DOI:10.19981/j.CN23-1581/G3.2025.16.039

数据加密技术在网络数据传输中的应用

霍莉莉
(太原城市职业技术学院,太原 030027)

摘 要:为增强网络数据传输的安全性,探讨数据加密技术的实际应用效果,该文报告数据加密技术的基本概念与主要类型,包括对称加密、非对称加密及混合加密,详细分析 AES、DES、RSA 和 ECC 等加密算法的选择与实现流程,同时研究数据加密技术在网络数据传输中面临的挑战,提出相应的解决方案。结果表明,数据加密技术能够有效保护数据的安全性和隐私性,但存在算法复杂度和跨平台兼容性问题,以及面临量子计算威胁和传统算法安全性降低等挑战,通过采用混合加密技术和优化密钥管理策略,可以提高数据加密技术的效率和安全性。说明数据加密技术是网络数据传输中不可或缺的安全手段,建议不断优化加密算法和技术,构建多层次安全防护体系,以应对日益复杂多变的网络安全威胁。

关键词:数据加密技术;网络安全;数据传输;实践应用;加密算法
中图分类号:TP399 **文献标志码**:A **文章编号**:2095-2945(2025)16-0168-04

Abstract: In order to enhance the security of network data transmission and discuss the practical application effect of data encryption technology. This paper reports the basic concepts and main types of data encryption technology, including symmetric encryption, asymmetric encryption and hybrid encryption, and analyzes in detail the selection and implementation process of encryption algorithms such as AES, DES, RSA, and ECC. At the same time, it studies the application of data encryption technology in network data transmission. Challenges faced and proposed corresponding solutions. The results show that data encryption technology can effectively protect the security and privacy of data, but there are problems of algorithm complexity and cross-platform compatibility, as well as challenges such as quantum computing threats and reduced security of traditional algorithms. By adopting hybrid encryption technology and optimizing Key management strategies can improve the efficiency and security of data encryption technology. It explains that data encryption technology is an indispensable security means in network data transmission. It is recommended to continuously optimize encryption algorithms and technologies and build a multi-level security protection system to deal with increasingly complex and ever-changing network security threats.

Keywords: data encryption technology; network security; data transmission; practical application; encryption algorithm

信息化时代背景下,网络数据传输已成为人们日常生活和工作中不可或缺的一部分,无论是电子商务交易、企业内部数据传输,还是政务信息交换、用户隐私保护,都离不开网络数据的传送与接收,但网络环境的开放性和复杂性使得数据传输过程中面临着诸多安全威胁。因此,如何保障网络数据传输的安全性成为了亟待解决的问题,而数据加密技术作为一种有效的安全手段,通过对数据进行加密处理,确保只有授权用户才能访问和解读数据,能够有效保护数据的安全性和隐私性。

1 数据加密技术概述

1.1 数据加密技术的基本概念

数据加密技术通过对原始数据进行一系列复杂的数学运算或逻辑处理,将明文数据转换为难以被直接解读的密文形式,从而确保数据在传输或存储过程中的安全性和隐私性。该技术的核心概念在于“加密”和“解密”2 个过程。加密是指利用特定的加密算法和密钥,将明文数据转换为密文的过程,这个过程中,算法是加密操作的规则和方法,而密钥则是控制加密和解密过程的秘密数字序列;解密则是加密的逆过程,

作者简介:霍莉莉(1989-),女,硕士,助教。研究方向为软件技术,信息安全技术。

即使用相同的算法和密钥,将密文还原为明文。

1.2 数据加密技术的主要类型

1.2.1 对称加密技术

对称加密技术,又称为单密钥加密或共享密钥加密,是数据加密技术中最基础也是应用最广泛的一种。在对称加密中,加密和解密过程使用相同的密钥,数据的发送方和接收方需要共享这个密钥。该技术的优点在于其加密和解密速度快,适合对大量数据进行加密处理,且算法相对简单,易于实现,但对称加密的缺陷在于密钥的分发和管理问题。

1.2.2 非对称加密技术

非对称加密技术,也称为公钥加密或双密钥加密,属于对称加密技术的重要补充。在非对称加密中,每个用户都拥有一对密钥:公钥和私钥。公钥用于加密数据,而私钥则用于解密数据,公钥可以公开分发给任何人,而私钥则必须严格保密。非对称加密技术的最大优势在于其解决了密钥分发的问题,由于公钥可以公开,因此不需要像对称加密那样担心密钥的泄露。

1.2.3 混合加密技术

混合加密技术,是将对称密钥体系与非对称密钥体系的优势互补,实现高效与安全并重的一种技术途径。在对称加密机制下,加密与解密采用同一密钥,确保了加密操作的高速与高效,尤其适用于大规模数据的加密通信。但对称加密面临的挑战在于密钥的分发与保护,一旦密钥外泄,整个系统的安全性将面临重大风险。相比之下非对称加密体系采用公钥-私钥对,公钥负责加密,私钥负责解密,巧妙解决了密钥分配难题,但其加密解密流程相对繁琐,效率不及对称加密。

2 数据加密技术在网络数据传输中的具体实现

2.1 加密算法的选择与实现

2.1.1 AES 与 DES 对称加密算法

AES 算法被广泛应用于各种安全协议和系统中,其采用分组加密的方式,每个分组长度为 128 位,并且支持 128 位、192 位和 256 位 3 种密钥长度。在实现上,AES 算法通过多轮的非线性变换和密钥扩展,确保了加密的复杂性和安全性,同时由于其高效的加密速度,AES 算法非常适合于对大量数据进行加密处理,如网络通信、文件存储等场景。

DES 算法是早期的对称加密算法,采用 56 位密钥对 64 位数据块进行加密,通过 16 轮的置换和替换操作实现加密过程,尽管 DES 算法的安全性相对较低,但其实现简单、速度快,适用于对加密强度要求不高、数据量较小的场景。

2.1.2 RSA 与 ECC 非对称加密算法

RSA 算法是非对称加密领域的经典之作,广泛应用于数字签名、密钥交换等安全协议中。在实现上,RSA 算法使用公钥进行加密,私钥进行解密,确保了数据的安全传输。同时,RSA 算法还支持数字签名功能,可以验证数据的完整性和发送者的身份。

ECC 算法与 RSA 算法相比,ECC 算法在提供相同安全性的前提下,所需的密钥长度更短,计算量更小,因此加密和解密速度更快。这让 ECC 算法在资源受限的环境中,如移动设备、物联网设备等,具有显著的优势,另外 ECC 算法还支持更高效的数字签名和密钥交换协议,为网络安全提供了更强的保障。

2.2 加密技术的实现流程

2.2.1 加密前的准备工作

加密前的准备工作是加密技术实施的基础,其确保后续加密过程的有效性和安全性。具体而言包含以下几个关键步骤。

第一,明确加密需求。全面分析数据的性质、传输方式、存储要求以及潜在的安全威胁,从而确定加密的具体目标、范围和安全级别。这一步是后续工作的指导,确保加密措施能够精准地满足实际需求。第二,选择加密算法。基于加密需求,综合考虑算法的安全性、效率、兼容性以及实现难度,选择最适合的加密算法。对称加密算法(如 AES、DES)适用于大量数据的快速加密,非对称加密算法(如 RSA、ECC)则更适合于密钥交换和数字签名等场景。第三,生成与管理密钥。密钥是加密技术的核心,其安全性直接关系到加密系统的整体安全。对于对称加密,需生成一个强随机数作为密钥;对于非对称加密,则需生成一对公钥和私钥,同时需建立有效的密钥管理机制,确保密钥的安全存储、分发和更新,防止密钥泄露或被恶意利用。第四,配置加密环境。根据所选算法和密钥,配置加密软件、硬件及网络环境,包括安装加密库、设置加密参数、配置安全策略等,确保加密过程能够在安全、稳定的环境中进行。

2.2.2 加密过程

加密过程是将明文数据转换为密文的过程,其确

保数据在传输和存储过程中不被未经授权的人员读取或篡改。加密过程包含以下几个步骤。

第一,数据输入。将待加密的明文数据输入加密系统。这些数据可能来自文件、数据库、网络传输等多种来源,需确保输入数据的准确性和完整性。第二,加密操作。利用选定的加密算法和密钥,对输入数据进行加密处理。加密操作通常涉及数据分组、替换、置换、异或等复杂运算,以确保密文的难以解读性。具体加密过程需严格按照算法规范进行,确保加密的强度和效果。第三,密文输出。将加密后的密文数据输出到指定的存储介质或传输通道。在输出过程中,需采取额外的安全措施,如加密传输协议、数据完整性校验等,以确保密文在传输过程中的安全性和完整性。

2.2.3 解密过程

第一,密文输入。将接收到的密文数据输入解密系统。这些密文通常来自网络传输、文件存储等渠道,需确保输入密文的准确性和完整性。第二,解密操作。利用加密时使用的算法和密钥,对输入的密文进行解密处理,解密操作是加密操作的逆运算,通过相应的数学运算和逻辑处理,将密文还原为原始的明文数据。第三,明文输出。将解密后的明文数据输出到指定的应用系统中或呈现给用户。在输出过程中,需确保解密环境的安全性和稳定性,防止数据被恶意篡改或泄露。图 1 为机构与普通方之间通过公钥、私钥、AES 加密及 RSA 签名实现的安全通信流程,整个流程分为 2 个主要部分:机构向普通方发送密文,以及普通方向机构发送密文。

如图 1 所示,机构与普通方之间的安全通信流程包含 2 个主要方向。在机构向普通方发送密文的流程中,机构首先接收普通方提供的公钥,并生成一个随机的 AES 密钥,机构使用这个 AES 密钥对要发送的消息进行加密,得到 AES 密文。同时,机构还使用自己的私钥对 AES 密文进行 RSA 签名,以确保数据的完整性和来源的真实性,随后机构将 AES 密文、原始消息的 RSA 签名以及机构自身的公钥组合成报文,并通过 HTTPS 请求发送给普通方,普通方在接收到报文后,首先使用机构提供的公钥验证 RSA 签名的合法性,确认消息未被篡改,最后普通方使用自己的私钥解密 AES 密文,得到机构发送的原始消息。

相反地,在普通方向机构发送密文的流程中,普通方首先生成一个随机的 AES 密钥,并使用机构的公钥对这个 AES 密钥进行加密,得到 AES 密文。普通方使用 AES 密钥对要发送的消息进行加密,得到 message 密文,普通方可能将 AES 密文、message 密文以及可能的签名组合成报文,并发送给机构。机构在接收到报文后,使用自己的私钥解密 AES 密文,得到 AES 密钥明文。最后机构使用 AES 密钥明文解密 message 密文,得到普通方发送的原始消息。这 2 个流程共同确保了机构与普通方之间数据的安全交换。

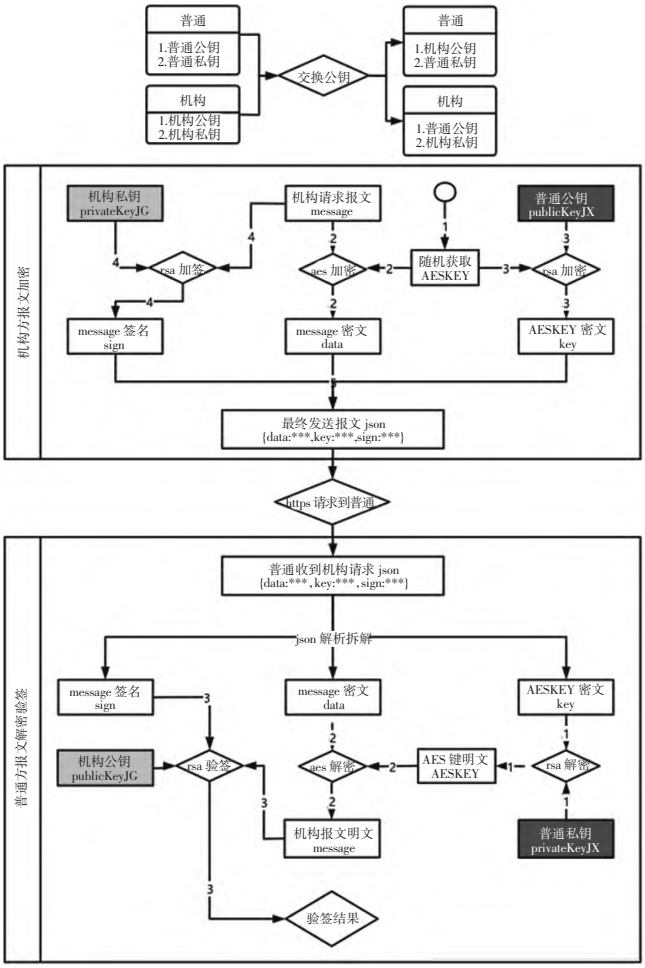

图 1 AES RSA 加解密流程

2.3 加密技术的优化与改进

2.3.1 提高加密效率的方法

首先,优化加密算法的实现是提升加密效率的关键,通过对加密算法进行深入研究,找出算法中的瓶颈和冗余部分,进行针对性的优化,可以显著提高加密速度。其次,现代处理器和专用加密芯片提供了强大的加密运算能力,通过合理利用这些硬件资源,可以大幅提升加密操作的执行速度。最后,还可以采用并行加密技术,将加密任务分割成多个子任务,在多个处理器或核心上并行执行,从而进一步缩短加密时间。

2.3.2 增强加密安全性的策略

为了提升加密系统的安全性，需要采取一系列策略。首先，选择强度更高的加密算法是基础，及时采用更加先进的加密算法，可以有效提升加密系统的抗攻击能力。其次，加强密钥管理是增强加密安全性的关键，因此需建立严格的密钥管理制度，确保密钥的生成、存储、分发和销毁等环节都符合安全规范。再次，采用多层加密、混合加密等策略，通过增加加密层次和复杂度，提高破解加密系统的难度。最后，定期对加密系统进行安全评估和漏洞扫描，及时发现并修复潜在的安全漏洞，也是增强加密安全性的重要措施。

3 数据加密技术在网络数据传输中面临的挑战与解决方案

3.1 加密技术的局限性

一方面，在追求高强度加密的同时，算法的高计算复杂度成为了制约加密效率的关键因素，特别是在大数据和高速数据传输场景下，加密和解密过程所需的时间和计算资源成为不可忽视的性能瓶颈。为了缓解这一问题，应尽快开发更加高效的加密算法，采用并行处理、硬件加速等技术手段，以在不牺牲安全性的前提下提升加密性能。另一方面，不同系统、设备和平台间对加密算法和协议的支持存在差异，导致数据在跨平台传输时可能出现解密失败或效率低下的问题。解决这一问题的关键在于推动加密技术的标准化进程，确保不同系统间的兼容性和互操作性，促进数据加密技术的广泛应用和普及。

3.2 加密技术的安全性

第一，随着密码学研究的深入和计算能力的提升，一些传统加密算法的安全性正面临严峻挑战，特别是量子计算技术的快速发展，可能对基于经典数学难题的加密算法构成根本性威胁。第二，密钥作为加密技术的核心，其管理不善或协议设计缺陷将直接导致数据安全的脆弱性，加强密钥的全生命周期管理，包括安全生成、存储、分发、更新和销毁，是确保数据安全的关键。同时对加密协议进行严格的审查和测试，及时发现并修复潜在的安全漏洞。第三，除了技术层面的安全威胁外，社会工程学攻击也是数据加密技术必须面对的挑战，攻击者可能通过欺骗、诱导等心理战术获取用户的敏感信息或访问权限。对此应当加强用户的安全教育和培训，提高用户的安全意识和防范能力。

3.3 解决方案与未来发展方向

首先，在算法层面，开发能够抵御量子计算威胁的后量子加密算法，以及针对特定应用场景优化的专用加密算法；利用硬件加速技术，如 GPU 并行计算、ASIC 芯片等，可以显著提升加密和解密的速度，降低计算资源的消耗。通过算法的可配置性设计，让加密算法能够根据实际应用场景的需求进行灵活调整，以达到性能与安全性的最佳平衡。其次，必须建立严格的密钥生命周期管理机制，包括密钥的安全生成、存储、分发、更新以及销毁等全过程。采用多因素认证、密钥分片、硬件安全模块（HSM）等技术手段，有效增强密钥的安全性，同时对加密协议进行定期的审查和更新，确保协议能够抵御新出现的安全威胁。

4 结束语

综上所述，数据加密技术作为信息安全领域的核心支撑，其通过复杂的算法和严谨的实现流程，为数据的机密性、完整性和可用性构筑了坚实的防线，从对称加密到非对称加密，每一种加密算法都在特定的应用场景中发挥着不可替代的作用。但也应当认识到，随着计算能力的提升、攻击手段的不断演变，数据加密技术同样需要不断创新，研发出更加高效、安全、易用的加密算法和技术，以应对日益复杂多变的网络安全威胁。

参考文献：

[1] 周杨堃.数据加密技术在计算机网络安全中的应用[J].中国宽带，2023，19（12）：139-141.
[2] 黎泽.光域数据加密解密技术[J].中国科技信息，2023（24）：105-109.
[3] 张鼎.基于对抗加密的无线通信网络数据安全传输方法[J].长江信息通信，2023，36（12）：181-183.
[4] 陈伟东，张驰.基于光通信技术的物联网数据加密技术分析[J].光源与照明，2023（11）：78-80.
[5] 唐高阳.数据加密技术在计算机网络安全中的实践探析[J].软件，2023，44（11）：85-87.