

m=0000111100001100111100001111001100110011000011

e(m)= 9983452045820 9919994395935075495 9994287580328747 9994286485726857

(1) eaqm=2601665781410825712194457431715435152509185751507025531358063582331887 67

(2) neaqm=2022772811410825712784164032600846302509185759933194125063953823318876 7

m=0000000000001 0000111100111 1 0000111100111 0 0000111100110 1 0011

e(m)=9983341500868828 99834520459304 40 9983452045930341 9983452045929446 9994286485726857

(1) eaqm=

1757633636368934520227728121747536320227728197248297260166578288855122506395382331887 67

(2) neaqm=

174246746139559949202277281217475363202277281214964030202277281192
260565250639538233188767

§4.4.2 数据分析

我们通过对算法的测试（其中数据的选取是比较有代表性的），可以发现以下几个方面：

（一）由于我们是把信息流映射到曲线上的，因而，比较接近的数据流加密得到的数据也是比较接近的。如果直接发送，可以进行差分攻击。解决方法：使用随机数及双密钥，即当密钥取 64 位时，把密钥分成两个等长的子密钥，然后用随机数来发送 $e_{im}Q_m$，e_{im} 为两个子密钥中的一个。

（二）在解密过程中，我们得到了相同的数据，可以证明我们的算法是有效的。

（三）大素数测试

这是当前还待解决的问题。

（四）由于计算机地址总线的限制，直接用计算机的操作来实现大数模乘的运算，位数是很有限的。（20 位地址总线）

（五）当 m 的首位是 0 时，加密效果不好。

解决方法：对信息块选取时，我们舍去一位。在加密时，在信息块前加上一个恒定的非零数据。

（六）当 m 达不到所需的位数时（最后一个信息块），我们用在末尾补零的方法来实现。

（七）速度

通过测试及分析，我们发现基于椭圆函数的加密解密算法要比一般的公钥密码系统具有更快的计算速度。

（八）局限

整个算法是针对 十进制数来做的，对其他的信息流的处理还有待完善。

第五章　结束语

计算机密码学这个课题的研究是拥有悠久的历史，但也是长久不衰的课题。本人通过这次论文工作，深刻体会到了密码学在实际应用方面的广泛性及重要性。同时通过对现有的许多的算法研究，认识了密码算法的复杂性，巧妙性以及实现密码系统的困难性。因而以“计算机密码学的加密解密算法的分析与改进”这一课题作为自己的硕士论文，以期通过毕业论文的研究对于实际的安全课题有一个较深的体验。

本文以现有的多数密码算法为基础，研究的核心内容是设计一套改进的密码算法。本文首先对现有的密码算法做了一个大致的介绍，之后对现有的比较普及的算法进行分析比较，揭示了密码学的核心内容、密码算法的特点及关键技术。特别是对椭圆曲线的密码体制进行深入的研究。在研究椭圆曲线的过程中，多次提到了椭圆函数的优良性质。在李老师的指导下，我对椭圆函数进行了详细的探讨和研究。经过深入研究椭圆函数的特点及性质的基础上，发现了一套可以用在密码算法中的函数对（$sn\mu,\mu$）。这在以往的加密解密算法中是几乎没有见到过的。通过对以往算法的安全性基础的研究，发现用椭圆函数来实现加密解密具有更有效，安全性更好的性质。之后，通过对现有的密码体制的比较，选择了椭圆曲线的密码体制，并结合椭圆函数对（$sn\mu,\mu$），设计了一套新的密码体制，并对该密码体制进行了可行性，安全性及计算复杂度分析。总之，基于椭圆函数的密码体制具有以下几个特点：

（1）　该算法达到了密码系统安全性的需求，而且有比其它现有的密码系统更好的抗攻击性能。

（2）　该算法具有比现有的公钥密码系统更快的计算速度。

虽然算法具有以上的优点，但还有许多值得改进的地方：

（1）　基于椭圆函数的密码系统的提出是从椭圆曲线密码系统的研究出发的。因而，我们可以利用我们提出的新的算法来弥补和完善椭圆曲线的密码系统。

（2）　在计算速度及精度上还有几个方向，

a) 我们在研究过程中注意到9函数具有与 FFT 变换相似的形式，为了提高计算的精确性及计算速度，我们是否可以通过这条途径来实现？

b) 在计算的过程中，我们用到的都是浮点数的运算，而且还涉及到超越数。为了提高计算精度，李老师曾提到用连分式来解决。我觉得

这是一个很值得研究的方向。

c) 此外，在系统的加密解密速度和安全性方面还有其他的潜力可挖，如用熵来研究密码系统的安全性及系统的可靠性等。在实际应用方面还有待深入的探索。

一个好的密码系统要在具体的实际安全课题中实现还涉及到许多方面，如信息传输的网络协议，密钥管理，算法的硬件实现等等。由于文章篇幅及时间有限无法进行进一步的研究。

总之，密码学的研究将是一个长久的研究热点，具有深远的意义。现有的加密产品很多，特别有好多成熟的算法都申请了专利。我国在这方面的研究也化了相当大的精力，但是由于起步较晚，力量分散，核心技术受控于人，现在许多领域用到的加密产品还是要靠进口的，主要的加密技术产品还是被国外垄断着，就好比我们的“钥匙”一直被心怀不轨的敌人控制着，严重地影响着我国信息领域的安全。因而，我们必须通过研究密码学，突破密码技术的难点，设计出自己的加密产品，才能挣脱其他国家的束缚。

参考文献

[1] 卢开澄：《计算机密码学—计算机网络中的数据保密与安全》，清华大学出版社，1998。

[2] 华罗庚：《高等数学引论》，第二卷，第一分册，科学出版社，1981。

[3] Bruce Schneier（美）著，吴世忠，祝世雄，张文政等译：《应用密码学—协议、算法与 c 源程序》，机械工业出版社，2000。

[4] 高本庆：《椭圆函数及其应用》，国防工业出版社，1991。

[5] 王萼芳，杨伟成：《密码学进展—CHINACRYPT' 2000》，2000。

[6] 王竹溪，郭敦仁：《特殊函数概论》，科学出版社，1979。

[7] R.L. Rivest, A. Shanmir, and L.M. Adleman, " A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v.21, n.2, Feb 1978, pp.120-126.

[8] W.Diffie, M.Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Nov 1976, pp.648.

[9] A. Sorkin, "Lucifer, a Cryptographic Algorithm," Cryptology, v.8, n.1, Jan 1984, pp. 22-41.

[10] H. Feistel," Block Cipher Cryptographic System," U.S Patent #3,798,359, 19 Mar 1974.

[11] H. Feistel," Step Code Ciphering System," U.S. Patent #3,798,360,19 Mar 1974.

[12] H. Feistel," Centralized Verification System," U.S. Patent #3,798,605,19 Mar 1974.

[13] R. Scott, "Wide Open Encryption Design Offers Flexible Implementations," Cryptologia, v.9, n.1, Jan 1985, pp.75-90.

[14] S. Miyaguchi, "The FEAL-8 Cryptosystem and Call for Attack," Advances in Cryptology-CRYPTO'89 Proceedings, Springer-Verlag, 1990, pp.624-627.

[15] S. Miyaguchi, "The FEAL Cipher Family," Advances in Cryptology-CRYPTO'90 Proceedings, Springer-Verlag, 1991, pp.627-638.

[16] M.C. Wood, technical report, Cryptech, Inc., Jamestown, NY, Jul 1990.

[17] T.W. Cusick and M.C Wood, "The REDOC-II Cryptosystem," Advances in Cryptology-CRYPTO'90 Proceedings, Springer-Verlag, 1991, pp.545-563.

[18] L. Brown, J. Pieprzyk, and J. Seberry," LOKI: A Cryptographic Primitive foe Authentication and Secrecy Applications," Advances in Cryptology-CRYPTO'90 Proceedings, Springer-Verlag, 1991, pp.229-236.

[19] R.C Merkle," Fast Software Encryption Functions," Advances in Cryptology-CRYPTO'90 Proceedings, Springer-Verlag, 1991, pp.476-501.

[20] R.C. Merkle," Method and Apparatus for Data Encryption, " U.S Patent #5,003,579,26 Mar 1991.

[21] X. Lai, "On the Design and Security of Block Ciphers," ETH Series in Information Proceedings, v.1, Konastanz: Hartung-Gorre Verlag, 1992.

[22] J. Daeman, R. Govaerts, and J. Vandewalle," Block Ciphers Based on Modular Arithmetic," Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 15-16 Feb 1993, pp.80-89.

[23] J. Daemen, R. Govaerts, and J. Vandewalle," A Hardware Design Model for Cryptographic Algorithms," ESORICS 92, Proceedings of the Second European Symposium on Research in Computer Security, Springer-Verlag, 1992, pp.419-434.

[24] H. Gutowitz, " A Cellular Automation Cryptosystem: Specification and Call for Attack," unpublished manuscript, Aug 1992.

[25] H. Gutowitz, " Method and Apparatus for Encryption, Decryption, and Authentication Using Dynamical Systems," U.S. Patent #5,365,598,15 Nov 1994.

[26] H. Gutowitz, " Cryptography with Dynamical Systems," Cellular Automata and Cooperative Phenomenon, Kluwer Academic Press, 1993.

[27] S.B Morris, " Escrow Encryption," lecture at MIT Laboratory for Computer Science, 2 Jun 1994.

[28] P. Gutmann, personal communication, 1993.

[29] M.E Hellman," The Mathematics of Public-Key Cryptography," Scientific American, v.241, n.8, Aug 1979; pp.146-157.

[30] R.C. Merkle and M. Hellman," Hiding Information and Signatures in Trapdoor Knapsacks," IEEE Transactions on Information Theory, v.24, n.5, Sep 1978; pp.525-530.

[31] R.L. Rivest, A. Shamir, and L.M. Adleman," Cryptographic Communications System and Method," U.S. Patent #4,405,829,20 Sep 1983.

[32] S.C Pohlig and M.E. Hellman," An Improved Algorithm for Computing Logarithms in GF(p) and Its Cryptographic Significance," IEEE Transactions on Information Theory, v.24, n.1, Jan 1978, pp.106-111.

[33] S.C Pohlig and M.E. Hellman," Exponentiation Cryptographic Apparatus and Method," U.S. Patent #4,424,414,3 Jan 1984.

[34] H.C. Williams," A Modification of the RSA Public-Key Encryption Procedure," IEEE Transactions on Information Theory, v.IT-26, n.6, Nov1980, pp.726-729.

[35] T. ElGamal," A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp.10-18.

[36] T. ElGamal," A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, v.IT-31, n.4, 1985, pp.469-472.

[37] R.J. McEliece, " A Public-Key Cryptosystem Based on Algebraic Coding Theory," Deep Space Network Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, 1978, pp.114-116.

[38] John Keley，Bruce Schneier,，David Wagner：对 IDEA，GDES，GOST，SAFER 和三重 DES 密钥表的密码分析，密码与信息，1998.1，P55-63。

[39] 赵战生：全球信息化带来了密码应用的新契机，密码与信息，1998，P1-7。

[40] 赵霖，张龙军：椭圆曲线密码体制实现探讨，密码与信息，1998.3，P23-27。

[41] Nigel P. Smart，时文平（译）：超椭圆密码体制的性能，密码与信息，1999.4，P15-22。

[42] E. Biham and A. Shamir," Differential Cryptanalysis of DES-like

Cryptosystems," Advance in Cryptology—CRYPTO'90 Proceedings, Springer-Verlag, 1991, pp.2-21.

[43] E. Biham and A. Shamir," Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, v.4, n.1, 1991, pp.3-72.

[44] E. Biham and A. Shamir," Differential Cryptanalysis of the Full 16-Round DES," Advances in Cryptology—CRYPTO'92 Proceedings, Springer-Verlag, 1993, pp.487-496

[45] M. Matasui," Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology-EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp.386-397.

[46] M. Matasui," Linear Cryptanalysis of DES Cipher (I)," Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93), Shuzenji, Japan, 28-30 Jan 1993, pp.3C.1-14. (In Japanese.)

[47] M. Matasui," Linear Cryptanalysis Method for DES Cipher (III)," Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp.4A.1-11. (In Japanese.)

[48] X. Lai and J. Massey," A Proposal for New Block Encryption Standard," Advances in Cryptology-EUROCRYPT'90 Proceedings, Springer-Verlag, 1991, pp.389-404.

[49] C. Connell," An Analysis of NewDES: A Modified Version of DES," Cryptologia, v.14, n.3, Jul 1990, pp.217-233.

[50] A. Shimizu and S. Miyaguchi," Data Randomization Equipment," U.S. Patent #4,850,019,18 Jul 1989.

[51] M.C. Wood," Method of Cryptographically Transforming Electronic Digital Data from One Form to Another," U.S. Patent #5,003,596,26 Mar 1991.

[52] J.B. Lacy, D.P. Mitchell, and W.M. Schell," CryptoLib: Cryptography in Software," UNIX Security Symposium IV Proceedings, USENIX Association, 1993, pp.1-17.

[53] J.H. Moore," Protocol Failures in Cryptosystems," Proceedings of the IEEE, v.76, n.5, May 1998.

[54] 吴永森，张芹：公开密钥密码体制 RSA 算法的实现和应用，计算机工程，vol.19, 1993; pp28-33。

[55] N.Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, V.48, n.177, 1987, pp.203-209.

[56] V.S. Miller, "Use of Elliptic Curve in Cryptography," Advances in Cryptology-CRYPTO'85 Proceedings, Springer-Verlag, 1986, pp.417-426.