计算机网络信息安全中数据加密技术

吴秀娟　荣　曦
济南市气象局　山东　济南　250000

摘　要：随着网络技术的飞速发展，人们在享受网络带来的便利和信息资源丰富的同时，也面临着日益严峻的信息安全问题。尤其是在涉及到国家利益、商业机密和个人隐私等方面，信息安全问题更是变得尤为重要。在这种情况下，数据加密技术成为保障信息安全的重要手段之一。

关键词：计算机；网络信息安全；数据加密技术

引言

随着我国科学技术的飞速发展，计算机技术作为一项至关重要的技术，逐渐走进了人们的生活，在计算机技术的应用过程中，随之而来的网络安全问题也逐渐受到人们的关注，为了保障计算机网络信息系统的安全性，应将数据加密技术运用其中，从而避免信息泄露等情况的发生，本文将对计算机网络信息安全当中数据加密技术的实际应用展开分析与探讨，加强对数据加密技术作用的了解。

1 计算机网络信息安全的重要性

随着计算机技术的飞速发展，网络已经成为人们日常生活和工作中不可或缺的一部分[1]。然而，网络安全问题也日益突出，各种攻击和欺诈活动已经给网络带来了极大的危害，造成了严重的经济损失和社会影响。因此，计算机网络信息安全已经成为当今社会非常重要的议题之一。

1.1 保护个人隐私和财产安全

计算机网络信息安全最基本的目的是保护个人隐私和财产安全。在互联网上，个人的敏感信息如姓名、地址、电话号码、银行卡号等可能被不法分子盗取，从而给个人带来极大的损失。同时，网络上的电子商务、在线交易等活动也容易造成财产安全风险，一旦被骗走，可能给个人造成无法挽回的经济损失。

1.2 维护国家安全

网络是信息传播和交流的重要平台，也是国家进行信息战和情报收集的重要手段。一些国家的政府和情报机构可能会利用网络进行间谍活动、网络攻击和病毒传播等行为，严重危害国家的安全和稳定。因此，维护计算机网络信息安全不仅是维护个人利益和权益的需要，也是维护国家利益和安全的需要。

1.3 保障企业合法权益

企业在开展电子商务、在线交易等业务时，需要保证信息的安全性和隐私性，防止敏感信息被盗取和泄漏。如果企业的网络信息安全得不到保障，不仅会对企业造成经济损失，还会影响企业声誉和客户信任度，甚至导致企业破产。

1.4 促进经济发展

网络经济已经成为国民经济的重要组成部分，维护计算机网络信息安全不仅有利于保护个人和企业的合法权益，也有利于促进经济发展。一旦网络遭受攻击和破坏，将严重影响经济活动的正常进行，甚至导致经济衰退。

2 计算机网络信息安全的现状

2.1 黑客攻击频发

黑客是指擅长利用计算机网络进行恶意攻击的人员[2]。近年来，黑客攻击事件频繁发生，攻击手段不断升级，给各行各业带来了巨大的损失。据统计，全球每年因黑客攻击导致的经济损失高达数千亿美元。

2.2 病毒和木马泛滥

病毒和木马是指能够侵入计算机系统并破坏数据或程序的计算机程序。随着互联网的不断普及，病毒和木马的传播速度也越来越快，危害也越来越大。据统计，全球每年因病毒和木马导致的经济损失超过数十亿美元。

2.3 信息泄露和诈骗

信息泄露和诈骗是指通过网络侵犯他人隐私和财产的行为[3]。随着互联网的普及，信息泄露和诈骗的危害越来越大，给个人和企业带来了巨大的损失。据统计，全球每年因信息泄露和诈骗导致的经济损失超过数百亿美元。

2.4 网络监管不足

网络监管是指对计算机网络系统进行监视、控制和管理的过程。当前，许多国家和地区的网络监管体系还不够完善，无法及时发现和有效应对网络安全威胁。此外，一些企业和个人也存在违规使用互联网、危害网络安全的行为，导致监管难度加大。

3 数据加密技术的原则

3.1 保证数据的机密性

数据加密的第一个原则就是保证数据的机密性。机密性是指数据只能被授权人员访问，其他人无法访问或者复制数据。这是数据加密技术的核心原则，也是保证数据安全的基础。

3.2 保证数据的完整性

数据加密的第二个原则就是保证数据的完整性。完整性是指数据在存储和传输过程中没有被篡改，并且在需要使用时能够正确地还原。如果数据在存储或传输过程中被篡改或者在需要使用时无法还原，那么数据的完整性就无法得到保证。

3.3 保证数据的可用性

数据加密的第三个原则就是保证数据的可用性。可用性是指数据在需要时能够被合法的用户访问，并且在使用过程中不会受到干扰或者破坏。如果数据在需要时无法被合法用户访问或者在使用过程中受到干扰或者破坏，那么数据的可用性就无法得到保证。

3.4 保证数据的可控性

数据加密的第四个原则就是保证数据的可控性。可控性是指数据的加密过程和密钥管理能够被授权人员控制，并且在需要时能够被授权人员撤销或者更改。如果数据的加密过程和密钥管理不能被授权人员控制，那么数据的可控性就无法得到保证。

3.5 提高安全性能

最后一个原则就是提高数据加密技术的安全性能。安全性能是指数据加密技术能够有效地防止攻击者对数据进行窃取、篡改或者破坏等攻击行为[4]。这需要选择合适的加密算法和安全协议，并且进行充分的测试和验证。

4 数据加密技术概述

4.1 分类

数据加密技术是指通过对数据进行加密处理，使其在传输、存储和处理过程中不易被非法获取或破解。数据加密技术主要包括对称加密和非对称加密两种方式。

4.1.1 对称加密是指使用相同的密钥对数据进行加密和解密，常用的加密算法有AES、DES等。在对称加密中，加密和解密使用相同的密钥，因此只有拥有相同密钥的人才能进行加密和解密，这样就增加了数据的安全性。但是，由于需要使用相同的密钥，如果密钥被泄露，整个数据就会被破解。下面是几种常见的对称加密技术：

1)AES

AES（Advanced Encryption Standard）是一种对称加密算法，它使用的是AES-256加密算法。AES算法使用了一种称为Cipher Block Chaining的技术，该技术将加密和解密过程分为多个阶段，每个阶段使用不同的密钥。这种技术使得AES算法具有很高的安全性。

2)2DES

DES（Data Encryption Standard）是一种对称加密算法，它使用的是DES-56加密算法。DES算法使用了一种称为Cipher Block Chaining的技术，但是它只能用于加密较小的数据块。

3)RMQ

RMQ（Relational-MD5）是一种基于哈希函数的对称加密技术，它使用的是MD5哈希函数。RMQ技术使用了一种称为分布式哈希的技术，将数据分散到多个节点上进行计算，然后将计算结果进行合并，以保证数据的安全性。

4.1.2 非对称加密技术是一种不同于对称加密技术的加密技术，它使用一对密钥，其中一个密钥是公钥，另一个密钥是私钥。公钥可以公开分享，而私钥则只能由发件人拥有[1]。这种加密技术具有更高的安全性，因为只有拥有私钥的人才能解密数据，而其他人则不能。下面是几种常见的非对称加密技术：

1)RSA

RSA（Rivest-Shamir-Adleman）是一种非对称加密算法，它使用的是RSA-2048加密算法。RSA算法使用了一种称为公钥和私钥的概念，两个密钥都是公钥和私钥的组合。使用公钥对数据进行加密，只有使用对应的私钥才能进行解密。

2)DSA

DSA（Digital Signature Algorithm）是一种非对称加密算法，它使用的是SHA-256哈希函数。DSA算法使用了一种称为签名者的概念，签名者需要将数据进行哈希处理，并将哈希值作为签名附加到数据上。接收方则需要使用相同的哈希函数对数据进行哈希处理，并比较哈希值是否与签名相同。如果相同，则说明数据未被篡改，否则数据可能已被篡改。

3)ECC

ECC（椭圆曲线公钥加密）是一种非对称加密算法，它使用的是ECDSA加密算法。ECC算法使用了椭圆曲线密码学的概念，将数据进行加密和解密过程都变成了计算密码学问题。这种技术使得ECC算法具有很高的安全性和不可伪造性。

4)ECJ

ECJ（Elliptic Curve Diffie-Hellman）是一种基于椭圆曲线密码学的非对称加密技术，它使用的是ECDSA加密算法。ECJ算法使用了一种称为共享密钥的概念，两个参与方都需要生成一个共享密钥，并使用该密钥对数据进

行加密和解密。这种技术使得ECJ算法具有很高的安全性和不可伪造性。

除了对称加密和非对称加密外，还有一种混合加密方式，即将对称加密和非对称加密结合起来使用。这种方式可以在保证数据安全性的前提下，提高数据传输的效率。

4.2 应用

数据加密技术在信息安全中的应用非常广泛。在网络传输中，数据加密技术可以保护敏感数据不被窃取或篡改。在电子商务中，数据加密技术可以保证交易数据的安全性和隐私性[2]。在云计算中，数据加密技术可以保证云端数据的安全性和隐私性。在政府和企业中，数据加密技术可以保证机密数据不被泄露或滥用。

虽然数据加密技术在信息安全中发挥着重要作用，但是其应用也存在一定的局限性。首先，数据加密技术只能保障数据在传输过程中的安全性，如果数据存储或处理不当，仍然可能被非法获取或破解。其次，数据加密技术需要使用特定的加密算法和密钥，如果这些算法和密钥被破解，数据的安全性就会受到威胁。此外，数据加密技术还存在着难以扩展和升级的问题，随着网络技术的不断发展，原有的加密算法和密钥可能会失效，需要不断进行更新和升级。

为了克服数据加密技术的局限性，需要不断研究和发展新的加密算法和技术，以提高数据的安全性和隐私性。同时，也需要加强对数据加密技术的管理和监管，确保其使用符合法律法规和道德标准。

5 数据加密技术在计算机网络信息安全中应用的措施

随着信息技术的快速发展，计算机网络已经成为人们日常生活和工作中不可或缺的一部分。然而，网络安全问题也变得越来越严重，数据泄露、黑客攻击等问题时有发生。数据加密技术是一种可靠的信息安全保障技术，它可以对传输的数据进行加密处理，保证数据的机密性、完整性和可用性，从而保护计算机网络信息的安全。下面是数据加密技术在计算机网络信息安全中应用的措施。

5.1 保证数据机密性

数据机密性是数据加密技术的核心原则，它是指在数据传输过程中，对数据进行加密处理，只有授权人员才能对数据进行解密和使用[3]。数据机密性的实现主要依赖于加密算法和加密协议。常用的加密算法有对称加密算法和非对称加密算法，如AES、RSA等。加密协议主要包括SSL、TLS等。

5.2 保证数据完整性

数据完整性是指数据在传输过程中没有被篡改，并且在需要使用时能够正确地还原。数据完整性的实现主要依赖于数据校验和技术。数据校验和是指在数据传输过程中，对数据进行校验和计算，以保证数据的完整性。数据校验和技术可以通过在数据传输前对数据进行校验和计算，或者在数据传输过程中对数据进行实时校验和计算来实现。

5.3 保证数据可用性

数据可用性是指数据在需要时能够被合法的用户访问，并且在使用过程中不会受到干扰或者破坏。数据可用性的实现主要依赖于数字签名技术和身份认证技术。数字签名技术是指在数据传输前对数据进行签名处理，以保证数据的来源和完整性。身份认证技术是指对访问数据的用户进行身份认证，以保证用户的合法性。

5.4 保证数据可控性

数据可控性是指数据的加密过程和密钥管理能够被授权人员控制，并且在需要时能够被授权人员撤销或者更改。数据可控性的实现主要依赖于密码学技术和访问控制技术。密码学技术是指通过对数据进行加密处理来保护数据的机密性和完整性[4]。访问控制技术是指对数据的访问权限进行控制，以保证数据不被非法访问。

5.5 提高安全性能

提高数据加密技术的安全性能可以采取以下措施：采用强度更高的加密算法和安全协议；采用分层安全设计，将加密逻辑与应用逻辑分开，使得系统更加安全；采用审计日志来记录网络访问行为，分析安全事件，发现安全隐患；采用抗审查技术，防止被破解或者追踪。

结束语：总而言之在大数据时代，计算机网络的应用逐渐普遍化，为了保障信息的安全应加强对网络安全技术的研发，在数据传输当中采取数据加密技术至关重要，随着多年的发展，数据加密技术的种类逐渐多样化，可满足不同的安全需求，因此我们应对数据加密技术合理运用，对网络安全防护体系有效建立，确保数据传输的完整性与安全性大大提升。

参考文献

[1]吴琳琳.探究计算机网络通信安全中数据加密技术的应用[J].电子世界，2020(23):166-167.

[2]刘静，张静，张金涛.数据加密技术在公安机关计算机网络安全中的应用探究[J].电脑知识与技术，2020,16(33):50-52.

[3]王晓兰.关于计算机网络信息安全中数据加密技术的运用分析[J].电脑知识与技术，2020,16(33):53-54.

[4]赵英.数据加密技术对计算机网络信息安全的重要性与应用[J].中国新通信，2020,22(16):115.