ISSN: 2661-3719(Print); 2661-3727(Online)

基于网络信息安全的密码学技术的应用

曹筠钰
无锡学院物联网工程学院　214105

摘　要：科技进步迅速推动着互联网安全的挑战日益严重，如病毒侵入、黑客袭击及数据外泄等问题。为了应对这些问题，密码学的研发与使用应运而生，其功能包括维护电脑系统的稳定性以防假冒或修改数据，同时确保系统内数据的保密性与完整性。本文主要阐述了当前社会中信息安全的重要性，并对密码学技术进行了详细介绍，特别探讨了密码学技术在网络信息安全领域的实际应用，以供各位同行进行参考。

关键词：密码学技术；网络信息安全；计算机网络

引言：

早在古时，密码技术已经开始广泛使用于诸如外交和军事等关键领域的保护信息安全中，现在由于互联网科技的飞速进步，它正在逐步深入到各个行业。除了确保电脑网络上的秘密数据得到严密保密之外，密码技术也适用于数字签章、网络系统的安防等方面。通过利用密码学的原理，我们可以在保障网络信息的安全性和隐私性的同时，也能维护其一致性和不可篡改的特点。此外，这也有助于防范个人资料可能遭受未经授权修改或者伪造的风险。

一、网络信息安全的重要性

尽管早些年就已经有了关于网络信息的讨论，但其重要性并未得到足够的关注。然而随着互联网的发展与广泛应用，通信保护逐渐成为公众关注的焦点。现在，我们已经充分认识到了网络信息安全的重大意义，这不仅仅关乎社会的安定、财富的安全和个人生活的稳定，还可能导致诸如黑客攻击、电子间谍活动、电脑罪行、数据遗失、网络协议及信息战争等问题。这些问题不仅会影响我们的工作和生活，还会给国家的安全、军事实力、国际关系乃至政府机构的运作带来巨大冲击。目前，网络信息系统的功能已然成为了一个国家经济发展、政治决策、文化和社交活动的核心部分，如果受到损害而不能运行，那么会对整个国家造成巨大的损失，例如军队战斗力的削弱、通讯线路的中断、金融系统的瘫痪等等，最糟糕的情况可能会引发国内经济危机、政局动荡和社会秩序紊乱，后果难以预料。总而言之，我们在日常生活中的密码正遭受着严峻的考验，尤其是来自一种被称为“集体威胁”的风险，这种风险就如同垃圾邮件一般，并不直接针对个体。并非所有的黑客都只专注于破译个体的账户，他们对于个人信息完全不知情，他们的目标只是收集一系列已被破译的账户密码列表，然后出售获利。窃取秘密的人会选择使用破解软件，他们先从安全性防护水平较低的网站开始行动。等到这些软件被成功猜中后，他们再利用相同的秘密和其变种去攻击更为安全可靠的账户，例如银行账户。因此，对于密码学的研究有着极高的价值和意义[1]。

二、密码学技术的相关介绍

密码学技术是计算机网络信息安全的核心保障手段之一，它主要利用对网络内关键信息的加密和解密过程来保护其完整性和机密性。只有经过认证或授权的用户才能被允许进入网络系统。该技术的主要目的是确保电脑上的敏感数据和重要信息的安全性。

1.密码学以及其在网络信息安全中的应用

作为一种基于计算设备的安全系统设计方法论，密码学的研究起源于其构建及解析过程之中。它不仅为各国的政府机构提供高度保守的数据保护措施，也成为商业公司和个人隐私的关键保障手段之一。从银行到军队再到国际商务交易场所，我们都能看到它的存在并发挥作用。随著社会进步和生活方式的变化，人们的数字生活越来越离不开这个工具。而互联网体系结构则完全取决于这种机制来确定使用者的真实身分。一旦这些秘密暴露或遭人篡改，可能会导致不可预料且严重的影响发生在这个由电脑连接起来的全球互连网上。所以为了确保个人资料不会受到侵犯或是遭受攻击者利用，必须采取有效的防护策略以防止这种情况的发生。目前为止最常用的也是最具安全的办法是通过各种先进的技术如代码生成器和实质性的检测程序对所有传输过来的资讯内容做严格审查处理工作。同时也会根据需要选择合适的强力可靠而且易用方便的高效能密码运算模型及其相应的数学公式组合方案，以便更好地保证信息的完整性和真实性不受任何形式的外部干扰影响，从而达到最佳效果。所以，这些可能导致计算机网络信息安全的行动可以互相依赖或对抗，这有助于推动密码学的进步和发展。目前，计算机网络中使用的密码学技术可分为两类：一种是基于数学应用的技术，包括密钥管理、虚拟专用网（VPN）技术及数字签名；另一种则不是基于数学应用

技术的，如基于生物特征的身份认证技术与量子加密等。为了确保计算机网络的信息安全，我们必须合理地利用这些密码学技术来构建有效的计算机网络信息安全系统。

2.私钥密码学技术

在互联网环境下，私钥密码学的应用具有悠久的历史，它允许两个参与者共享相同的密码，以实现对数据和信息的加密或解密。每个参与者的任务是利用这个密码执行相应的加密或解密动作。由于只有同一把钥匙可以用于这两个过程，这使得整个流程变得更加简洁明了。只要私人密钥未被任何一方透露出去，就能确保消息内容的安全性和完整性。

3.公钥密码学技术

作为一种常用的加密方式，电脑公共钥匙编码技巧也叫作不对称代码策略。每个使用者都拥有对应于其自身的数字相关的，分别是公开密钥和私密密钥，尽管这两种不同的解法是由一对产生的但只有掌握了其中的任何一组才能破译另一方的信息内容。此项科技不但能确保互联网上的个人信息的安全性和保密度，而且还能增强网路通讯系统的可信度。该科学可以使互联网上两端的人们无需先共享他们的个人识别号码就能实现安全的交流沟通；同时它也可以用于各种重要的场合如：客户验证等等[2]。

三、计算机网络安全方面面临的威胁

1.非授权访问

未经个人或互联网管理者事前许可而私用网路资源的行为会被认定为无权限访问类别，此种类型的侵犯包括有意避开电脑网络监控系统、访问限制系统和不当利用电脑网络资源等违规行为，甚至可能超越其应有的权力去获取电脑网络数据等。这类无权限访问的主要形式有伪装或违法登录特定系统的操作，或是合法登录者的未获准许的操作等。

2.计算机信息丢失或者泄露

信息丢失或泄露是指计算机网络中的敏感数据被无意或故意泄露，比如网络黑客通过窃听或电磁泄露相关秘密数据，从而导致重要计算机信息的损失。

3.破坏计算机网络数据的完整性特点

一旦在电脑网络上盗取了未经授权的信息后，若采取添加或更改关键信息的行为，其目的在于引起黑客的积极反应。通过篡改或增加原始信息的元素来扰乱电脑网络的使用者，使他们的正常和合理的操作受到影响。

4.干扰服务系统

在电脑网络环境下，各种潜在的风险和危险会对电脑网络服务体系造成持续性的影响，从而迫使该服务体系调整其常规运作方式以运行非必要的软件或者降低对网络服务的反应速度，这可能最终会导致整个服务体系崩溃。所以，那些正常的电脑网络使用者无法顺利地访问电脑网络并且享受到相应的服务。

四、密码学在网络信息安全中的实际应用

1.起到加密保护的作用

作为密码学的核心部分，变换密码的功能是把原始文字合理地转换为只有授权用户能理解的密文。这个过程包含两个主要类型：一是传递消息时的加密；二是储存信息的加密。对于第一种情况，它涉及到保护通过电脑网络传播的所有类型的资讯，并将其划分为不同级别的加密等级以满足各种安全需求。第二种则是针对电脑网络中的档案和实质资料进行加密处理，这包括了档案库的加密和数据库的加密。然而，储存信息的加密相对较为复杂，因为它面临着如何平衡计算机数据加密和相关信息检索的问题，因此，这项加密技术仍需进一步研究和发展。

2.保证信息的完整性

为确保个人信息不受恶意更改，相应用户可采用密码学方法，通过计算网络信息和网络数据生成匹配的结果，即网络验证码。当计算机网络用户获取到网络信息后，应执行相同的实际操作以获得新的验证码，然后将其与已接收的信息验证码对比，确认其一致性，从而判断出网络信息的准确性。利用此种信息认证的密码学技巧能迅速检测用户信息是否有损毁情况。

3.数字签名与身份验证技术的应用

在计算机网络中，数字签名技术的实施是通过用户对电子信息的签署过程实现的。该方式可以被用于公钥、私钥加密系统，但由于其更能满足实际应用及研究需求，因此公钥加密系统更为常用。关于数字签名在计算机网络中的使用，主要包括以下几种策略：椭圆曲线上的数字签名、有限自动机下的数字签名等等，此外，这也包含了国家和地区法律法规的问题，许多国家已经设立了专用的法规以管理和指导数字签名技术的发展[3]。

五、结语

如今，由于互联网的高度普及和广泛应用，密码学已成为保护网络数据安全的核心工具。然而，仅依赖于密码学的手段并不能完全确保网络信息的绝对安全，因此需要综合运用多种技术以全面提升网络安全水平。无论如何，密码学一直以来都对网络的发展起到关键作用，而其不断的优化也使得网络信息的安全得到了更有效的保障。

参考文献：

[1]彭鸣戈，姚本武.密码学技术在网络信息安全中的应用[J].信息与电脑（理论版），2016（20）：193-194.

[2]吕彩霞.密码学技术在网络信息安全中的应用[J].科技广场，2011（09）：104-107.

[3]葛小虎.密码学技术在网络信息安全中的应用与发展[J].电子技术与软件工程，2020（06）：236-237.