密码学技术的发展与网络安全研究

丁子康, 黄　锐, 杨鸿靖宇
（中国计量大学, 浙江　杭州　310018）

摘　要: 随着计算机技术的飞速发展, 信息网络已经成为社会发展的重要保证。而密码学技术是网络信息安全的核心技术手段。文章主要介绍了密码学的发展历程和现存的网络安全问题以及最新的密码学技术在网络安全中的运用。

关键词: 密码学发展历程; 网络安全问题; 现代密码学技术的应用

互联网发展已经有多年的历史，我国的互联网发展相对比较晚，虽然如此，但是随着社会的发展与进步以及网络安全全球化的发展趋势，我国的网络安全也得到了长足的发展，对于网络安全的需求也有迅猛的增长，特别是近几年来，随着我国的政府和企业信息化建设步伐的加快，网络安全问题日益突出，逐渐成为社会热点问题，促使整个网络安全行业在不断地进行革新和创新，满足了广大人民群众对于具有时代特色的安全产品的需求，也进一步促进了网络安全技术的发展。

密码指的是按照一定规则编译而成的符号，研究密码的学科就是密码学。密码学技术，是一项年代比较久远的信息编译传输技术，它的运用使网络信息安全得到了极大的提高，也是网络安全的核心基础技术[1]。它包括了密码编码与密码破译两个部分，用马克思主义哲学的理论来解释那就是对立统一的关系，正是如此才推动了密码学持续、长久的发展。

1　网络安全问题

网络安全是指网络系统中的硬件和软件及其系统中的数据受到保护，不因偶然或恶意的原因遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网路安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科交叉的综合性学科。网络安全从本质上来说就是网络上的信息安全[2]。从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性、可靠性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

信息保密性是指信息不被泄露给非授权的个人和实体，或供其使用的特性。信息的保密性包括文件的保密性、传输过程中的保密性两个方面。

（1）信息完整性是指信息在存储或传输时不被修改、破坏、插入，不延迟、不乱序和不丢失的特性。

（2）信息可用性是指信息可被合法用户访问并能按要求顺序使用的特性。

（3）信息真实性是指信息反映和描述客观世界及其变化的准确程度。

（4）信息可控性是指授权机关可以随时控制信息的机密性。每一个用户只能访问自己被授权访问的信息。同时对系统中可利用的信息及资源也要进行相应地分级, 确保信息的可控性。

（5）信息的可靠性是指以用户认可的质量连续服务于用户的特性。这不仅是要保证信息的安全可靠, 还和信息系统本身的可靠性有关。

以上特性的存在，网络信息安全问题随之产生，网络黑客利用这些特性用中断、截获、修改和伪造4种方式进行网络攻击。

在当前互联网和大数据高速发展的阶段，网络安全涉及硬件、软件、数据、服务等方方面面的内容，所以网络安全问题是不容忽视的。技术是核心，要通过核心技术的突破，构建起整个国家的信息安全技术防范体系。管理是关键，政府通过网络安全制度的制定与建立，形成一套完整的制度体系，同时还要加强宣传、教育和提高整个社会的网络信息安全观[3]。

2　密码学的发展历程

密码学到现在为止经历了3个发展阶段：古典密码学、近代密码学、现代密码学。

2.1　古典密码学

古典密码学是密码学发展的基础与起源，比如历史上第一个密码技术——恺撒密码，还有后面的掩格密码等。虽然大都比较简单但对于今天的密码学发展仍然具有参考价值。

2.2　近代密码学

近代密码学开始于通信的机械化与电气化，为密码的加密技术提供了前提，也为破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来前所未有的自由，他们可以利用电子计算机设计出更为复杂、保密的密码系统。

2.3　现代密码学

之前的古典密码学和近代密码学，都是现代人给予的定义，其研究算不上真正意义上的一门科学。直到1949年香农发表了一篇名为“保密系统的通信理论”的著名论文，该文将信息论引入密码，奠定了密码学的理论基础，开启了现代密码学时代。

由于受历史的局限，20世纪70年代中期以前的密码学研究基本上是秘密进行，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应用是从70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，给这门学科以巨大的生命力[4]。

1976年，美国密码学家迪菲和赫尔曼在“密码学的新方向”一文中提出了一个崭新的思想，不仅加密算法本身可以

作者简介: 丁子康（1997— ），男，浙江金华人，本科生；研究方向：网络安全。

公开，甚至加密用的密钥也可以公开，但这并不意味着保密程度的降低，因为加密密钥和解密密钥不一样，将解密密钥保密就可以，这就是著名的公钥密码体制。若存在这样的公钥体制，都可以将加密密钥像电话簿一样公开，任何用户想经其他用户传送一加密信息时，都可以从这本密钥薄中查到该用户的公开密钥，用它来加密，而接收者能用只有它所具有的解密密钥得到明文，任何第三者不能获得明文。1978年，美国麻省理工学院的里维斯特、沙米尔和阿德曼[5]提出了RSA公钥密码体制，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。

在现代密码学中，除了信息保密外，还有另一方面的要求，即信息安全体制还要能抵抗对手的主动攻击。所谓主动攻击指的是攻击者可以在信息通道中注入自己伪造的消息，以骗取合法接收者的相信。主动攻击可能窜改信息，也可能冒名顶替，这就产生了现代密码学中的认证体制。该体制的目的就是保证用户收到一个信息时，能验证消息是否来自合法发送者，同时还能验证该信息是否被窜改。在许多场合中，如电子汇款，能对抗主动攻击的认证体制甚至比信息保密还重要。

3 现代密码学新技术的应用

（1）代理密码学：包括代理签名和代理密码系统，两者都是代理功能。

（2）在线/离线密码学：将一个密码体制分为在线执行阶段和离线执行阶段两个阶段。在线执行阶段执行低计算量的工作，离线执行阶段可预先执行耗时较多的计算。

（3）密钥托管系统：为满足用户之间保密通信以及政府对群众用的有效监控所建立的系统。对于密钥托管系统而言，其核心是构造一个法律强制访问域（Law Enforcement Access Field，LEAF），即被通信加密和存储的额外信息块，用来保证合法的政府实体或者被授权的第三方获得通信的明文消息。为了更趋向合理化，可将已经密钥分成一些密钥碎片，用不同的密钥托管代理的公钥加密，再将加密的密钥碎片通过门限化的方法合成。

（4）圆锥曲线密码学：在圆锥曲线群上的编码和解码很容易执行，还可以建立模n的圆锥曲线群，构造等价与大整数分解的密码。圆锥曲线群上的离散对数问题在圆锥曲线的阶和椭圆曲线的阶相同的情况下，是一个不比椭圆曲线容易的问题。圆锥曲线密码学已经成为密码学中的一个重要研究内容。

（5）基于身份的密码学：Shamir在提出基于身份的公钥密码概念的同时，也给出了基于身份的签名方案，2001年，Boneh和Franklin提出了第一个实用基于身份的加密方案，该方案使用了双线性映射，并基于随即预言机模型证明了安全性。不过ROM是一个理想模型，基于ROM的安全并不一定意味着真实的世界安全，密码学家们有基于标准模型的基于身份密码方案[6]。

（6）多方密钥协商问题：密钥协商问题是密码学中又一基本问题。Diffie-Hellman协议是一个众所周知的，在不安全的信道上通过交换消息来建立会密钥的协议。它的安全性基于Diffie-Hellman离散对数问题。然而，Diffie-Hellman协议的主要问题是它不能抵抗中间人攻击，不能提供用户身份验证。当前已有的密钥协商协议包括双方密钥协商协议、双方非交互式的静态密钥协商协议、双方一轮密钥协商协议、双方可验证身份的密钥协商协议以及三方相对应类型的协议。

4 结语

互联网的飞速发展导致了信息数据的爆炸式增长，大数据时代已经到来，如何确保数据信息安全早已经是整个社会所追求的。密码学技术是核心技术之一，然而仅仅靠密码技术并不能彻底地解决这个问题，它涉及了人、技术、管理和操作等多方面因素。安全系统防御等级遵循“木桶效应”，取决于最薄弱环节。要将密码学建立成一个完整的科学的体系，是将来的发展方向。强化密码学科建设，完善密码专业规范，培养数量充足、质量优良的密码人才，强化密码意识和密码思维教育等都是未来需要做的，这样才能实现网络强国、保障网络安全。习近平总书记指出，没有网络安全，就没有国家安全。网络安全是维护国家安全的战略制高点，必须发展自主可控的关键核心技术，壮大网络安全人才队伍。“网络空间的竞争，归根结底是人才的竞争”。在这个不学会在信息空间中生存就将被淘汰的时代，密码人才必将在国产自主可控信息化建设过程中为信息化保驾护航，发挥中流砥柱的重要作用。

[参考文献]

[1]杜明泽.密码学的研究与发展综述[J].中国科技信息，2010（24）：32-34.

[2]汤惟.密码学与网络安全技术基础[M].北京：机械工业出版社，2004.

[3]冯国登.国内外密码学研究现状与发展趋势[J].通信学报，2002（5）：18-26.

[4]李书晋.浅谈当前计算机网络安全应用问题及防范策略[J].计算机光盘软件与应用，2004（10）：183-184.

[5]耿芸.计算机网络安全中的密码技术研究及其应用[J].决策与信息，2016（5）：265.

[6]周霞.信息安全现状及发展趋势[J].大众科技，2006（7）：85-86.

Development of cryptography technology and network security research

Ding Zikang, Huang Rui, Yanghongjingyu
（China Jiliang University, Hangzhou 310018, China）

Abstract: With the rapid development of computer technology, information networks have become an important guarantee for social development. And cryptography technology is the core technical means of network information security. This paper mainly introduces the development of cryptography and existing network security issues and the application of the latest cryptography technology in network security.

Key words: cryptography development history; network security issues; application of modern cryptography