 DOI: https://doi.org/10.12349/iser.v5i8.3247

Application of Data Encryption Technology in Computer Network Communication Engineering

Xuliang Liu

Wuhan Donghu University, Wuhan, Hubei, 430000, China

Abstract

With the rapid development of computer network communication technology, information security issues have become increasingly prominent. Data encryption technology, as an important means of ensuring network communication security, has received widespread attention. This paper discusses in detail the application of data encryption technology in computer network communication engineering. By analyzing its principles and characteristics, this paper elaborates on the important role of data encryption technology in ensuring information security and improving network communication reliability. Introduced common data encryption algorithms and provided prospects for future development trends. Therefore, the research on computer network security technology has been elevated to an unprecedented level and has become an important research direction in the field of information science.

Keywords

data encryption technology; computer network communication; information security; application

数据加密技术在计算机网络通信工程中的应用

刘栩良

武汉东湖学院，中国 · 湖北 武汉 430000

摘　要

随着计算机网络通信技术的飞速发展，信息安全问题也日益凸显。数据加密技术作为保障网络通信安全的重要手段，受到了广泛关注。论文详细探讨了数据加密技术在计算机网络通信工程中的应用。通过分析其原理和特点，阐述了数据加密技术在保障信息安全、提高网络通信可靠性方面的重要作用。介绍了常见的数据加密算法，对未来发展趋势进行了展望。为此，计算机网络安全技术的研究被提升至前所未有的高度，成为信息科学领域的重要研究方向。

关键词

数据加密技术；计算机网络通信；信息安全；应用

1 引言

随着网络共享性的不断拓展，网络安全问题也日益凸显，成为社会各界普遍关注的焦点。网络安全不仅关乎个人隐私的保护，更直接影响到国家安全以及经济发展的各个领域。在这一背景下，数据加密技术作为保障网络安全的关键手段之一，其应用显得尤为重要。数据加密技术通过先进的算法对敏感数据进行加密处理，确保数据在传输和存储过程中的机密性、完整性，为构建安全可信的网络环境提供了坚实的技术支撑。为此，这一技术在计算机网络通信工程中的应用具有深远的研究意义。

2 计算机网络安全数据加密技术概述

2.1 计算机网络安全

计算机网络安全是指通过一系列技术手段和管理措施，保护计算机系统中的硬件、软件和数据免受非法访问、篡改或者泄露的过程。随着信息化时代的到来，计算机网络在军事、文化等各个领域的应用日益广泛，其安全性也显得愈发重要。为了维护计算机网络安全，需要采用多种防护策略，其中数据加密技术是最为核心和有效的手段之一。通过数据加密，可以将敏感信息转换为无法直接识别的密文形式，从而防止未经授权的访问。

2.2 数据加密技术简介

数据加密技术是一种通过加密算法和密钥将明文（原始数据）转换为密文（加密后的数据）的技术，以保护数据在传输和存储过程中的安全性和隐私性。其核心技术是密码学，包括对称加密和非对称加密两种主要方式。对称加密使用相同的密钥进行加密和解密，而非对称加密则使用一对密钥（公钥和私钥）分别进行加密和解密。数据加密技术在金融、军事等多个领域有广泛应用，是保障信息安全的重要手段 [1]。置换算法是最简单的加密算法，循环位移算法是一种对资料定位进行转换的方法，数据加密技术类型分为对称与

【作者简介】刘栩良（2000–），男，中国广西苍梧人，本科，从事通信工程研究。

非对称技术。在不公开密钥的情况下，发送和接收方都可以利用同样的密钥进行加密，从而保证了数据的保密。DES 是一种基于 64 比特的对称数据块密码算法，它在银行资金转移中得到了广泛的使用。DES 是由美国 IBM 公司所推出的一种包密码技术，它被应用于各种类型的对称加密中。在这种情况下，发送和接收方采用不同的密钥进行加密和解码，而通信双方在没有预先交换密钥的情况下可以进行保密的通讯。

3 计算机网络通信工程中的安全需求

3.1 数据保密性需求

计算机网络通信工程中，数据保密性是至关重要的安全需求之一。随着信息技术的飞速发展，大量敏感信息在网络中传输，如个人隐私信息、商业机密、金融交易数据等。这些数据若被未经授权的第三方获取，可能会导致严重的后果。比如，个人的医疗记录、银行账户信息等一旦泄露，可能会被用于欺诈、身份盗窃等违法活动，给个人带来巨大的经济损失和精神困扰。对于企业来说，研发成果、财务报表等机密信息的泄露可能使其在市场竞争中处于劣势，甚至面临破产的风险。

为满足数据保密性需求，需要采取有效的加密措施，将数据转换为密文形式进行传输，只有拥有正确密钥的授权方能够将密文解密还原为明文，从而确保数据在传输和存储过程中的保密性。

3.2 身份认证需求

身份认证是计算机网络通信工程中的另一个关键安全需求。在网络环境中，确认通信双方的真实身份是建立安全通信的前提 [2]。在电子商务、网上银行等应用场景中，身份认证尤为重要。客户需要确认所访问的网站是真实可靠的，而服务提供商也需要确认客户的身份，以防止欺诈行为。常见的身份认证方式包括基于口令的认证、基于证书的认证、生物特征认证等。同时，多因素认证方式的结合使用能够进一步提高身份认证的安全性和可靠性。

4 数据加密技术在计算机网络通信工程中的应用场景

4.1 电子邮件加密

电子邮件作为一种常用的通信方式，在日常工作和生活中被广泛应用。然而，由于电子邮件在网络中传输时是以明文形式存在的，如果被不法分子截获，其中的信息可能会被泄露。因此，电子邮件加密技术应运而生。对称加密算法如 AES 可以用于对电子邮件的内容进行加密。寄件者在传送信息前，会先用预设的金钥将其中的内容加以加密。接收方在接收到消息后，采用同样的密匙将其解密，以获得纯文本的信息。通过这种方式，即便消息在传送途中被截获，因为没有密钥，攻击方也不能破译消息的内容。像 RSA 这样的不对称密码演法则也经常被用来进行电邮密码。寄件者利用接收方的公开密钥来对消息进行加密，而接收方则用自己的私有密钥将其解密。这样既能避开对称密码体制下的密钥分配困难，又能保证信息的安全。

4.2 电子商务交易加密

电子商务领域，数据加密技术对于保障交易安全至关重要。当消费者在网上进行购物时，需要输入个人信息如姓名、地址、信用卡号等敏感信息。如果这些信息在传输过程中没有加密，很容易被黑客窃取，导致消费者遭受经济损失。用户与电商平台之间的通信过程中，通常使用 SSL/TLS 协议进行加密。SSL/TLS 协议基于非对称加密算法和对称加密算法的结合，首先使用非对称加密算法交换对称加密的密钥，然后使用对称加密算法对后续的通信数据进行加密。

此外，电商平台还会对用户的交易记录和订单信息进行加密存储，以防止数据泄露。只有经过授权的人员，在拥有正确的密钥和权限的情况下，才能够访问和读取这些数据。比如，一位消费者在网上购买了一件昂贵的商品，并使用信用卡进行支付。在输入信用卡信息时，数据被加密传输到支付网关。支付网关解密数据并完成支付处理，同时将交易记录加密存储。整个过程中，消费者的信用卡信息得到了有效保护，避免了被不法分子盗用。

4.3 虚拟专用网络（VPN）加密

虚拟专用网络（VPN）作为现代网络通信的利器，不仅为用户在广阔的公共网络空间中开辟出一条专属的、加密的“信息高速公路”，还极大地提升了数据传输的安全性与隐私保护水平。通过精密的数据加密技术，VPN 能够确保无论是敏感的商业资料、个人身份信息还是其他关键数据，在穿越复杂多变的互联网环境时，都能免受窥探与篡改的风险。

IPsec 与 SSL 作为 VPN 中广泛采用的两大加密协议，各自展现了独特的优势。IPsec 以其在网络层直接工作的能力，实现了对数据包的全面加密与认证，确保了数据从源头到目的地的全程安全。而 SSL VPN，则凭借其基于 SSL/TLS 协议的强大加密机制，以简洁的网页形式提供了灵活便捷的远程访问服务，让用户能够轻松穿越网络边界，安全访问企业内部资源。对于现代企业而言，VPN 技术已成为实现远程办公、跨地域协作不可或缺的基础设施。它让员工无论身处何地，都能通过加密的 VPN 连接，无缝接入企业网络，享受如同身处办公室般的工作体验，同时确保企业数据的安全无忧，为企业的数字化转型与全球化发展奠定了坚实的基础。

4.4 国密算法在工业互联网安全中的应用

国密算法在工业互联网安全中的应用日益凸显其重要性，尤其是在中国网络空间安全战略中占据举足轻重的地位。随着全球网络空间竞争加剧，密码技术作为保障信息安全的核心手段，已成为国家战略资源的关键组成部分。工业互联网，作为新工业革命的核心驱动力，其安全性直接关系

到国家经济命脉和社会稳定，因此，工业互联网安全自然成为了网络安全领域的重要议题。

鉴于当前部分国际主流密码算法面临的安全挑战与潜在风险，中国高度重视并加大了对国产密码算法（即国密算法）的研发力度。国密算法不仅旨在解决现有密码体系的安全性问题，更致力于构建自主可控的信息安全防线。在商用领域，国密算法已构建起一套完整且坚实的基础型密码体系，如 SM1、SM4 等对称加密算法，以及 SM2、SM3 等非对称加密算法，这些算法均获得了国家相关部门的正式批准，成为行业密码标准的重要组成部分。尤为值得一提的是，SM2 算法在安全性上展现出超越国际通用 ECDSA 算法的卓越性能，这一成就不仅彰显了中国密码技术的创新实力，也为工业互联网安全提供了更为坚实的保障。随着工业互联网的快速发展，国密算法的应用范围不断拓展，从数据传输加密、身份认证到数字签名等多个环节，均能看到国密算法的身影，有效提升了中国工业互联网的整体安全防护能力 [3]。

5 数据加密技术的未来发展趋势

5.1 量子加密技术的发展

随着科技的不断进步，量子加密技术正逐渐成为数据加密领域的一个重要发展方向。量子加密技术基于量子力学的原理，利用量子态的特殊性质来实现信息的加密和解密。与传统加密技术相比，量子加密技术具有更高的安全性。传统加密技术的安全性依赖于数学难题的计算复杂度，随着计算能力的不断提高，这些难题可能会被逐渐攻克。而量子加密技术使得任何对量子态的测量都会改变其状态，从而保证了加密信息的绝对安全性。

目前，量子密钥分发技术是量子加密技术的一个重要应用。通过在发送方和接收方之间传输量子态，双方可以生成共享的密钥，用于对信息进行加密和解密。由于量子态的特殊性，任何对密钥传输过程的窃听都会被发现，从而确保了密钥的安全性。未来量子加密技术有望在更广泛的领域得到应用。随着技术的不断成熟和成本的降低，量子加密技术可能会逐渐取代传统加密技术，成为保障信息安全的主流手段。例如，在军事、政府等对信息安全要求极高的领域，量子加密技术将发挥重要作用。然而，量子加密技术的发展也面临一些挑战。目前，量子加密技术的传输距离和传输速率还受到一定的限制，需要进一步的研究和改进。此外，量子加密技术的设备复杂、成本高昂，也限制了其大规模的应用。但随着技术的不断突破，这些问题有望逐步得到解决。

5.2 与人工智能技术的融合

人工智能技术的快速发展为数据加密技术带来了新的机遇和挑战。将人工智能技术与数据加密技术相融合，有望实现更加智能、高效和自适应的加密解决方案。加密算法的设计方面，人工智能可以通过学习和分析大量的数据，帮助设计更加复杂和安全的加密算法。例如，利用机器学习算法来优化加密算法的参数，提高加密的强度。同时，人工智能可以用于加密系统的安全监测和预警。通过对网络流量、系统日志等数据的分析，人工智能系统可以实时检测到异常的访问行为和潜在的安全威胁，并及时发出警报，采取相应的防护措施。

此外，人工智能还可以在密钥管理方面发挥作用。通过对用户行为和环境的分析，智能地生成和更新密钥，提高密钥的安全性。身份认证方面，人工智能技术如人脸识别、语音识别等可以与传统的加密认证方式相结合，提供更加便捷和安全的认证方式。例如，利用深度学习算法对用户的生物特征进行准确识别和验证，同时结合加密技术保障认证过程的安全性。但是，人工智能与数据加密技术的融合也带来了一些新的问题。例如，人工智能系统本身可能存在安全漏洞，被攻击者利用；人工智能算法的复杂性可能导致加密系统的可解释性降低，增加了安全评估的难度。为充分发挥人工智能与数据加密技术融合的优势，需要加强相关的研究和开发，解决技术融合中出现的问题，制定相应的安全标准和规范。同时，还需要加强对人工智能与数据加密技术融合应用的监管，确保其在合法、安全的框架内运行。

6 结语

总之，数据加密技术在计算机网络通信工程中的应用，不仅是信息安全防护的坚实盾牌，更是推动数字化转型与智能化升级的重要驱动力。它以其高效、可靠的安全性能，确保了数据在传输过程中的机密性、完整性和可用性，为各类敏感信息的交流筑起了一道不可逾越的安全屏障。随着技术的不断进步和应用场景的日益丰富，数据加密技术将持续演进，为计算机网络通信工程提供更加全面、智能的安全保障，助力构建一个更加安全、可信、高效的数字世界。

参考文献

[1] 宋凯,汪庆伟,张媛媛,等.数据加密技术在计算机网络安全防护中的应用研究[J].中国军转民,2023(7):35-36.

[2] 林嘉.数据加密技术在计算机网络通信安全中的应用策略[J].无线互联科技,2023,20(9):7-9.

[3] 杨冬.基于数据加密技术的计算机网络通信安全防御研究[J].电子通信与计算机科学,2023(9).