计算机网络通信安全中数据加密技术研究

窦　琨
新疆农业职业技术大学　新疆　昌吉　831100

摘　要：数据加密对计算机网络通信安全至关重要，可保障数据机密性、完整性，实现身份认证与访问控制，维护通信可信度。但网络通信面临数据窃听、篡改、身份伪造与否认等威胁。为此需合理选择加密算法，加强密钥管理，并定期更新加密技术与安全策略，以构建全方位、多层次的加密安全防护体系。

关键词：计算机网络通信安全；数据加密；技术研究

引言：在数字化浪潮席卷之下，计算机网络通信已成为社会运转的关键支撑，但数据窃听、篡改、身份伪造等安全威胁如影随形。数据加密技术作为保障网络通信安全的核心手段，不仅能确保数据机密性与完整性，还可实现身份认证与访问控制，维护网络可信度。本文将深入剖析计算机网络通信面临的安全威胁，详细阐述对称加密、非对称加密、哈希函数等数据加密技术，并探讨保障其有效应用的措施。

1 数据加密技术在计算机网络通信安全中的重要性

数据加密技术在计算机网络通信安全中具有不可替代的重要性。（1）保障数据的机密性。在网络通信中，数据从发送方传输到接收方的过程中，可能被未授权的第三方窃听。数据加密技术通过将明文数据转换为密文，使窃听者无法读懂数据内容，只有拥有解密密钥的授权者才能将密文还原为明文，从而确保敏感信息（如银行卡信息、个人隐私、商业秘密等）不被泄露。（2）确保数据的完整性。数据在传输过程中可能因网络故障、恶意攻击等原因被篡改，导致数据失真。数据加密技术结合哈希函数等手段，能够为数据生成唯一的校验值，接收方通过验证校验值可判断数据是否被篡改，若校验值不一致，则说明数据在传输过程中发生了变化，从而保证数据的完整性。（3）实现身份认证与访问控制。数据加密技术可用于网络通信中的身份认证，如通过数字签名技术，发送方用私钥对数据进行签名，接收方用发送方的公钥验证签名，确认发送方的身份真实性，防止身份伪造。同时，基于加密技术的访问控制机制，能够限制未授权用户对敏感数据的访问，确保只有授权用户才能获取和使用数据。（4）维护网络通信的可信度。有效的数据加密技术能够增强用户对网络通信的信任，促进电子商务、在线金融等网络应用的发展，保障网络经济的健康运行[1]。

2 计算机网络通信面临的安全威胁

2.1 数据窃听

数据窃听作为网络通信领域极为普遍且危害巨大的安全威胁，始终是网络安全防护的重点与难点。它指的是未获得授权的个体或实体，借助多种技术手段，非法获取处于传输状态的数据。（1）攻击者常用的手段是利用网络嗅探工具，像Wireshark这类专业软件，对网络中的数据包进行实时监听与捕获，进而获取其中包含的敏感明文信息，诸如用户名、密码以及聊天记录等。在无线局域网环境下，由于信号具备开放性特征，数据窃听变得更为简便。攻击者只需成功破解无线网络的加密方式，例如WEP、WPA等，就能顺利接入网络并肆意窃听数据。（2）数据窃听所带来的后果不堪设想，不仅会造成个人隐私的严重泄露，还可能给企业和国家带来难以估量的重大损失。企业的商业谈判内容一旦被窃听，商业机密便会泄露，进而削弱企业在市场中的竞争力；而国家机密若遭窃听，则可能直接威胁到国家的安全与稳定。

2.2 数据篡改

数据篡改作为网络安全领域中一种极具危害性的攻击手段，指的是攻击者未经授权，恶意修改处于传输过程中的数据，进而改变数据的原始内容或呈现形式，其核心目的在于欺骗数据接收方或者破坏数据的完整性。（1）攻击者常采用中间人攻击等手段，在数据传输的路径中巧妙拦截数据包。他们凭借专业的技术工具和恶意程序，对拦截到的数据进行肆意修改，之后再将篡改后的数据发送给原本的接收方。由于整个过程隐蔽性极强，发送方和接收方往往难以察觉数据已被篡改。（2）数据篡改可能引发一系列严重后果。在电子商务交易场景里，攻击者可能会篡改商品价格或交易金额，使交易双方遭受经济损失；在工业控制系统环境中，篡改控制指令极有可能引发生产流程紊乱，甚至导致严重的生产事故；在金融领域，篡改转账信息更是会造成资金被非法转移，严重威胁金融安全与稳定。

2.3 身份伪造与否认

身份伪造与否认是网络安全中两类极具危害性的问题。（1）身份伪造，即攻击者通过技术手段，精心伪装成合法用户或网络节点，以此绕过安全认证机制，获取未授权的访问权限，或者发送虚假信息来误导其他用户。例如，攻击者会搭建与真实银行网站高度相似的虚假页面，利用用户对银行的信任，诱骗其输入账号和密码等敏感信息，进而窃取用户资金；还会伪造电子邮件发送者身份，发送带有恶意链接或病毒的邮件，诱导接收者点击，从而植入恶意程序，控制用户设备。（2）身份否认则表现为发送方在完成数据发送后，矢口否认自己曾发送过该数据，或者接收方否认接收过相关数据，以此逃避应承担的责任。如在电子合同签订场景中，一方可能为了自身利益，否认签订过合同，引发不必要的纠纷；在网络攻击事件里，攻击者常利用技术手段隐藏真实身份，让溯源工作困难重重。

3 计算机网络通信中的数据加密技术

3.1 对称加密技术

对称加密技术作为一种经典且应用广泛的加密手段，其核心特征在于加密和解密过程使用完全相同的密钥。（1）其基本原理是，在通信双方进行数据交互前，需预先协商并确定一个密钥。发送方获取该密钥后，运用特定的加密算法对明文信息进行加密处理，将明文转化为密文，随后将密文传输给接收方。接收方在收到密文后，使用相同的密钥，通过对应的解密算法对密文进行解密操作，从而还原出原始的明文信息。（2）常见的对称加密算法包含DES（数据加密标准）、AES（高级加密标准）、IDEA（国际数据加密算法）等。其中，AES算法优势显著，它支持密钥长度可变，有128位、192位、256位三种选择，且加密速度快、安全性高，因而成为当前应用最为广泛的对称加密算法，在文件加密、数据库加密以及网络传输加密等众多领域均有广泛应用。（3）对称加密技术的优势在于加密和解密速度较快，尤其适合对大规模数据进行加密处理。然而，它也存在明显不足，密钥的分发与管理难度较大。在多用户通信场景下，需为每对用户分配不同的密钥，导致密钥数量急剧增加，不仅增加了管理成本，还提高了密钥泄露的风险。

3.2 非对称加密技术

非对称加密技术，亦被称作公钥加密技术，是一种与对称加密截然不同的加密体系。它采用一对相互关联但功能不同的密钥，即公钥和私钥，来实现加密与解密操作。其中，公钥可自由公开传播，而私钥则由用户严格自行保存并确保其保密性。（1）在实际应用中，存在两种主要的操作模式。一种是由发送方利用接收方的公钥对明文进行加密，接收方收到密文后，使用自己独有的私钥进行解密，从而获取原始信息；另一种则是发送方使用自己的私钥对数据进行签名（相当于加密），接收方借助发送方的公钥进行验证（相当于解密），以此确保数据的完整性和来源的真实性。（2）常见的非对称加密算法涵盖RSA、ECC（椭圆曲线密码体制）、DSA（数字签名算法）等。RSA算法基于大整数分解问题，安全性颇高，然而加密速度相对较慢，更适用于对少量数据，如密钥等进行加密。ECC算法基于椭圆曲线数学问题，在相同安全级别下，其密钥长度比RSA更短，加密速度更快，因而广泛应用于移动设备、物联网等资源受限的场景。（3）非对称加密技术的优势在于密钥管理简便，公钥的公开性消除了密钥分发泄露的担忧；但缺点是加密和解密速度较慢，不适合大规模数据的加密处理[2]。

3.3 哈希函数

哈希函数，亦被称为散列函数，在信息安全领域扮演着至关重要的角色。它具备独特的数学特性，能将任意长度的输入数据，经过特定算法处理后，转换为固定长度的输出数据，这个输出数据就被称作哈希值。（1）哈希函数具有两个关键特性。其一为单向性，这意味着基于哈希值，几乎无法通过逆向计算还原出原始的输入数据，为数据的安全性提供了基础保障。其二为抗碰撞性，即不同的输入数据极难生成相同的哈希值，有效避免了数据混淆和冲突。（2）常见的哈希函数包括MD5、SHA-1、SHA-256等。其中，SHA-256作为SHA系列的一员，输出长度为256位，因其较高的安全性，在数据完整性校验、数字签名等众多领域得到广泛应用。（3）在网络通信场景中，哈希函数常与加密技术协同工作。发送方先对原始数据计算哈希值，再用私钥对哈希值加密生成数字签名，随后将原始数据和数字签名一同发送给接收方。接收方收到后，对原始数据计算哈希值，并用发送方公钥解密数字签名，若两个哈希值一致，便可确认数据未被篡改，且发送方身份真实可靠。

4 保障数据加密技术有效应用的措施

4.1 合理选择加密算法

合理选择加密算法是确保数据加密成效的基石，需综合多方面因素进行审慎考量。（1）数据的敏感程度是首要考量因素，对于涉及国家机密、金融交易等高度敏感的数据，必须选用安全性极高的加密算法，像AES-256凭借其较长的密钥长度和复杂的加密机制，以及ECC基于椭圆曲线数学难题的高安全性，能有效抵御各类攻击，保障数据安全。（2）传输场景和性能要求也不容忽视。在视频会议、实时监控等对实时性要求严苛的场景

中，加密速度至关重要，此时AES算法是理想之选，它能快速完成加密解密操作，减少对实时传输的延迟影响。（3）对于密钥分发场景，非对称加密算法如RSA、ECC可发挥优势，用于加密对称密钥，实现密钥的安全传递。此外，还需密切关注加密算法的安全性更新，及时淘汰已被破解或不安全的算法，如DES、MD5、SHA-1，积极采用新算法以应对不断演变的安全威胁。

4.2 加强密钥管理

密钥作为数据加密技术的核心要素，其管理的有效性直接关乎加密安全。因此，必须构建一套完备的密钥管理机制，涵盖生成、分发、存储、更新和销毁等各个环节。（1）在密钥生成环节，要采用具备密码学安全性的随机数生成器，以此保证密钥的随机性与不可预测性，从源头上提升密钥的安全性。密钥分发时，需借助安全渠道，例如利用非对称加密算法对对称密钥进行加密后再分发，防止密钥在传输过程中被窃取。密钥存储方面，应采用加密存储方式，像硬件安全模块（HSM）、密钥管理系统（KMS）等，为密钥提供可靠的物理和逻辑保护。同时，要定期更新密钥，降低长期使用同一密钥带来的安全风险。密钥销毁时，则要确保彻底，杜绝密钥被恢复的可能性。（2）还需实施严格的密钥访问控制，严格限制密钥的使用权限，仅允许授权人员接触和使用密钥，并对密钥的使用情况进行详细的日志记录，以便后续进行审计和追溯，全方位保障密钥安全[3]。

4.3 定期更新加密技术与安全策略

在网络安全威胁持续动态演变的当下，加密技术的更新迭代刻不容缓，唯有如此才能有效抵御层出不穷的新型威胁。为此，需定期对现有加密技术的安全性展开全面评估，依据评估结果及时引入前沿的加密技术与安全机制。例如，面对量子计算可能带来的颠覆性冲击，应积极关注并探索量子加密技术，提前布局以应对潜在风险。与此同时，安全策略的制定与完善同样关键。要清晰界定加密技术的应用范畴、操作规范以及应急预案，确保在面对突发安全事件时能够迅速响应、妥善处理。此外，加强员工的安全意识培训不可或缺，通过系统培训让员工深刻认识加密技术的重要性，熟练掌握正确使用方法，从源头上避免因人为操作失误致使加密失效。为进一步保障加密技术的有效应用，还应定期开展安全演练与漏洞扫描工作，精准发现加密系统中存在的安全漏洞，并及时进行修复，构建起全方位、多层次的加密安全防护体系。

结束语

在计算机网络通信中，数据加密技术是保障安全的核心手段。从应对数据窃听、篡改、身份伪造与否认等安全威胁，到运用对称加密、非对称加密、哈希函数等技术，再到通过合理选算法、加强密钥管理、定期更新技术与策略等措施保障其有效应用，每一步都至关重要。随着网络安全威胁不断演变，数据加密技术也需持续创新与完善。只有紧跟时代步伐，不断优化加密方案，强化安全防护体系，才能确保计算机网络通信中数据的机密性、完整性和可用性，为网络经济的健康发展以及个人、企业和国家的信息安全筑牢坚实防线

参考文献

[1]翟宗香,陶金涛,贾晓晨,张风娟.计算机网络通信安全中数据加密技术分析[J].黑龙江科学,2020,11(20):102-103

[2]陈又铜,李勃翰.计算机网络通信安全中数据加密技术的应用研究[J].计算机产品与流通,2020(06):56

[3]梁海玲.计算机网络通信安全中数据加密技术的分析与探讨[J].通信电源技术,2020,37(04):222-223