浅析密码学在信息安全中的应用

随着人们生活水平的快速提高和现代电子信息技术的发展，互联网开始走进千家万户，不断改变着人们的生活和工作方式。与此同时，也给人们的个人信息和隐私带来了极大的安全隐患。相关的恶性事件也多次被新闻媒体曝光，对网络信息安全提出了巨大的挑战。因此，密码学逐渐被业内人士发现并进行深入研究后，被广泛应用到网络信息安全中来，以确保网络信息达到真正意义上的安全。

1 密码学技术主要的分类

加密技术使确保网络信息安全的重要手段，工作原理就是将网络信息转化为密文，然后通过网络突进进行传送，即使被不法分子捕获，也无法识别其中的有效信息，在输出时，再将信息转化为人们交流使用的明文。通过这种方式来确保网络信息的安全。加密目前有两种主要的分类即专用密钥加密和非对称加密。

1.1 专用密钥加密或对称加密方法

专用密钥加密或对称加密主要的特点就是加密密钥和解密密钥是同一种密钥，大大简化了对信息加密的过程。传输双方要想获得有用的信息只需要共享就可以得到，不需要再进行交换彼此的算法[1]。但是这种方法有一定的缺陷，就是在信息传输过程中无法识别信息的发起方和信息的最终方，而且只能是一一对应的映射方式。

专用密钥加密的密钥总共是 56 位，在传统的 DES 加密技术的基础上，进一步优化改进成三重 DES，大大加大了信息的安全性。并且 RCZ 和 RC4 加密技术也逐渐被广泛应用，这种算法的密钥长度是可以改变的，可以根据不同的情况使用不同长度的密钥。

1.2 非对称加密或公共密钥加密方法

在加密过程中，密钥被进一步分解成一对密钥，这一对密钥中的任何一个密钥都可以作为公开的密钥被大量使用，但是为确保信息安全必须把另外一把密钥保存起来，由一方单独掌握。非对称密钥常用的加密方法就是 RSA 算法，它有一个明显的缺点就是运算的速度非常的缓慢[2]。在做一些信息量相对较大的加密算法时往往要花费很长的时间，因此处理较大信息量的加密问题一般都采用对称加密方法。

2 现阶段密码学在信息安全中的具体应用

密码学已经逐渐被人熟知并且在大学教学的课程安排之中。人们对密码的认识主要是密码编码和密码分析两个方面。显然，密码编码是针对密码算法安全性问题进行研究的，主要作用就是对信息进行加密。密码分析的作用恰好相反，就是用来对别的认证信息进行破解或者伪造的，目的就是窃取有用的信息。二者各有利弊，关键是看技术人员如何进行运用，在关键时刻也都能发挥重要的作用。

2.1 链路加密

链路加密在实际生活中的应用较少，主要在特定范围内进行运用。利用这种方法进行加密首先得对网络中的某一条链路进行解密，之后再对解密的链路进行二次加密。最重要的是这种加密方法要求设置大量的破译密码或者编制密码。虽然可以确保信息安全的通过链路抵达接受方，但也存在明显的缺点就是因为对某些节点忘记设置密码会成为被网络攻击的对象，影响整个链路的安全性。

2.2 节点加密

节点加密就是要对链路中的节点进行加密，可以看出是链路加密的细化加密动作，但是在安全性能方面，节点加密显然更有优势。节点加密是不允许以明文

的方式存在的，并且要求必须要设置一定的密码装置。但是节点加密也有明显的缺点就是整个加密过程的信息透明，容易受黑客攻击，存在一定的安全隐患，影响加密算法的安全性。

2.3 端端加密法

端端加密法是在链路加密和节点加密存在缺点的基础上加以改进后提出来的一种新的算法。这种算法使信息在传输过程中始终以密文的形式存在，不需要再进行二次解密，也不怕被黑客攻击，从而能够确保网络信息的安全。端端加密法的操作方法相比另外两种加密方法也更加简单，在安全性能方面也更加可靠，最重要的是成本也较低，因此得以被广泛应用。

3 结语

密码学已经成为信息安全领域必不可少的一门科学，在网络快速发达的今天其重要性不言而喻。本文对密码学的分类以及密码学的应用进行了深入的分析，以期促进业内人士对密码学这一学科的理解程度。当然本文的研究内容还存在许多方面的不足，比如对密码学的算法没有进行深入的分析，也没有厘清每种加密算法的具体应用领域。笔者将在今后的工作和研究中更加注重对密码学应用的具体研究，促进密码学在信息安全领域中更加广泛的应用。