1.密码学以及其在网络信息安全中的应用

计算机网络中的密码学就是在密码的编制与实践破解过程中发展开来的。密码学技术的研究成果就是世界中每个国家以及各个企业的高度机密。密码在各个国家的现代金融领域以及军事国防、贸易等实际应用方面都有着较大规模的实际运用。随着社会的不断发展 以及计算机网络技术的广泛应用，人们对于密码产生了更深的依赖性。计算机网络中的因特网分类就主要依赖于密码能够具体识别计算机用户的实际身份，当人们设置的密码被泄露或者被人们恶意破坏之后，随之产生的恶意、严重的后布偶就会在计算机联结成的因特网中，对于计算机应用中的用户识别时就会依靠密码，因此在密码被破译后就会带来一定的后果。

现代计算机网络技术中密码技术就是网络信息安全技术的核心，主要包含了对计算机的编码技术和实际分析技术。当前很多有着较高安全系数的有效密码算法以及密码学协议就会被密码学技术对应寻找到，并且能够充分满足用户的信息数据加密与数据认证方面的重要条件。当前计算机网络中的密码分析技术如果反过来运用假冒的认证信息或者运用密码学技术进行破译，进而有效窃取计算机网络机密或者对于计算机网络技术实施破坏的相关活动。因此这些影响计算机网络信息安全的活动既能够相互依存，还能够相互对立的表现，能够有效帮助计算机网络密码学技术得到进一步发展。

当前计算机网络中的密码学技术主要有两种技术分类，一类就是建立在数学应用的基础上，包含着密钥管理、VPN网络技术以及数字签名等。另一类并不是建立在数学应用技术的基础上，这类技术包含着建立在生物基础特征进行识别的应用技术，还有量子密码等等相关技术。在当前的计算机网络发展过程中只有合理的运用这些计算机密码学技术，才能够高效的建立起计算机网络信息安全体系并保证计算机网络信息的安全性。

私钥密码学技术：在计算机网络中私钥密码学技术有着一定的传统性，在计算机网络发展使用过程中，进行网络通信的双方共用同一个密码，其中一个通信用户用密码来进行数据与信息的加密，另一方则用来解密。私钥密码的加密与解密操作都是用同一个钥，并且一把钥只能打开一把锁，进而有助于进行简化的处理。当私有密钥没有被双方泄露时，就可以有效保证通讯双方信息内容的机密性与完整性。

公钥密码学技术：计算机网络运用过程中的公钥密码学技术又被称为非对称密码技术，每位计算机用户都会有相应的数学相关性密钥，分别是公开密钥和私密密钥，及时这两个密钥是成对生成的，但是仅仅知道其中一个密钥却不可以知道另一个密钥。计算机公钥密码学技术不仅能够保证计算机用户的网络信息与数据的机密性，还能够提升自身网络信息的可靠性。计算机公钥密码学技术能够让计算机网络通信双方在没有进行密钥交换时就能够进行安全通信，并且这种公钥密码学技术能够被广泛的应用在用户身份认证等重要领域。计算机公钥密码学技术一般都是建立在有难度的数学题基础上，并且有一定代表性的公钥密码体制被称为RSA。

密码学在网络信息安全中的实际应用：

起到加密保护的作用：计算机密码学技术的变换密码功能能够将明文合理的转化成合法用户能够自主解读出来的密文，这也是密码的一个基本功能。变换密码这一功能主要分为两种方式，分别称之为传输信息加密与存储信息的加密。前者就是对计算机网络中传输的各类信息进行加密，并且传输信息的加密可以被分为不同的加密层次，根据不同的保密需要进行分别采用。后者就是对计算机网络中存储的文件与实际数据进行加密，这种加密形式又被分为文件库的加密与数据库的加密。存储信息加密的难度系数较大，由于存在计算机数据加密与相应信息查询之间的各类矛盾，这种加密形式的关键性技术有待重点突破。

保证信息的完整性：为了有效防止计算机网络用户的信息被肆意篡改，相应的用户可以运用密码学技术来将相关网络信息与网络数据进行实际的运算，并产生一组对应的数据，也就是网络信息的验证码。在计算机网络用户的接收方接收到网络信息之后，就应当进行相应的实际同样运算，进而将最新产生的验证码与计算机网络用户所接受到的信息验证码进行比对，检验两者是否一折，进而确定计算机网络信息的正确性，运用这种信息验证的密码学技术能够及时的发现用户的信息是否遭到了破坏。

数字签名与身份验证技术的应用：计算机网络中的数字签名技术就是指用户对电子信息进行签名的实际运用方法。这种方法适用于公钥密码体制与私钥密码体制，但是公钥密码体制更有助于数字签名技术开展实际的应用与研究。数字签名在计算机网络中的应用研究有这几种方法：椭圆曲线的数字签名、有限自动机的数字签名等算法，不仅如此，它还涉及到了国家的法律相关问题，很多国家制定了专门的法律来规范数字签名技术。

2.结合密码学发展趋势，阐述密码学对社会经济发展的关键作用

随着数字技术的迅速发展，密码学的重要性在当前社会经济中变得越来越显著。密码学是一门研究信息安全的学科，它涵盖了数据加密、数字签名、认证协议等内容。密码学技术是保护数字信息安全的核心，对于现代社会经济的各个方面都具有关键作用。在本文中，我们将阐述密码学对社会经济发展的关键作用，并探讨其未来的发展趋势。

网络安全是数字经济发展的重要基石。密码学技术可以保护用户的隐私数据不被恶意攻击者窃取，保证网络交易的真实性和完整性，有效防止网络犯罪和信息泄露，维护了数字经济发展的稳健性和可持续性。随着人工智能和物联网技术的不断发展，网络安全问题将会变得更加复杂和严重。密码学技术将继续发挥其在保障网络安全方面的关键作用，以应对日益增长的网络攻击和数据泄露风险。

电子商务已成为现代经济的一个重要组成部分。数字签名技术可以保证电子商务中的合同和交易的真实性和完整性，数字证书可以验证在线商家和消费者的身份信息，有效降低了电子商务中的欺诈风险，推动电子商务的健康发展。未来，随着区块链技术的发展和普及，密码学技术将扮演更加重要的角色，以确保区块链上的数字交易的安全和真实性，促进数字经济的可持续发展。

金融安全是全球经济稳定的关键因素。随着金融业务的数字化、网络化和全球化，金融数据安全问题变得越来越复杂和严峻。密码学技术可以保护金融数据和交易信息不被黑客攻击和窃取，保障金融机构的信息安全和业务稳定，增强了金融市场的信心和稳定性。未来，随着区块链技术的广泛应用，密码学技术将在保障数字货币的安全和稳定方面发挥更加重要的作用。

在信息社会中，个人隐私受到了前所未有的侵犯。密码学技术可以有效地保护个人隐私信息不被盗取或滥用，确保了个人权利的保护和隐私安全。随着智能设备的普及和人工智能技术的发展，个人数据和隐私问题将变得更加复杂和敏感。密码学技术将继续发挥其在保障个人隐私方面的关键作用，以确保数字社会的公平和健康发展。

除此之外，密码学技术还具有广泛的应用场景，如政府机构、军事领域、医疗保健等领域。例如，在军事领域，密码学技术可以保障国家安全和战争胜利，确保军事通信和数据传输的保密性和可靠性。在医疗保健领域，密码学技术可以保护病人隐私和医疗数据的安全，推动医疗信息化和智能化的发展。

未来，随着量子计算技术和量子密码学的发展，密码学技术将进入一个全新的时代。传统密码学算法将面临破解的风险，因此需要采用更加安全和可靠的量子密码学算法。量子密码学技术可以实现无条件安全通信和数据传输，极大地提高了密码学技术的安全性和可靠性，将为数字社会的可持续发展提供更加强大的保障。

总之，密码学技术已经成为数字社会发展的基础和保障，它的重要性不断增加。它不仅在保障网络安全、促进电子商务发展、维护金融安全、保障个人隐私、促进医疗信息化和智能化等方面具有关键作用，而且还可以扩展到其他领域。例如，在区块链技术中，密码学技术可以保障数据隐私和交易安全；在物联网技术中，密码学技术可以保障设备通信和数据传输的安全。未来，随着数字技术的不断创新和发展，密码学技术也将不断更新迭代，以满足数字社会的安全需求和发展需求，为数字经济和数字社会的可持续发展提供更加强有力的支持和保障。