目　录

第 1 章
绪　论

随着 Internet(互联网)在全世界的广泛应用,人们纷纷开办了网络银行、网上商城、网上书店、网上影院、数字图书馆或从事微商等,一种新兴的商务模式——电子商务自然而然地产生。有别于传统的商务模式,电子商务借助于开放的 Internet 网络环境和现代信息技术,完成商品(服务)发布、商品(服务)选购、发货通知、货款支付、收货确认等工作。这些工作必然涉及客户和商家身份的验证、客户和商家隐私信息的保护、交易过程中机密信息的安全传输、交易行为的确认等问题。为此,电子商务的应用必须解决数据安全、身份认证、信息认证、网络安全、软件安全、交易协议安全、区块链安全等问题。本章将从提出电子商务的安全问题开始,给出电子商务的安全体系结构,并且讨论电子商务安全技术的发展趋势。

1.1　电子商务的安全问题

当今的世界已经是数字化的信息社会,数字经济正迅速发展。不管是城市还是乡村,计算机成为家庭的常用物品,有些家庭甚至拥有多台台式计算机或者笔记本电脑、平板电脑,几乎人人都拥有智能手机。借助于 Internet,人们可以通过电子邮件、短信、即时通信软件(如 QQ、微信等)进行交流,也可以传送文件、听音乐、看电影、购物、存款和付账等。

Internet 被设计成为一个高度开放的信息交换的媒介,人们可以在任何时候、任何地点,跨越时空,通过 Web 浏览器访问他们所需的信息和获取他们所需要的服务。Internet 不仅深刻地影响了个人的生活和工作方式,而且对商业的运作产生了巨大的冲击。将传统的贸易活动移植到 Internet 平台上而产生的电子商务已经发展成为人们在 21 世纪里进行商务活动的一种有效模式。基于 Internet 的电子商务正成为世界工商业和服务业的一个重要组成部分。可以说,几乎所有可以买卖的东西都能在 Internet 上进行交易。统计数据显示,2020 年中国电商市场规模达 37.21 万亿元,2021 年中国跨境 B2B 电商市场规模达 5.7 万亿元,2021 年第二季度中国网络零售 B2C 市场交易规模达 22 742.8 亿元。“十三五”期间,我国电子商务交易额年均增长超过 11.6%。电子商务的发展形势喜人、前景诱人。

B2C 的电子商务方式被迅速接受的一个原因是其方便性,人们可以坐在家里方便地购

买东西(或信息服务)并享受送货上门服务。对于行动不方便的人来说,购物变得容易多了;对于想寻找更好交易的人来说,简单多了,因为不再需要到处逛商店来货比三家。所有一切,只需轻轻按一下鼠标或者点击确认就可以完成,不会再腰酸脚痛。此外,不算运费,考虑一下到处寻找商店和比较所花的交通费用,电子购物事实上也能节省费用。对于 B2B 领域,电子商务削减了传统商业意义上的差旅费、商品展示费、场地租用费、仓储费以及销售人员工资等商业运作成本。其实,Internet 本身就是一个巨大的电子商务展台,它显著地降低了商业运作成本。

基于 Internet 进行的电子商务活动主要有:商务信息通过计算机网络进行传输,在网络上传输的信息是加密数据并保持完整性,贸易双方进行身份认证和确保交易的安全性。安全问题在电子商务的发展和应用中越来越突出,如何建立一个安全、便捷的电子商务应用环境,对信息提供足够安全的保护,已经成为商家和用户都十分关心的话题。目前,大多数用户端使用的计算机操作系统是微软的 Windows 系统和苹果的 Mac 操作系统,智能手机使用的操作系统有 Android、iOS、HarmonyOS 等,这些操作系统提供的安全性强度近些年来得到了提高,但仍然存在安全威胁。更让人担心的是,黑客使用一些病毒进行拒绝服务(Denial of Service,DoS)攻击,大多用户根本没有意识到自己的计算机已经被攻击。DoS 病毒利用多个系统发送大量请求信息包轰击网站,造成目标站点“死机”,使得系统无法响应服务。2003 年 8 月,冲击波(MSBlaster)和冲击波杀手(Nachi)病毒利用 Windows 操作系统等的远程过程调用 RPC 漏洞大量感染 Internet 的计算机,使得系统不断被要求重启,无法进行正常的操作和使用,危害面极广、危害后果极为严重。

一波未平,另一波又起。2003 年 9 月中旬,另一个 Windows 操作系统的远程过程调用 RPC 接口又被发现存在多个远程安全漏洞。这些漏洞是由不正确处理畸形消息所造成的,漏洞实质影响了使用 RPC 的 DCOM 接口(此接口处理由客户端计算机发送给服务器的 DCOM 对象激活请求,如 UNC 路径)。攻击者通过 135(UDP/TCP)、137/UDP、138/UDP、139/TCP、445(UDP/TCP)和 593/TCP 端口进行攻击,而对于启动了 COM Internet 服务和 RPC over HTTP 的用户来说,攻击者还可通过 80/TCP 和 443/TCP 端口进行攻击。由于 Windows 的 DCOM 在处理参数的时候没有检查长度,因此通过提交一个超长(数百字节)的文件名参数可以导致堆溢出,从而使 RPC 服务崩溃。这样,攻击者利用这些漏洞向目标发送畸形 RPC DCOM 请求来取得本地系统权限,在系统上执行任意操作(如安装程序、查看或更改、删除数据或创建系统管理员权限的账户),严重影响 Windows 系统的正常运行。可以想象,在这些被病毒感染的计算机网络和电脑上进行电子商务操作,是很难保证其安全性的。

近些年来,智能手机操作系统安全事件时有发生。例如,2015 年 7 月,意大利知名监控软件厂商 Hacking Team 遭遇数据泄露,其中著名的间谍软件 Android RCS 通过远程监控系统利用 3 个通用的提权漏洞,对 Android 2.0 到 Android 4.3 版本的系统实施提权攻击,非法获取 Root 权限,进而实现远程监控。2015 年 8 月,KeenTeam 团队在黑帽大会上曝光了其利用一个提权漏洞实现的通用 Root 方案,号称可以对任何品牌的 Android 设备实施提权攻击。

2016 年 8 月苹果手机曝出 iOS“三叉戟漏洞”,攻击者通过短信发送给手机两个链接,在用户点击链接后即可远程控制手机,并且窃取手机上的短信、邮件、通话记录、电话录音、存储的密码等隐私数据,还能监听并窃取 WhatsApp、微信等社交软件的聊天信息。该链接利用了苹果手机 iOS 操作系统中的 3 个 0-day 漏洞,这 3 个漏洞就是在安全圈名声大噪的“三叉戟漏洞”。2017 年 5 月,安全公司 Check Point 的报告显示,现有的 Android 系统中存在漏洞,该漏洞利用了在 Android 6.0 里启用的权限许可功能,这个功能允许用户手动同意请求手机相关权限的应用程序,可以在 Android 手机上直接运行盗号、广告和勒索软件。2017 年 4 月,360 安全报告显示:99.1%的 Android 设备受到中危级别漏洞的危害,99.9%的 Android 设备存在高危级别漏洞,87.7%的 Android 设备受到严重危害级别的漏洞影响。2017 年 5 月 17 日,苹果公司连发了 iOS 10.3.2 和 MacOS 10.12.5 新系统,紧急修复 20 多个漏洞。

电子商务应用的另一个风险是有效性、实用性问题。对一个运用 Internet 作为交易手段的商业组织,它需要投资数十亿美元进行信息基础建设。据有关公司发布的市场调查报告,黑客(Hacker)的攻击使得一些诸如 Yahoo 和 eBay 这样的热门网站出现暂时性“死机”,它们的损失超过了 12 亿美元,严重影响了 Internet 上电子商务的应用和发展。著名的美国在线公司由于人为操作和技术上的失误,使得其 600 多万用户陷入瘫痪 10 小时。美国另一家网络在线通信服务公司的主干网出现重大故障,其后果是 40 万用户被迫中断联络 40 小时之久。因此,电子商务网站的访问无效或者网络瘫痪,将会促使顾客另外寻找新的供应商或者回到更传统的老办法——一家一家地逛商店来进行交易。

在 Internet 上进行电子交易自然需要安全、快捷的网络银行来支撑。然而,如果金融计算机网络系统缺乏安全防护、传输网络缺乏安全保障、转账支付缺乏安全通道、授权认证缺乏安全措施、个人私有信息和单位敏感信息缺乏保密措施,现代化的 Internet 就会出现好比使用“不加锁的储柜”存放资金、“公共汽车”运送钞票、“邮寄托寄”方式传送资金、“商店柜台”方式存取资金和“平信”邮寄机密信息的不安全局面。如此一来,用户运用 Internet 进行电子交易的热情和信心就会大打折扣。

为了保证基于 Internet 的电子商务的安全性,必须解决如下问题。

①信息的机密性。机密性要求保证系统存储的信息(用户个人资料、企业或者部门商业机密等)不泄露给非授权的人或实体,并且保证这些加密信息在网络传输过程中只有合法接收者才能获取和读懂。防止攻击者通过 Internet、搭线、在电磁波辐射范围内安装截收装置,或者在数据包经过的网关和路由器上截获数据,以获取用户的银行账号、密码以及企业商业机密等信息。

②信息认证。它检验信息的完整性,要求保证数据在传输过程中没有被非授权建立,没有在消息中插入信息以使得接收方读不懂或接收错误的信息,没有删除某条消息或者消息的某部分,没有改变信息流的次序或者更改替换信息的内容(如更改资金划拨方向等)和没有将信息截留并延迟一段时间后再重传给合法的接收方等现象。

③用户身份(实体)认证、数字签名。要求能够确认信息的发送方和接收方是否为合法用户并经过授权,以杜绝假冒他人身份发布指令调阅机密文件、冒充他人消费与栽赃、冒充主机

欺骗合法主机及合法用户、冒充网络控制程序套取或者修改使用权限和密钥信息等现象。

④可靠性。要求系统不能拒绝合法用户对网络系统中信息和资源的使用。

⑤不可抵赖性。系统确保发送方事后不能否认已经发送的数据和所执行的操作,接收方同样也不能事后否认已经接收的数据和执行了相应的操作。

⑥可控性。要求系统确保合法用户在指定的时间、指定的地点能够访问、控制、使用指定的资源。数据加密、身份和实体认证、信息认证、数字签名(电子签名)等技术取代了传统贸易中的纸质文件、手写签名和盖章,实现电子贸易的可靠性和不可抵赖性。

我们知道,由于传统的买卖双方是面对面地以一手交钱、一手易货的方式完成交易的,因此比较容易保证交易过程的安全性和可信性。而对于电子商务交易,买卖双方通过电话或者网络进行联系,跨越时空、互不谋面,交易双方彼此之间很难建立安全和信任的关系。因此,除了通常的计算机网络安全问题之外,电子商务领域面临的安全威胁还有以下几条。

①攻击者侵入网络数据库系统篡改用户信息、获取客户资料等商业机密。

②建立另一个与真正销售者服务器名字相似的服务器来假冒销售者,生成虚假交易数据、获取他人机密交易信息。

③信用威胁,买方提交订单后不付款或者延迟付款、卖方收到汇款后不发货或者无故延误交货。

④恶意竞争者以他人名义订购商品,以掌握竞争对手的库存信息、物流和资金流传输渠道及其方式。

⑤攻击者向销售商网络服务器发送大量虚假订单信息,阻塞通道、独占资源,使系统不能向其合法用户提供及时的服务。

⑥供应链攻击。其中以 Solar Winds 为代表的供应链攻击事件越发严重。最近的调查数据表明,大企业和中小型企业涉及第三方供应商(服务和产品)的数据泄露事件发生率分别为 43%和 38%。供应链攻击意味着攻击者仅需对一个供应商进行攻击,将会让成千上万的关联企业同时受到攻击。

我国的信息安全体系和信息安全基础设施建设起步较晚,但随着近年来国家的高度重视和大量物力与财力的投入,以及广大科研和工程技术人员的不懈努力,我们国家已经构建自己的信息安全体系,建设安全的 Internet 应用平台和示范工程。这些工作和成就为发展我国的安全电子商务事业奠定基础。电子商务在中国已经发展成为一个大有前途的行业。

1.2 电子商务安全体系结构

电子商务安全既是计算机和网络安全技术问题,又是安全管理问题。要确保电子商务的安全,首先需要加强对有关人员的电子商务技术安全教育,建立和完善电子商务法律和法规,严格按照各种法律、法规和制度来管理和运作电子商务。

在 Internet 上实现 B2B 和 B2C 电子商务活动时,因为需要处理资金支付等敏感问题,所以对安全技术提出了较高的要求。可以说,只有真正解决了电子商务的安全性问题,电子商

务才会得到真正的推广和普及。当然,要实现电子商务的安全就必须付出相当的努力和代价。为此必须建立与国际接轨、具有我国特色的电子商务安全理论体系,开发具有我国自主知识产权的安全电子商务软件系统。

众所周知,Internet 横跨五大洲、覆盖全球,具有开放性,网上终端动态加入和退出、自适应能力要求高,网上用户众多、个性化突出,网络信息内容广泛、结构复杂,网络操作系统和数据库异构、信息融合难度大。这些因素都是构建电子商务安全体系必须面对的困难和现实。Internet 上的电子商务安全涉及安全路由选择、追踪和监控交易过程、控制资金流和物流、敏感信息保密、信息完整性、通信可靠性、身份和实体认证、交易公证和仲裁等问题,是一个综合性的电子商务信息系统安全工程。

安全电子商务系统通过 Internet,将商家、客户和银行三方连接起来,使用安全代理服务器和 CA 认证系统等实现电子商务交易数据的机密性、完整性、不可抵赖性等安全功能。其中,商家这一方由服务器安全代理、数据库管理系统、审计信息系统和 Web 服务器等部分组成;客户方的计算机安装 WWW 浏览器和客户安全代理软件。客户安全代理的主要任务是负责对敏感信息进行加密、解密和数字签名,与商家或银行服务器进行通信并通过 CA 认证系统和商家服务器安全代理或银行安全代理一起实现用户身份认证;银行安全代理通过与商家或客户进行通信,对商家、客户进行身份认证。

一个实用的安全电子商务系统必须有机集成现代计算机密码学、信息安全技术、网络安全技术和电子商务安全支付技术等。其中,电子商务安全技术是电子商务技术体系的重要组成部分。一个电子商务安全体系结构如图 1.1 所示。

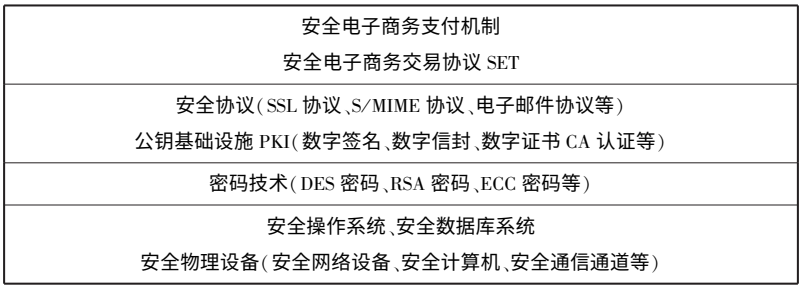

图 1.1　电子商务安全体系结构

从图 1.1 可知,安全电子商务是建立在安全的物理设备、安全操作系统、安全数据库、密码技术、数字签名、身份认证和信息认证、安全网络和安全应用协议之上的。安全物理设备包括安全网络设备、安全计算机、安全通信通道、安全存储系统与设备等。电子商务安全体系确保了电子商务活动的有效性、机密性、完整性和不可抵赖性。

密码技术利用密钥对敏感信息进行数学变换(密码算法),以达到保密的目的。密码技术包括密码算法的选取、密钥的生成和管理及分发等。密码技术分为对称密码系统和非对称密码系统两种。对称密码系统的加密密钥和解密密钥是相同的,它的安全性依赖于密钥的保护。目前,常用的商用对称密码系统是 DES 密码系统。对称密码系统加密、解密速度快,但密钥管理相当困难。非对称密码系统又称为公钥密码系统,它的加密密钥是公开的,

存储在密钥数据库里,需要进行秘密通信的双方可以在网上查找出对方的加密密钥对数据进行加密,然后将密文发送给对方;对方接收到密文后使用只有其自己知道的解密密钥进行解密、恢复原文。公钥密码系统灵活且大大减少了密钥量,但速度相对较慢。著名的公钥密码系统有 RSA 密码系统和椭圆曲线密码系统 ECC。RSA 密码系统利用将两个大素数相乘生成一个合数是容易的、但将某个合数分解还原成两个素数却十分困难的事实来确保它的计算安全性。椭圆曲线密码系统利用椭圆曲线的离散对数问题的难解性来构造密码系统,使得破译者在有限时间内不能破解密码,它被认为是最具有应用前景的公钥密码技术。我们国家颁布中国国家商用密码算法。此外,近年来兴起的量子密码是一种基于量子力学原理和量子计算范式的密码体制,目前处于理论探索和实验研究阶段,量子密码将是一种很有发展潜力的新型密码系统。

众所周知,传统的方法是通过手工签名/盖章来保证文件的真实和有效性。而在电子商务应用中,文件是数字化信息。为了验证数据来源的可靠性和输入时间的不可否认性,必须应用新的验证手段和方式,于是数字签名技术应运而生。数字签名技术由数字签名算法、数字信封结构、公钥基础设施 PKI 等构成。其中,数字信封将待签名的数据、时间组合成整体以抵抗重传攻击和替换攻击,确保数字签名之法律效力。除了常规的数字签名之外,数字签名技术还包括盲签名(匿名签名)、双重签名、群签名、门限签名、代理签名、门限代理签名和不可否认门限代理签名等。安全电子交易协议 SET 应用了双重签名技术,使得当签名方希望验证方仅知道报价单、中间人只知道授权指令时,在签名方和验证方两者报价相同的情况下中间人可以进行授权操作。

在电子化、计算机网络环境下进行商务交易之前,交易双方必须确认对方的身份。由于交易的双方可能远隔千里,不可能也没必要谋面,因此身份认证工作就交由所谓的身份认证技术来实现。目前,常用的身份认证技术有个人 ID、口令、生物特征(指纹、视网膜、DNA 基因)、智能卡身份认证、Keberous 身份认证、移动计算环境下的身份认证等。数字证书是解决这一问题的有效方法。它通常是一个签名文档,标记特定对象的公开密钥。现在比较通用的做法是由大家普遍信赖的第三方——认证中心 CA 给交易用户签发数字证书并由认证中心 CA 来承担安全电子交易认证服务、确定用户身份的服务结构等。

身份认证仅仅用于完成对交易双方的鉴别。为了确认所交易的数据的完整性,电子交易的双方还需要进行信息认证。信息认证技术的作用:合法的接收者能够验证其所接收到的信息是否真实,发送者无法抵赖自己所发送的信息,而且接收者也无法抵赖自己已经接收信息,当发送者和接收者双方发生争执时可交由第三方仲裁;可以发现交易信息在传输过程中是否被延时、重传。

现代电子商务交易是在开放的 Internet 上运作的,因此要确保电子商务安全首先要求传输商务信息的计算机网络基础设施本身是安全的。安全计算机网络系统要求计算机是安全的,网络互联设备是安全的,操作系统是安全的,Web 协议是安全的。安全芯片、安全存储介质、安全电源系统等构成安全计算机。安全网络交换机、安全路由器和安全集线器等是主要的安全网络设备。操作系统的安全是计算机系统安全的关键技术,也是安全电子商务的关

键要素。目前,在一般用户端上安装、使用的操作系统都存在着这样那样的安全漏洞,使各种业务应用系统的安全运行难以得到保障,尤其是某些国外公司设计的操作系统软件可以定时地将安装此操作系统的机器里的文件或者数据通过 Internet 自动发送出去,严重威胁用户个人的隐私、单位的商业机密和国家安全。安全网络协议是实现身份认证、数据加密、信息认证和不可抵赖等安全机制的基础,网络协议的安全性很大程度上决定了网络系统的安全性。安全网络协议包括安全的 TCP/IP 协议、SSL 协议、HTTP 超文本传输协议、IPsec 协议和 S/MIME 消息传送协议等。

为了确保基于 Internet 的电子商务系统的安全,还需要有虚拟专用网 VPN、防火墙、安全电子邮件、防治病毒、网络入侵检测等技术的支持。防火墙是一个建立在安全的内部网和不可信的外部网之间的强制的安全策略系统,它决定外部网用户可以访问内部网的什么信息、获取哪些服务以及哪些用户能够访问这些信息和服务,通过这些访问限制措施来确保内部网信息的安全。在电子商务领域,安全电子邮件意味着:一方面要有相应的技术来识别电子邮件传递的虚假商务信息;另一方面要有相应的措施和技术来防范和抗击电子邮件病毒引起的侵害。计算机病毒的感染和扩散将危害计算机和网络系统的正常运行,严重的甚至会导致整个系统的瘫痪。抗击病毒和制作病毒此消彼长,是一个长期、艰苦的斗争过程。为了取得抗击计算机病毒斗争的最后胜利、确保电子商务系统的安全运行,既需要有健全的计算机安全法律和电子商务安全法律作为保障,又需要有强大的计算机和电子商务安全理论与技术支撑。网络入侵检测的目的就是要检测用户访问计算机和网络系统的操作序列有无违反安全策略的行为和攻击迹象,及时报警并做出相应的措施。网络入侵检测技术是信息安全保障体系结构中四个不同层次上的重大关键技术之一。市场上已开发出一些入侵检测系统产品,在一定程度上发挥了积极的作用。目前,人们正规范公共入侵检测框架 CIDF 的体系结构、通信机制以及语言格式,并重点研究在分布式环境、移动计算环境、边缘计算下自适应的协同入侵检测模型、方法和技术。

基于健壮的计算机网络基础设施、数据安全技术、身份和信息认证技术以及网络安全技术,在安全的支付机制和交易协议支持下,一个完整、安全的电子商务系统就建立起来了,可以安全地应用和服务社会、造福人类。

1.3 安全电子商务的发展

电子商务安全问题伴随着电子商务的诞生而存在,伴随着电子商务的应用而发展。尤其是基于 Internet 的交易,其安全性更是电子商务发展和应用的关键。无论是国外的国际商业机器(IBM)公司的电子商务解决方案、甲骨文(Oracle)公司的电子商务解决方案,还是国内各银行推出的电子钱包、一卡通和一网通及其网上购物系统等,它们的安全性都得到了较好的体现。

IBM 电子商务解决方案的安全机制由 IBM Registry for SET 模块实现,它可以同时担当起持卡人认证中心、商家认证中心和付款网关认证中心的角色。其中,Administrator 提供服

务器管理、密码和密钥管理，Approver 负责接收和检验 SET 证明申请的应用程序与特定的界面，SETCA Server 分布申请并处理 SET 证明申请和签名。

Oracle 电子商务解决方案从高端到低端均基于 Internet 体系结构，使用户可以在标准的浏览器上按照权限进行访问，通过 Web 页面完成报价、订单、支付、执行和服务等业务环节，在网络上构建企业的需求链、供应链和内部管理链，实现整个商务过程的信息化和电子化。因此，无论是在国外还是国内都有 Oracle 电子商务解决方案的成功应用实例。Oracle 电子商务解决方案的 Oracle8i 数据库安全机制采用了工业标准 X. 509v3 证书提供的安全、单一的 dign-on 功能，使得用户只需验证一次而无须记住多个密码即可连接到数据库和其他应用中；其 Oracle 钱包存储 X. 509 证书、私有密钥和委托证书等数据；其 Oracle Advanced Security 支持安全套接字层协议 SSL，支持 Java、确保 IIOP 连接的安全性，使用 Java Database Connectivity（JDBC）接口保护交易安全；提供了防止攻击者在网络上窃听、篡改和伪造消息的手段并且提供对客户机和服务器进行验证的技术。

中国银行采用安全电子交易协议 SET 建立了符合国际标准的安全认证中心 CA 和支付网关，在保障客户资金安全的同时实现长城电子借记卡的网上实时支付功能，为网络信息供应商提供便捷的支付工具。此外，中国银行采用 SET 协议、利用香港中银信用卡（国际）有限公司的支付网关，在国内推出基于长城国际卡的网上支付手段，使得任何持有带 Visa 或 Master Card 标志的信用卡持卡人都可通过该网关进行网上支付、完成网上购物等。

招商银行开发的“一卡通”和“一网通”系统采用 X. 509 标准数字证书体系，运用数字签名技术和基于证书的强加密通信管道，确保电子银行业务和电子交易过程中客户身份认证和数据传输以及密码输入的安全。同时，招商银行推出国际信用卡网上支付的“VISA 验证”服务、提供跨国网上购物安全服务，用户使用信用卡进行全球网上支付时，交易界面会自动弹出有关信息，如果这些信息与用户在信用卡网站上设定的个人化信息一致，就说明这是一家通过“VISA 验证”的网上商家，刚刚进行的交易安全可靠，并通过输入交易密码的再次安全验证解决了网上支付无密码的状况，保证了客户个人资料和财产的安全。

Internet 是一种国际化、社会化、开放化和个性化特征明显的网络，无论是计算机系统结构还是操作系统平台，抑或是数据库平台都是异构的，信息不再局限于静态的文本文档，而是完全动态的多媒体内容，网上用户众多、关系复杂且动态加入/退出网络，这些都大大增加了网络管理的难度并带来不安全的隐患，使得基于 Internet 的电子商务应用安全性问题日益突出，电子商务的风险控制将是一个持久的课题。既便宜又有快速的计算能力的个人计算机机、平板电脑、智能手机以及商业组织结构的变化和更开放的电子商务模式使得 Internet 的规模越来越大，信息跨越网络实现共享，传统的安全手段已不能满足需要。

越是功能强大的电子商务应用就越需要更加开放的网络环境，这导致了防火墙技术有效性的缩减；日益庞大、复杂的电子商务组织和商业模式增加了电子商务内容的技术和法律风险；层出不穷的攻击针对的是诸如电子商务这样的应用而不是计算机系统本身。一些网络协议和应用系统的设计能够通过防火墙边界及防火墙技术进行某种程度的安全控制。防火墙可提供的安全能力与防火墙所使用的协议的控制粒度相关。一般的协议使用唯一的默

认的端口运行,如 Telnet 使用 23 端口、Email 使用 25 端口、Syslog 使用 514 端口、80 端口运行 HTTP Web 服务等。如果能够知道哪个端口执行什么服务,那么就可以配置防火墙实现一个高层次粒度的控制,阻塞某些服务而允许通过另一些服务。防火墙的代理功能可以提供更深度的控制,比如对进来的 Telnet 会话增加认证。如果允许多种类型的服务使用同一端口的话,那么防火墙将很难区分各个应用程序和过滤服务(过滤恶意的代码),同时很难对数据通道进行访问控制。但是,更加开放的 B2B 链接使许多厂商正在以突破或者绕过防火墙而不是协商通过防火墙控制的方式来开发他们的电子商务应用,从而产生应用日益开放、自动互连和系统安全的新矛盾。因此,安全电子商务要求除了应用防火墙技术之外,还需要依靠更高层次的操作系统和商业应用程序来理解和控制安全风险。

不断变化的商业环境推动着商业组织之间更开放的交流和信息共享的需求。许多电子商务企业正在通过合并或者合作来扩大“电子商务大家庭”,将这些原来可能是竞争对手、互不信任的公司纳入一个统一的“可信任的网络”,通过信息共享程序来请求访问内部资源,这自然携带着隐含的安全问题(电子商务应用中非技术性的安全问题)。

电子商务内容安全的另一方面来自技术威胁。计算机病毒借助用户桌面上的应用程序和编程环境(例如 Microsoft Office 文档中的宏编程环境、工作组环境)进行传播,修改存储的文档或者删空硬盘、破坏商业用户的信任;像 IIS 这样的网页服务软件和浏览器也同样存在着大量的安全漏洞。值得庆幸的是,黑客们针对 UNIX 或 VMS 这样的操作系统编写的病毒和蠕虫大多都不成功。因此, 安全电子商务系统要求人们尽量采用安全可靠的操作系统平台,最好是采用具有自主知识产权、独立开发的国产安全操作系统。

电子商务安全应用中所需要使用到的公开密钥等信息通常是存储在数据库之中的。如果对数据库的访问不加以控制、不采取任何安全措施,那么存储在数据库中的秘密信息就没有秘密可言。因此,必须解决好密钥数据库的安全问题。另外,在分布式网络、边缘计算环境下,密钥数据库的并发读并发写和同步更新问题仍然需要继续研究。

电子商务方面的隐私问题需要通过数据加密等技术来加以保证。但是,在电子商务应用中强调对机密信息进行保护的同时,也要考虑在法律授权下能够恢复出被加密的信息,这就需要我们解决密钥恢复技术问题,需要足够重视这方面的工作并加大对它的投入。

W3C 于 1998 年 2 月开发了具有良好的数据存储格式、可扩展性、高度结构化和便于网络传输的可扩展标记语言 XML。提出 XML 的一个主要目的是解决电子商务交易过程中信息和数据表达的复杂性,使交易变得方便简捷。但是如果应用通常的公钥基础设施 PKI 技术来解决基于 XML 的电子商务的安全问题,那么就需要 XML 应用程序支持整个 PKI,并且使用数字证书进行验证,这将使基于 XML 的电子商务应用变得复杂起来。同时,PKI 技术中的 X.509 证书使用了不同于 XML 的 ASN.1 语言进行描述,因此需要研究如何将 PKI 证书信息记入 XML 文档以保证 X.509 证书和 XML 文档同时在 Internet 上安全传输。此外,XML 支持第三代移动电话用户通过手机上网传输交易信息进行电子商务应用,但是移动电话的存储容量非常有限,难以应用现在的公钥基础设施 PKI 技术来进行身份验证和数字签名鉴别等工作。这些都表明人们需要进一步研究和开发基于 XML 的电子商务安全技术。

人们通过严格的形式化的逻辑验证,已经发现现在普遍使用的安全电子交易协议 SET 存在安全漏洞,因此,需要通过“防抵赖”和“可追踪(可溯源)”这两种机制来进一步保障 SET 中的信息安全。

电子商务应用离不开数字现金,提高数字现金支付系统的执行效率、解决数字现金的可分割性与可传递性、将群组盲签名技术应用到传统的离线数字现金方案以真实模拟现实生活及开发电子商务支付系统的基于通用标准的安全性测试与评估标准,这些将是安全电子支付系统中需要加以研究解决的问题。近些年来,新出现了比特币——点对点的电子现金系统,使区块链安全问题成为一个十分重要的新的安全问题,需要深入开展研究开发区块链安全技术及应用。

在电子商务安全管理与法律法规保障方面,多年来,我国陆续发布了信息系统安全保护、国际联网管理、商用密码管理、计算机病毒防治、安全产品检测与销售等方面的相关规定,制定实施了电子商务安全的人员管理制度、保密制度、跟踪与审计和稽核制度、应急措施制度、电子商务安全风险的识别与测量、电子商务风险管理流程和风险管理策略,颁布了《中华人民共和国电子签名法》等。我国已经正式开始施行《中华人民共和国电子商务法》《中华人民共和国网络安全法》和《中华人民共和国数据安全法》。这些为我国电子商务事业的健康发展提供了强有力的制度和法律保障。

1.4 本章小结

电子商务交易安全系统紧紧围绕传统商务在网络上应用时产生的各种安全问题,在计算机网络安全的基础上,保障电子商务过程安全、可靠进行。计算机网络安全与电子商务交易安全实际上是密不可分的,两者相辅相成,缺一不可。没有计算机网络安全作为基础,电子商务交易安全就犹如空中楼阁,无从谈起。没有电子商务交易安全保障,即使计算机网络本身再安全,仍然无法达到电子商务所特有的安全要求。

本章介绍了电子商务的安全问题、电子商务安全体系结构,以及电子商务系统安全技术问题、电子商务安全的管理和法律法规。期望读者通过本章的学习,对电子商务安全基本知识体系有一个总体的印象和认识。

习题 1

1. 试归纳总结电子商务应用中常见的安全问题。
2. 请分析电子商务安全体系结构中各层次安全技术的作用。
3. 请了解点对点的电子现金系统的安全问题。
4. 安全计算机网络系统具体有什么要求?
5. 请列举一些电子商务安全方面的法律法规。
6. 请查资料了解电子商务安全技术的新进展。

第 2 章
密码技术及应用

电子商务技术安全在很大程度上决定了电子商务发展的走向。没有技术的保障,电子商务的安全就无从谈起。技术保障中最重要的是密码学技术,加密技术及其应用提供了电子商务安全的技术保障。

本章主要介绍电子商务安全的技术基础,主要内容有对称密码系统和非对称密码系统、国密算法、数字签名、密钥管理、身份认证技术和信息认证技术。

2.1 对称密码系统和非对称密码系统

密码学是研究信息系统安全保密的科学,包含密码编码学和密码分析学两个分支。密码编码学对信息进行编码以实现隐蔽信息,而密码分析学则研究分析破译密码。两者相对独立、相互促进。加密和解密模型如图 2.1 所示。

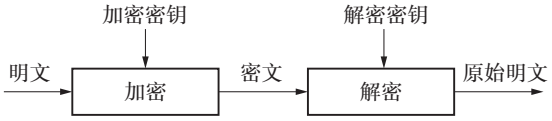

图 2.1 加密和解密模型

所谓“加密”,简单地说,就是使用科学的方法将原始信息(明文)重新组织变换成只有授权用户才能解读的形式(密文),而“解密”就是将密文重新恢复成明文。密码的出现可以追溯到远古时代,古代和早期的密码体制(又称“密码系统”)有置换密码、希尔密码、维吉尼亚密码、替换式密码、恺撒密码、摩尔斯电码等。密码学和其他学科一样随着社会的发展而发展,先后经历了纯手工阶段、机械化阶段、电子阶段,而现在则进入了计算机和网络时代阶段。目前,密码学已发展成一门系统的技术科学,是集数学、计算机科学、电子通信等诸多学科于一身的交叉学科。

密码技术是电子商务系统采取的主要安全技术手段之一。密码技术为电子商务提供以下 4 种基本服务。

①机密性:满足电子商务交易中信息机密性的安全需求,可以避免敏感信息泄露。

②不可否认:防止交易伙伴否认曾经发送或者接收过某种文件或数据。

③验证:消息的接收者应能确认消息的来源,入侵者不可能伪装成他人。

④完整性:消息的接收者应能验证在传递过程中消息没有被篡改,入侵者不能用假消息代替合法消息。

密码技术可以有效地用于身份认证、信息认证、隐私敏感信息保护、数字版权保护等,以防止种种电子欺骗。密码技术是实现信息的机密性、完整性、可用性的有力手段,它可以在一种开放的、潜在不安全的环境中保证通信及存储数据的安全。可以说,密码技术是认证技术及其他许多安全技术的基础,也是信息安全的核心技术。

密码技术包括密码设计、密码分析、密钥管理、验证技术等内容。密码设计的基本思想是伪装信息,使局外人不能理解信息的真正含义,而局内人却能够解读伪装信息的真实含义。密码设计的中心内容就是数据加密和解密的方法。出于种种原因,密码算法实际上很难做到绝对保密,因此现代密码学的一个基本原则是:一切秘密寓于密钥之中。在设计加密系统时,总是将加密密码算法公开,用户只需要保密密钥。

根据不同的标准,密码体制的分类方法很多,其中最常用的分类是将密码体制分为对称密码体制(也称为单钥密码体制、秘密密钥密码体制、对称密钥密码体制)和非对称密码体制(也称为双钥密码体制、公开密钥密码体制)。

在对称密码体制中,解密密钥与加密密钥是相同的或者可以通过加密钥匙推导出来。早期使用的加密算法大多是对称密码体制,所以对称密码体制通常也称为传统密码体制(常规密码体制)。在这种密码体制下,有加密(或者解密)的能力就意味着必然也有解密(或者加密)的能力。对称密码体制的优点是具有很高的保密强度,甚至可以经受国家级破译力量的分析及攻击,但它的密钥必须通过安全可靠的途径传播。因而密钥管理成为影响使用对称密码体制系统安全的关键性因素,难以满足 Internet 网络系统的开放性要求。

20 世纪 70 年代产生了非对称密码体制。在这种密码体制下,人们把加密过程和解密过程设计成不同的途径。当密码算法公开时,在计算上不可能由加密密钥求得解密密钥,因而加密密钥可以公开,而只需要秘密保存解密密钥即可。

在信息传输和处理系统中,攻击者会通过各种办法(如搭线窃听、电磁窃听、声音窃听等)来窃取机密信息。他们虽然不知道系统所用的密钥,但通过分析可能从截获的密文推断出原来的明文或密钥,此过程称为密码分析。对保密系统采取截获密文进行分析的攻击类型称为被动攻击。现代信息系统还可能遭受的另一类攻击是主动攻击,非法入侵者、攻击者采用篡改、增添、重放、伪造等手段向系统注入虚假消息,达到利己害人的目的。

2.1.1 对称密码系统

目前商用的对称密码系统主要有 DES、IDEA 和 SM4 等。我们重点介绍数据加密标准 DES(Data Encryption Standard),它由 IBM 公司研制,并被国际标准化组织(ISO)认定为商用数据加密的国际标准。DES 技术采用 64 位密钥长度,其中 8 位用于奇偶校验,剩余的 56 位

可以被用户使用。

1) DES 的产生和发展

DES 系统是由 IBM 公司的沃尔特·塔奇曼和卡尔·迈歇尔于 1971—1972 年研制成功的。该算法于 1975 年 3 月公开发表,1977 年被美国国家标准局(现在的美国国家标准与技术研究院)在联邦信息处理标准(FIPS)出版物第 46 号颁布为商用数据加密标准,这是美国国家标准局公布的第一个分组密码,并授权在非密级政府通信中使用。1980 年 DES 又成为美国国家标准协会(ANSI)的标准。自此 DES 成为国际上商用保密通信和计算机通信的最常用的密码系统。

随着 DES 的应用范围迅速扩大到美国以外的公司,某些美国军事部门也使用了 DES,这引起了美国国家安全局的忧虑,因为担心这种方法被敌对国使用,美国政府不允许出口该算法的加密软件。

2) DES 算法加密解密过程

DES 系统是一种分组密码,是为二进制编码数据设计的、可以对计算机数据进行密码保护的数学变换。DES 通过密钥对 64 位的二进制信息进行加密,把明文的 64 位信息加密成密文的 64 位信息。DES 系统的加密算法是公开的,其加密强度取决于密钥的保密程度。加密后的信息可用加密时所用的同一密钥进行求逆运算,变换还原出对应的明文。在 DES 系统中,64 位密钥中的 56 位用于加密过程,其余 8 位用于奇偶校验。确切地说,密钥分成 8 个 8 位的字节,在每一个字节中的前 7 位用于加密,第 8 位用于奇偶校验。

(1) DES 加密过程

DES 数据加密算法流程如图 2.2 所示。

DES 算法的加密步骤如下:

①将明文分组,每个分组输入 64 位的明文。

②初始置换(IP)。初始置换过程是与密钥无关的操作,仅仅对 64 位码进行移位操作。

③迭代过程,共 16 轮运算,这是一个与密钥有关的对分组进行加密的运算。

④逆初始置换(IP^{-1}),它是第②步中 IP 变换的逆变换,这一变换过程也不需要密钥。

⑤输出 64 位码的密文。

初始置换和逆初始置换是简单的移位操作。

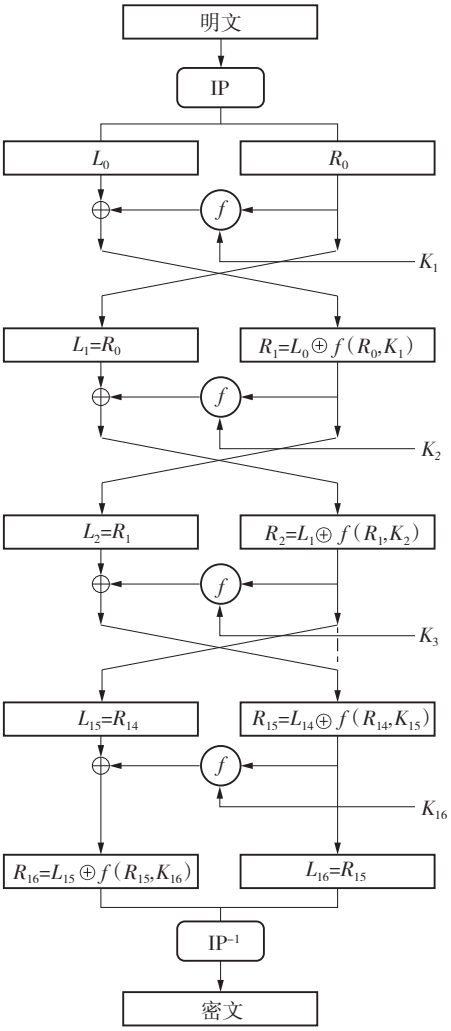

图 2.2 DES 数据加密算法流程图

DES 加密算法属于分组密码体制,在迭代过程这一步骤中,替代是在密钥控制下进行的,而移位是按固定顺序进行的。它将数据分组作为一个单元来进行变换,相继使用替代法和移位法加密,从而具有增多替代和重新排列的功能。迭代过程是 DES 加密算法的核心部分。

在图 2.2 中,设 B_i 是第 i 次迭代的结果,L_i 和 R_i 分别是 B_i 的左半部分和右半部分,K_i 是第 i 次迭代的 48 位子密钥,f 是进行替代、置换及密钥异或等运算的函数,⊕是按位作不进位加法运算,而其中的一次迭代过程如图 2.3 所示。

(2)DES 解密过程

DES 的解密过程和加密过程使用相同的算法,解密时每一轮迭代所使用的密钥与对应的加密迭代轮次所使用的密钥是相同的,也就是说,如果各轮的加密密钥分别是 K_1,K_2, K_3,…,K_{15},K_{16},那么解密密钥就是 K_{16},K_{15},…,K_2,K_1。显然,DES 的解密过程是加密过程的逆过程。

DES 解密过程如图 2.4 所示。

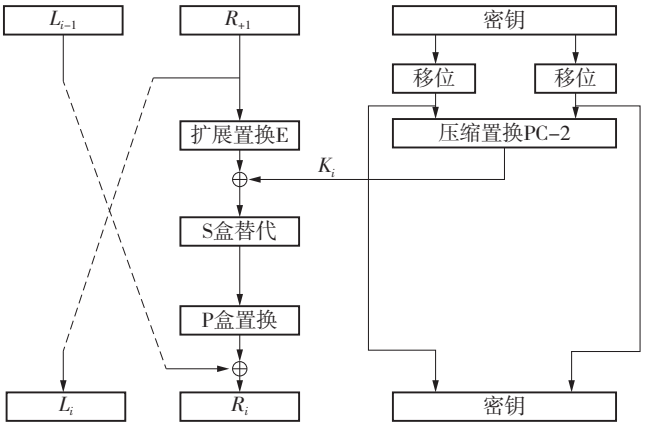

图 2.3 一轮迭代过程

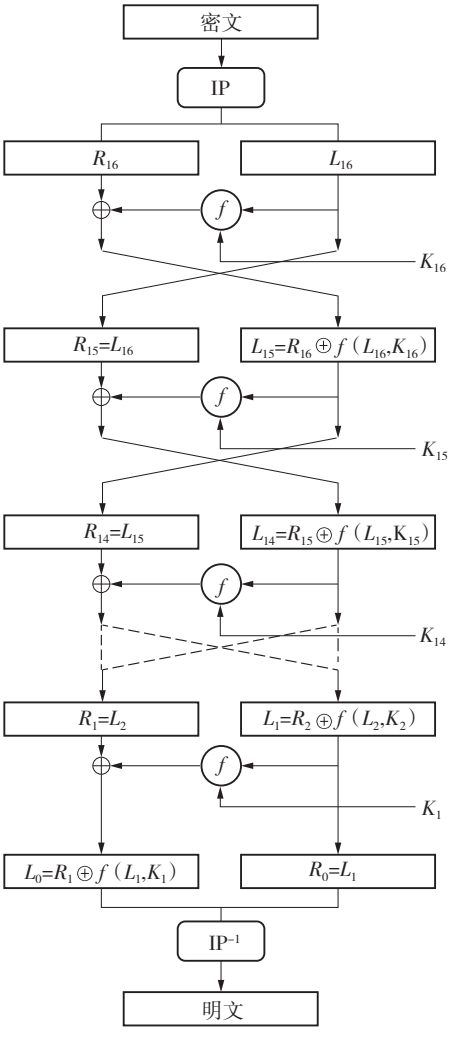

图 2.4 DES 解密过程

3) DES 系统的安全性

DES 加密算法重复地使用替代法和置换法来破坏对密码系统所进行的各种统计分析。DES 算法的设计者认为,替代法可将输出变换成输入的非线性函数,而置换法则是一种线性变换,它扩散了输出对输入的依赖性。通过连续使用这两种变换,将一种弱的密码变换变成一种强的密码变换。但是,长期以来,人们一直对 DES 的可靠性持怀疑态度,在密钥长度、迭代次数以及 S 盒的设计方面争论不休。

(1) 弱密钥和半弱密钥

许多密码系统都有坏密钥,DES 也一样。如果 DES 密钥置换中所产生的 16 个子密钥均相同,则这种密钥称为弱密钥。不难知道,当密钥全是 1、全是 0,或者一半全是 1、另一半全是 0 时,将是弱密钥。以下给出 4 种十六进制的弱密钥(每个第 8 位是奇偶校验位)。

01 01 01 01 01 01 01 01
1F 1F 1F 1F 0E 0E 0E 0E
E0 E0 E0 E0 F1 F1 F1 F1
FE FE FE FE FE FE FE FE

如果一个密钥能够解密用另一个密钥加密的密文,则这样的密钥称为半弱密钥,它们的 16 轮迭代仅仅产生了 2 个不同的子密钥,而不是 16 个不同的子密钥,以下是 6 对十六进制半弱密钥(每个第 8 位是奇偶校验位)。

01 FE 01 FE 01 FE 01 FE 和 FE 01 FE 01 FE 01 FE 01
1F E0 1F E0 0E F1 0E F1 和 E0 1F E0 1F F1 0E F1 0E
01 E0 01 E0 01 F1 01 F1 和 E0 01 E0 01 F1 01 F1 01
1F FE 1F FE 0E FE 0E FE 和 FE 1F FE 1F FE 0E FE 0E
01 1F 01 1F 01 0E 01 0E 和 1F 01 1F 01 0E 01 0E 01
E0 FE E0 FE F1 FE F1 FE 和 FE E0 FE E0 FE E1 FE E1

因而,为了确保 DES 加密系统的安全性,选择密钥时不能使用弱密钥或者半弱密钥。

(2) DES 系统的破译和安全使用

研究表明,DES 加密算法经过 8 轮迭代后,密文基本上是所有明文和密钥位的随机函数。既然这样,为什么还要采用 16 轮迭代呢? 近年来,人们试图降低迭代轮数,但都被成功攻破。Biham 和 Shamir 的差分密钥分析阐明了在迭代次数少于 16 次的情况下,对任意 DES 的已知明文的攻击比穷举攻击有效,而当迭代次数是 16 次时,采用穷举攻击却是最有效的。

对称分组密码算法最主要的问题是,由于加解密双方都要使用相同的密钥,因此在发送、接收数据之前,必须完成密钥的分发。因而,密钥的分发便成了 DES 加密体制中一个相当薄弱的环节。此外,当使用同一密钥对相同的信息块加密后,将得到相同的密文,这有可能为破译留下后门。

对 DES 加密体制,共有 2^{56} 个密钥可供用户选择。2^{56} 相当于 7.6×10^{16},若采用穷举法进

行攻击,假如 1 微秒钟穷举一个密钥,则需要用 2 283 年的时间,因此看起来是很安全的。但是 Diffie 和 Hellman 指出,如果设计一种 1 微秒钟可以核算一个密钥的超大规模集成芯片,那么它在一天内可以核算 8.64×10^{10} 个密钥,如果由一百万个这样的集成芯片构成专用机,那么它可以在不到一天的时间里用穷举法破译 DES 密码。在 1994 年的世界密码学大会上,Matsui 提出一种攻击 DES 的“线性密码分析法”,在一台普通的计算机工作站上,使用 2^{43} 个已知的明文及其密文,50 天内找到了 DES 的密钥。1998 年 7 月,美国电子新产品开发基金会(EFF)花了不到 25 万美元研制了一台计算机“Deep Crack”,以每秒测试 8.8×10^{10} 个密钥可能组合的速度,连续测试了 56 个小时,最终破译了 DES 密码。

4)DES 的改进

随着研究的深入,针对 DES 的缺陷,DES 算法在基本不改变加密强度的条件下,对 DES 进行了改进。

(1)DES 级联

DES 主要的密码学缺点就是密钥长度相对来说比较短。为了增加密钥长度,专家建议将一种分组密码进行级联,在不同的密钥作用下,连续多次对一组明文进行加密,通常把这种技术称为多重加密技术。对于 DES,也可以采用级联的方式来增加密钥长度以增强安全性。

在多重 DES 的级联方式的选择上,人们通常采用三重 DES。其基本原理是将 128 比特的密钥分为 64 比特的两组,对明文多次进行普通的 DES 加解密操作,从而增强加密强度。这种方法用两个密钥对明文进行三次加密。假设两个密钥是 k_1 和 k_2,三重 DES 的加密过程如下。

①使用密钥 k_1 进行第一次 DES 加密。

②用密钥 k_2 对第①步中 DES 加密的结果进行 DES 解密。

③将第②步中 DES 解密的结果再用密钥 k_1 进行 DES 加密。

三重 DES 是 DES 算法扩展其密钥长度的一种方法,可使加密密钥长度扩展到 128 比特(112 比特有效)或者 192 比特(168 比特有效)。这是密码学专家 Merkle 及 Hellman 推荐的方法,采用三重 DES 可以实现在不改变算法的基础上增加加密强度,减少因扩展加密强度而增加的各种开销。

(2)S 盒可选择的 DES 算法

Biham 和 Shamir 证明通过优化 S 盒的设计,甚至仅仅改变 S 盒本身的顺序,就可以抵抗差分密码分析,达到进一步增强 DES 算法加密强度的目的。

(3)具有独立子密钥的 DES

具有独立子密钥的 DES 是 DES 的另一种变形,在每轮迭代中都使用不同的子密钥,而不是由 56 比特密钥来产生子密钥。因为 16 轮 DES 的每轮都需要 48 比特密钥,所以这种变形的 DES 密钥长度是 768 比特,这一方法可以增强 DES 的加密强度,大大增强了破译 DES 密钥的难度。但是 Biham 和 Shamir 证明,利用 261 个选择明文便可破译这个 DES 变形,而不是原先所希望的 2 768 个选择明文,因此这种方法并不见得比 DES 更安全。

5) DES 的替代算法 AES

随着 DES 被破译的速度越来越快,DES 已经迫切需要被更新换代。1997 年 4 月 15 日,美国国家标准和技术研究院(NIST)发起征集高级加密标准 AES(Advanced Encryption Standard)算法的活动,并成立了 AES 工作组。其目的是确立一个非保密的、公开的、全球免费使用的加密算法,用于保护下一世纪政府的敏感信息,同时也希望能够成为秘密和公开部门的数据加密标准。1997 年 9 月 12 日, NIST 在联邦登记处(FR)公布了征集 AES 候选算法的通告。NIST 对 AES 候选算法有 3 条基本要求。

①对称密码体制。

②算法应为分组密码算法。

③算法明密文分组长度为 128 比特,应支持 128 比特、192 比特以及 256 比特的密钥长度。

1998 年 8 月 20 日,NIST 召开了第一次 AES 候选会议并公布了 15 个候选者。经过多次评测,NIST 选择了 Rijndael 算法。这种算法的两位设计者为国际质子中心的比利时密码专家 Joan Daemen 博士和 Vincent Rijmen 博士。

NIST 的 AES 标准选择小组撰写了有关 AES 的开发报告,这是一个综合的涉及面很广的报告。报告中对于各种有关 AES 的版本进行探讨,罗列了一些分析和评论。报告中提出了 Rijndael 算法的各种独特优点:Rijndael 在无论有无反馈模式的计算环境下的硬、软件中都能显示出非常好的性能;它的密钥安装时间很短,并具有很好的灵敏度;Rijndael 对内存容量需求非常低,因而适用于很多受限环境中;Rijndael 操作简单,并可抵御强大和实时的攻击;Rijndael 在数据块和密钥长度的设计上也很灵活,算法可提供不同的迭代次数;从全方位来考虑,Rijndael 汇聚了安全、性能好、效率高、易用和灵活等优点,使它成为 AES 密码体制最合适的选择。

2.1.2 非对称密码系统

非对称密码系统又称公开密钥密码系统。公开密钥密码系统(简称公钥体制)是现代密码学最重要的发明和进展。一般理解密码学就是保护信息传递的机密性,但这仅仅是当今密码学主题的一个方面,对信息发送和接收人的真实身份的验证、对所发送/接收信息在事后的不可抵赖以及保障数据的完整性是现代密码学主题的另一个方面。公开密钥密码系统对这两个方面的问题都给出了出色的答案。公开密钥密码学的概念由 Diffie 和 Hellman 于 1976 年提出,公开密钥密码体制最大的特点是采用两个不同的加密密钥和解密密钥,加密密钥公开,解密密钥保密,其他人无法从加密密钥和明文中获得解密密钥的任何消息,于是通信双方无须交换密钥就可以进行保密通信。自 1976 年以来,各种各样的公开密钥密码算法被提了出来。这些公开密钥密码算法都是建立在一定的数学基础之上的,按其建立的数学基础来分,这些经受住密码分析学家长时间分析检验的公钥算法可以分成三类:建立在大整数素因子分解基础上(如 RSA)、建立在有限域的离散对数问题上(如 ELGamal)以及建立在椭圆曲线之上(ECC)。将离散对数和素因子分解问题结合起来,又可以产生同时基于离散

对数和素因子分解难题的公钥算法。还有一种素因子分解的特殊情况,就是数学中的二次剩余难题,基于二次剩余问题可以设计多种公钥算法。

1)RSA 密码系统

私钥密码系统要求保密通信双方使用的密钥是通过秘密信道传送的。将私钥密码系统用于大量用户的网络通信会给密钥的管理和更换带来极大不便。例如,若有 n 个网络用户需要作两两保密通信,则需要 $C(n,2)=n(n-1)/2$ 个密钥,当 $n=1\ 000$ 时,$C(1\ 000,2)\approx 500\ 000$。这表明每个用户必须保存、牢记与其他 $n-1$ 个用户通信所需的密钥,显然是很不安全的。

美国斯坦福大学电子工程系的 Diffle 和 Hellman 于 1976 年在其论文《密码学的新方向》中提出了公钥密码的新思想:若用户 A 有一个加密密钥 k_a,一个解密密钥 k_b,k_a 公开而 k_b 保密,要求 k_a 的公开不能影响 k_b 的安全。若用户 B 要向用户 A 秘密地送去明文 m,则他查得 A 的公开密钥 k_a,并用 k_a 对 m 加密得密文 $c\equiv E_{k_a}(m)$;当 A 收到 c 后,使用只有 A 自己掌握的解密密钥 k_b 对 c 进行解密恢复出明文 $m\equiv D_{k_b}(c)$。

一年之后,麻省理工学院三位博士 Rivest, Shamir 和 Adleman 受 Diffle 和 Hellman 公钥密码思想的启发,设计了以他们姓名命名的 RSA 公开密钥密码算法。RSA 算法的关键思想是利用了将两个大素数相乘生成一个合数很容易,但要把一个大合数分解还原为两个素数却十分困难的事实。

假设要传送的明文为 m,那么可以将 RSA 密码算法描述如下。

(1)密钥的生成

①任选两个秘密的大素数 p 与 q。

②计算 n,使得 $n=p\times q$ 并且 $n>m$,然后公开 n。

③选择正整数 e,使得 e 与 $\psi(n)=(p-1)(q-1)$ 互素,公开 e,n 和 e 便是用户的公钥。

④计算 d,使 $e\times d \bmod \psi(n)=1$,$d$ 保密,d 便是用户的私钥。

(2)加密过程

$c=E(m)\equiv m^e \bmod n$,c 是对应于明文 m 的密文。

(3)解密过程

$m=D(c)\equiv c^d \bmod n$,m 是对应于密文 c 的明文。

关于 RSA 密码算法的安全性,从算法可知,若 $n=p\times q$ 被因子分解成功,则非常容易计算出私有密钥 d,从而可以攻破 RSA 密码系统。因此,我们必须非常注意 p、q 的选取。例如,从安全素数中选取 p、q,具有下列特点的素数 p、q 称为安全素数。

①p 和 q 的长度相差不大。

②$p-1$ 和 $q-1$ 有大素数因子。

③公因子$(p-1,q-1)$很小。

另外,由于某些特殊的值特别容易进行因子分解,因此还需要避开这些值以提高 RSA 算法的安全性。可以增强 RSA 安全性的另一种方法是加大密钥长度,不过这将导致计算量

的剧增。

因子分解是个不断发展的领域。自 RSA 算法发明以来,越来越有效的因子分解方法不断被发现,降低了破译 RSA 算法的难度。在 RSA 算法中,n 的长度是控制系统可靠性的重要因素。目前,大多数的应用系统采用 231、308 甚至 616 位的 RSA 算法。由于目前破解 RSA 密码系统的速度已经越来越快,因此专家建议采用 1 024 位的 RSA 算法。

下面举一个使用 RSA 密码进行加密、解密的例子。

【例 2.1】 用 RSA 密码算法对明文信息“public key encryptions”进行加密和还原。

第一步,假设选取素数 $p=43$ 和 $q=59$,则计算 $n=p\times q=43\times 59=2\ 537$,$\psi(n)=42\times 58=2\ 436$,并且选取 $e=13$,解同余方程 $e\times d \bmod 2\ 436=1$ 得到 $d=937$。

第二步,将明文“public key encryptions”以两个字符为一组进行分组,得到:

pu bl ic ke ye nc ry pt io ns

第三步,将明文数字化,用 00 表示 a,01 表示 b,02 表示 c,…,25 表示 z。这样将上述分组字符进行数字化成如下形式。

1 520 0 111 0 802 1 004 2 404 1 302 1 724 1 519 0 814 1 418

现在,讨论对明文数字 $m=1\ 520$ 的加密 $c=E(m)\equiv m^e(mod\ n)=1\ 520^{13}(\mathrm{mod}\ 2\ 537)=(1\ 520^2)^6\ 1520(\mathrm{mod}\ 2\ 537)$。

由于 $(1\ 520^2)\equiv 1\ 730(\mathrm{mod}\ 2\ 537)$,因此 $c\equiv(1\ 730)^6\ 1\ 520(\mathrm{mod}\ 2\ 537)=(1\ 730^2)^3\ 1\ 520(\mathrm{mod}\ 2\ 537)$。注意到 $1\ 730^2\equiv 1\ 777\ \mathrm{mod}(2\ 537)$,我们有 $c\equiv(1\ 777)^3\ 1\ 520(\mathrm{mod}\ 2\ 537)=(1\ 777)^2(1\ 777\times 1\ 520)(\mathrm{mod}\ 2\ 537)$。因为 $1\ 777^2\equiv 1\ 701\ \mathrm{mod}(2\ 537)$ 以及 $1\ 777\times 1\ 520\equiv 1\ 672(\mathrm{mod}\ 2\ 537)$,所以密文 $c\equiv 1\ 701\times 1\ 672(\mathrm{mod}\ 2\ 537)\equiv 95(\mathrm{mod}\ 2\ 537)=0\ 095$。

读者可以应用上述同样的过程求得其他数字明文对应的密文。对明文信息“public key encryptions”采用 RSA 密码算法加密后得到的密文序列为:

0 095 1 648 1 410 1 299 1 365 1 379 2 333 2 132 1 751 1 289

使用类似加密的方法可以进行 RSA 解密运算。对密文数字 $c=0\ 095$ 的解密过程为:

$$\begin{aligned} D(c) &\equiv c^d \bmod n \\ &\equiv 95^{937} \bmod 2\ 537 \\ &= 1\ 520 \end{aligned}$$

RSA 算法和 DES 算法各有优缺点。

①加、解密处理效率方面,DES 算法优于 RSA 算法。DES 算法的密钥长度只有 56 比特,可以利用软件和硬件实现高速处理;RSA 算法需要进行诸如至少 200 比特整数的乘幂和求模等多倍字长的处理,处理速度明显慢于 DES 算法。

②在密钥的管理方面,RSA 算法比 DES 算法更加优越。RSA 算法可公开分配加密密钥,对加密密钥的更新很方便。DES 算法要求通信前进行密钥分配,密钥的更换困难,对不同的通信对象,DES 需要产生和保管不同的密钥。

③在签名和认证方面,由于 RSA 算法采用公开密钥密码体制,因此能够很容易地进行数字签名和身份认证。

RSA 密码算法在许多系统(设备)中应用,例如,当时的诺基亚手机就采用了 RSA 密码系统。

2)椭圆曲线密码系统 ECC

1985 年,Koblitz 和 Miller 把椭圆曲线的研究成果应用到密码学中,分别独立提出在公钥密码系统中使用椭圆曲线的思想。他们虽没有发明出一种新的公钥密码算法,但他们采用椭圆曲线技术实现了已存在的密码算法如 Diffie-Hellman 算法等,这就是椭圆曲线密码学的开端。从提出椭圆曲线密码技术到 1995 年,人们对椭圆曲线密码技术的研究主要以理论为主。在这段时期,人们对椭圆曲线密码系统的安全性作了进一步的探讨;对椭圆曲线密码算法进行了初步的研究,提出了许多实现 ECC 操作的算法,其中对域和域操作算法的研究成果最为显著。1995 年以后,人们对椭圆曲线密码技术的研究开始偏重于应用方面。除了继续改善椭圆曲线密码算法的性能外,一些实验性的 ECC 系统已被实现,并且其性能也得到分析。从 1998 年起,一些国际化标准组织开始了研究椭圆曲线密码的标准化工作。1998 年年底美国国家标准与技术研究院(NIST)公布了专门针对椭圆曲线密码的 ANSI-F9. 62 和 ANSI-F9. 63 标准,1998 年,IEEE-P1363 工作组正式将椭圆曲线密码写入了当时正在讨论制订的“公钥密码标准”的草案中。

下面介绍 Weierstrass 方程和椭圆曲线的有关概念。

任意一条椭圆曲线都可以用一个三次方程来表示,这个三次方程一般称为 Weierstrass 方程。设 Weierstrass 方程为:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

方程中的参数取自域 F 上,F 可以是有理数域、实数域或者有限域 $GF(q^r)$。参数定义如下:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= b_2^3 - 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta
\end{aligned}$$

其中,Δ 称为 Weierstrass 方程(2. 1)的判别式。设 E 是由方程(2. 1)定义的曲线,当且仅当 $\Delta \neq 0$ 时 E 是光滑的,此时 Weierstrass 方程(2. 1)给出的曲线就是椭圆曲线。

定义 2. 1 设 F 是一个域,$\bar{F}$ 是 F 的代数闭域,$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$,$a_i \in \bar{F}$,定义椭圆曲线 $E(\bar{F})$ 为 $\bar{F}\times\bar{F}$ 上满足方程的点再加上一个无穷远点 O 所构成的集合,简记为 E。如果 $a_i \in \bar{F}$,则称椭圆曲线 E 定义在 F 上。

在密码系统中,我们比较关心的是有限域上的椭圆曲线。而有限域主要考虑素数域 F_p

和特征为 2 的域 F_{2^m}。有限域 F_q 的秩是此域中元素的个数。当 q 是素数时,便存在秩为 q 的有限域,用 F_q 表示。如果 $q=p^m$,p 是一个素数,m 为正整数,便称 p 为 F_q 的特征值,m 为 F_q 的扩充度(extension degree)。目前制订的大部分标准限制指定椭圆曲线密码技术只能使用单个素数($q=p$)的基本有限域或者特征值为 2($q=2^m$)的有限域。

椭圆曲线上的点在所定义的加法运算下形成一个阿贝尔群(Abelian group)。令 E 是由 Weierstrass 方程(2.1)给出的椭圆曲线,则 E 上的两点 P 和 Q 相加的加法法则如下:

对所有的 $P,Q\in E$,

①$O+P=P$ 并且 $P+O=P$,即 O 是恒元;

②$-O=O$;

③如果 $P=(x_1,y_1)\neq O$,那么 $-P=(x_1,-y_1-a_1x_1-a_3)$;

④$Q=-P$,那么 $P+Q=O$;

⑤如果 $P\neq O$,$Q\neq O$,$Q\neq -P$,令 R 是 PQ 连线($P\neq Q$ 时)交椭圆曲线 E 所得的另一交点,或曲线 E 在点 P 的切线($P=Q$ 时)交曲线 E 所得的另一交点,那么 $P+Q=-R$。

计算 $P+Q=-R$,称作计算点 P 和点 Q 的加法,计算点 P 加点 P,也称作计算 P 的倍点。定义在特征值为 2 的域和秩为素数的域上的椭圆曲线具有不同的方程,具有不同的加法和倍点公式。

令 P 和 Q 是椭圆曲线 E 上不同的两个有理点。则直线 PQ 必交曲线 E 于另一有理点 R。如果沿 x 轴作关于 R 的对称点,将得到另一个点(图 2.5),我们称该点为点 $P+Q=-R$。

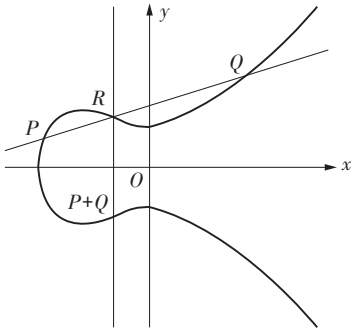

图 2.5　椭圆曲线上的加法操作

(1)定义在域 F_p 上的椭圆曲线加法公式

若椭圆曲线 E 定义在秩不为 2 和 3 的域 F_p 上,且 p 为素数,则曲线 E 的方程可简化如下。

$E:y^2=x^3+ax+b;a,b\in F_p$ 且 $4a^3+27b^2\neq 0(\bmod p)$。令 $P=(x_1,y_1)\in E$,那么 $-P=(x_1,-y_1)$。如果 $Q=(x_2,y_2)\in E$,$Q\neq -P$ 且 $P\neq Q$,那么 $P+Q=(x_3,y_3)\in E$,这里 x_1,y_1,x_2,y_2,x_3 和 y_3 有下列关系:

$$x_3=\lambda^2-x_1-x_2$$

$$y_3=\lambda(x_1-x_3)-y_1$$

其中

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

(2)定义在域 F_{2^m} 上的椭圆曲线加法公式

若曲线 E 是定义在特征值 $P=2$ 的域 $K=F_q(q=2^n$,整数 $n\geqslant 1)$ 上,则其加法公式的形式依赖曲线 E 的 j-不变量 $j(E)$ 分为 j-不变量为 0 和 j-不变量不为 0 两种情况。

①$j(E)\neq 0$ 时的加法公式。

令 $P=(x_1,y_1)\in E$,那么 $-P=(x_1,y_1+x_1)$。如果 $Q=(x_2,y_2)\in E$,$Q\neq -P$ 且 $P\neq Q$,那么 $P+Q=(x_3,y_3)\in E$,这里

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

其中

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}。$$

②$j(E)=0$(即 E 是超奇异椭圆曲线)时的加法公式。

令 $P=(x_1,y_1)\in E$,那么 $-P=(x_1,y_1+a_3)$。如果 $Q=(x_2,y_2)\in E$,$Q\neq -P$ 且 $P\neq Q$,那么 $P+Q=(x_3,y_3)\in E$,这里

$$x_3 = \lambda^2 + x_1 + x_2$$

$$y_3 = \lambda(x_1 + x_3) + y_1 + a_3$$

其中

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}。$$

下面,讨论椭圆曲线上的倍点公式。

为了计算点 P 加点 P,即 P 的倍点,过点 P 作椭圆曲线 E 的切线。因为 E 是由三次方程定义的,所以,切线必定与椭圆曲线 E 相交于且仅相交于另一点,我们称相交点为 R 点。作 R 点关于 x 轴的对称点得到椭圆曲线上的另一个点,即 P 的倍点,称该点为点 $[2]P=P+P$(图 2.6),为方便起见,常把"$[2]P$"写为"$2P$",即 $[2]P$ 可以表述为 $2P$。若过点 P 的椭圆曲线 E 的切线垂直于 x 轴,那么切线交椭圆曲线 E 于无穷远点,此时 $P+P=O$,也就是说点 P 是一个阶为 2 的点(P 点的阶为 2)。椭圆曲线选择的域类型不同,倍点公式也不一样。

(3)定义在域 F_p 上的椭圆曲线倍点公式

特征值 P 为素数的倍点公式定义如下。

令 $P=(x_1,y_1)\in E$,$Q=(x_2,y_2)\in E$,且 $P=Q$,那么 $P+Q=(x_3,y_3)$,这里

$$x_3 = \lambda^2 - 2\lambda,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

其中

$$\lambda = \frac{3x_1^2 + a}{2y_1}。$$

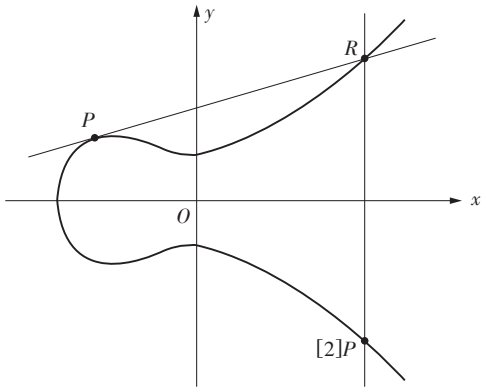

图 2.6　椭圆曲线上的倍点操作

(4)定义在域 F_{2^m} 上的椭圆曲线倍点公式

根据 j-不变量的不同,特征值为 2 的域有两种不同的倍点公式。

①$j(E)\neq 0$ 时的倍点公式。

令 $P=(x_1,y_1)\in E, Q=(x_2,y_2)\in E$,且 $P=Q$,那么 $P+Q=(x_3,y_3)$,这里 $x_3=\lambda^2+\lambda+a_4$, $y_3=(x_1+x_3)\lambda+x_3+y_1$,

其中

$$\lambda=\frac{y_1}{x_1}+x_1。$$

②$j(E)=0$(即 E 是超奇异椭圆曲线)时的倍点公式。

令 $P=(x_1,y_1)\in E, Q=(x_2,y_2)\in E$,且 $P=Q$,那么 $P+Q=(x_3,y_3)$,这里

$$x_3=\frac{x_1^4+a_4^2}{a_3^2},$$

$$y_3=\left(\frac{x_1^2+a_4}{a_3}\right)(x_1+x_3)+y_1+a_3。$$

椭圆曲线上的点乘(亦称数乘,scalar multiplication)操作是椭圆曲线密码系统的核心操作之一。椭圆曲线上的点乘操作定义为:给定一条椭圆曲线 E 和曲线上的一点 P,E 上的 P 点的点乘 xP 定义为点 P 与自身相加 x 次之和,即 $xP=P+P+\cdots+P$,共 x 个 P 相加。

椭圆曲线公钥密码系统的安全性依赖于椭圆曲线离散对数问题的计算困难性。

定义 2.2　设 G 是任一有限阿贝尔(加法)群,P 和 $Q\in G$ 为 G 的任意两点。如果已知存在整数 m,使 $Q=mP$,则如何由 P,Q 及 G 求出 m 的问题称为 G 上的离散对数问题。离散对数问题简记为 DLP(Discrete Logarithm Problem)。

定义 2.3　用 $E(K)$ 表示定义于有限域 F_q 上的椭圆曲线 E 在扩域 K 上的有理子群,P 和 $Q\in E(K)$ 为 $E(K)$ 的任意两点。且已知某个整数 m,有 $Q=mP$,则如何由 P,Q 及 E 求出 m 的问题称为 E 上的椭圆曲线离散对数问题。椭圆曲线离散对数问题简记为 ECDLP(Elliptic Curve Discrete Logarithm Problem)。

在椭圆曲线公钥密码系统中,密文不仅依赖于待加密的明文,而且依赖于一个随机数 k,所以,即使加密相同的明文,由于随机数不同,因此得到的密文也不同。由于这种加密体制的不确定性,因此又称为概率加密体制,它可以有效抵抗已知明文攻击。

就椭圆曲线密码来说,各种椭圆曲线密码体制的安全性都与求解相应曲线离散对数问题的困难性等价。目前针对 ECDLP 的求解方法主要有以下 3 种。

①针对一般 DLP 的 Pollard-ρ 方法以及依据椭圆曲线特殊性的改进方法。

②针对超奇异曲线的 MOV 演化算法。

③针对"畸形"曲线(Anomolus Curve)的 Smart 方法或 Semaev 方法。

到目前为止,对一般离散对数问题的求解仍没有很好的办法。假设离散对数问题所基于有限群的阶中的最大素因子是 n,则目前最好的求解方法(即 Pollard-ρ 方法)的时间复杂度是 $O\left(\sqrt{\frac{\pi n}{2}}\right)$。为避免这种攻击,椭圆曲线上有理点的数量要可以被一个足够大的素数 n 整除,ANSI X9.62 要求 $n>2^{160}$,当确定一个有限域 F_q 后,应选择尽量大的 n。还必须指出,人们对基于两类特殊的曲线上的 ECDLP 已经找到了有效的求解方法。这两类曲线的一类是"超奇异"型曲线,另一类是"畸形"曲线。在实际应用中,应避免选用这两类曲线。

20 世纪 80 年代中期,一系列针对公钥密码系统应建立在椭圆曲线应用上的建议被提出。宏观上看,可以认为 ECC 是建立在椭圆曲线而非有限域上的公钥系统。这样,不论 RSA 还是 DSA 算法,都可以将其在椭圆曲线上实现。这具有更加诱人的现实意义,如果一种广泛使用的密码算法(比如 RSA)被淘汰,那么只要将其建立的数学基础——大素数分解改为椭圆曲线,则原来的系统就又可以继承重用了。从这个角度出发,可以说椭圆曲线密码系统并非新建了一种完全不同的密码体制,这样的系统安全性得到了保证而且没有增加系统的额外开销。因而,建立在有限域离散对数机制上的密码系统和建立在椭圆曲线上的密码系统可以被认为与其数学基础相关,它们均建立在解离散对数问题的难度上。椭圆曲线的独特之处在于提供了由"元素"和"组合规则"来组成群的构造方式。用这些群来构造密码算法,密钥长度减小、算法速度加快、存储空间占用减少,却没有减少密码分析的分析量,甚至非超奇异椭圆曲线离散对数问题的难度远远超过了有限域上离散对数问题的难度。

表 2.1 列出了 RSA、ECC 和 DSA 3 种公钥密码算法在安全强度相同情况下的密钥长度及系统参数的长度;图 2.7 对它们的密钥长度及密钥相应攻破时间进行了比较。可见,在安全强度相同情况下,ECC 算法所使用的密钥长度最短,这使得 ECC 算法的执行速度更快、占用存储空间更小、效率更高。并且当加密短消息时,ECC 算法所占用的带宽最小。这些优点使得 ECC 算法相对于其他公钥算法更具有竞争力。

表 2.1　密钥及系统参数长度表

密码算法	公钥长度/bit	私钥长度/bit	系统参数长度/bit
RSA	1 088	2 048	*n/a*
DSA	1 024	160	2 208

续表

密码算法	公钥长度/bit	私钥长度/bit	系统参数长度/bit
ECC	161	160	481

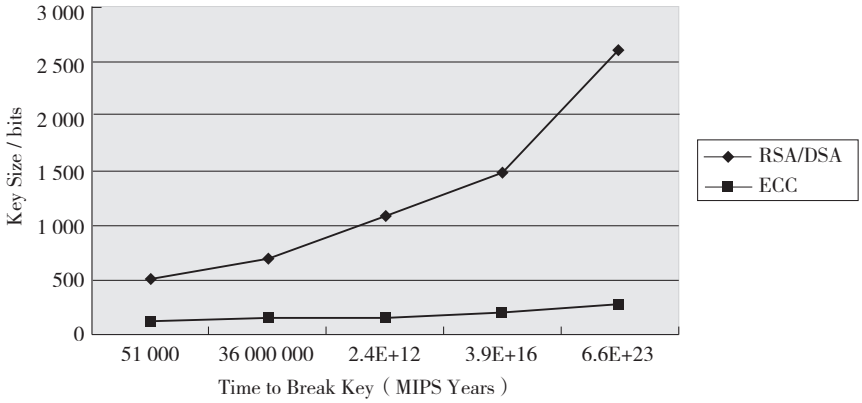

图 2.7　RSA/DSA 算法和 ECC 算法的难度比较

2.2　中国国家商用密码算法

为了保障中国商用密码的安全性,国内相关机构制定了一系列密码标准,包括 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法(ZUC)等。其中“SM”代表“商密”,即用于商用的、不涉及国家秘密的密码技术。

其中最基础最重要的是 SM4、SM3、SM2。SM4 为分组密码算法,用于替代 DES/AES 等算法,SM3 为 Hash(散列,杂凑)算法,用于替代 MD5/SHA-1/SHA-256 等算法,SM2 为基于 ECC 的公钥密码算法,包含数字签名、密钥交换和加解密,用于替换 RSA/Diffie-Hellman 等算法,它们共同构成了我国商用密码(简称国密算法)的基础架构。

2.2.1　SM4 算法

为配合我国 WAPI 无线局域网标准的推广应用,SM4 于 2006 年公开发布,2012 年 3 月成为中国国家密码行业标准(GM/T 0002—2012),2016 年 8 月成为中国国家标准(GB/T 32907—2016),2021 年 6 月,SM4 作为 ISO/IEC 18033—3:2010/AMD1:2021《信息技术 安全技术 加密算法 第 3 部分:分组密码 补篇 1:SM4》发布,正式成为国际标准。

SM4 密码算法是一个分组算法。该算法的分组长度为 128 比特,密钥长度也为 128 比特。加密算法与密钥扩展算法均采用非线性迭代结构,运算轮数均为 32 轮。数据解密和数据加密的算法结构相同,只是轮密钥的使用顺序相反。

SM4 分组密码算法主要包括加密算法、解密算法以及密钥的扩展算法 3 部分。