Universe Scientific Publishing
Computer System Networking and Telecommunications
计算机系统网络和电信，2019,1(2)
ISSN:2661-3719 (Print); 2661-3727 (Online)

Talking about the Application of Data Encryption Technology in University Network Security

Mengfei JIA Zhengde BAO Chenxi LI
Jincheng College, Sichuan University, Chengdu 611731, China

Abstract

The continuous development of network information technology has promoted the construction of networked platforms in colleges and universities. At the same time, the issue of network information security has become increasingly prominent. There are still many problems in the network security of major universities. Various factors limit the security of colleges and universities. In-depth exploration of aspects. This paper mainly expounds the problems of campus network security and its application in colleges and universities, introduces the common algorithms of data encryption, and analyzes the application of data encryption technology in college network security.

Key Words

Network Security, Campus Network, Data Encryption Technology

DOI:10.18686/jsjxt.v1i2.638

浅谈数据加密技术在高校网络安全中的应用

贾梦飞 鲍正德 李晨曦
四川大学锦城学院，四川，成都，611731

摘 要

网络信息技术的不断发展推动了高校网络化平台的建设，与此同时网络信息安全问题日益凸显，各大高校网络安全仍存在许多问题，各种各样的因素限制了高校对于保障网络安全这一方面的深入探究。本文主要阐述了校园网络安全存在的问题以及在高校中的运用，介绍了数据加密常见的算法，并浅析了数据加密技术在高校网络安全中的运用。

关键词

网络安全；校园网；数据加密技术

1.引言

近年来，网络技术的不断发展和广泛应用，使其已经成为了高校学生学习和学生日常生活中必需的工具。但随之而来的数据失窃、个人信息倒卖等高校网络安全问题也浮出水面，给高校的网络信息安全埋下了很大的安全隐患，把数据加密技术应用于高校长期网络规划和建设以及网络数据库资源之中，同时数据加密技术对数据和软件进行相应的数据加密。可以很好地的维护校园网的安全。

2.高校网络安全存在的问题

2.1 学生不重视网络安全

随着互联网技术的不断发展和大学生人数的不断增加，整个校园个人网络也在迅速增加。经过了三年的鏖战，踏入大学校园之后，学生们的心思大多花在了网络游戏和日常追剧之中，对计算机一般故障都了解甚少，网络安全这一方面更是没有引起足够的重视。比如2017年的勒索病毒事件，学子们恰逢毕业季，全国各大高校的毕业生们都在紧张的撰写毕业论文，突如其来的网络病毒攻击使学生陷入勒索的噩梦。校园网成为了重灾区，许多学生的毕业设计被加密只有支付固定赎金才能解密。校园网络安全问题是一个摆在眼前的问题，

学生一定要足够的重视网络安全这个问题，加强网络安全意识，未知网站链接不要去点，未知文件不去下载，不清楚邮件不要打开。

2.2 研究重心偏离

网络信息技术在教育领域得到广泛的应用，而在具体的网络技术运用过程中，相应的网络安全问题却不断显现出来，严重威胁着校园网络的安全。大数据和人工智能的快速发展，更是将所有的目光转移到这个热门话题上，但它从根本上忽略了保证大数据和人工智能健康发展的网络安全问题。就算是研究，也只是专注于对信息的拦截与屏蔽。通过调查可知，许多高校将防止垃圾信息和阻止不健康信息的网络安全管理放到首位，缺忽视了对非法入侵防范和网络病毒防范系统的建设，这也使得校园网在运行和维护阶段面临着巨大挑战。

2.3 校园网络安全体系不完整

校园网络安全是校园内部网络搭建的主要内容，高校人数庞大，对于网络稳定性和网络安全有着更高的要求，这使得校园网络规划显得极为重要。

一方面是由于校园网络安全建设资金投入不足，很多高校特别是民办高校不愿意去购买昂贵的网络安全设备，校园网安全问题没有明确规定，甚至存在网络安全意识不足等问题。一系列因素导致了很多高校没有配置达到标准的网络安全设备。还有一大批高校购买了网络安全设备，但也只是一些低端的网路设备产品，没有足够的能力去应对网络攻击以及病毒的入侵。资金问题大大降低了校园网的安全性。另一方面是在校园网络实际搭建的过程中，一些工作人员专业知识不够扎实以及对校园网络环境不够了解等，导致网络综合布线不够科学，设备安装不合理，存在很高的安全隐患。另外还存在校园网络设备老旧，机房设备维护不当等因素，这都是校园网络安全所面临的问题。

3.数据加密技术的常见算法

3.1 DES 算法

DES 算法是目前最为普遍的加密算法之一，DES 算法是使用同一个密钥来加密和解密数据，数据加密应用过程中，DES 算法应用频率更高一些。作为分组密码，DES 具有典型的 Fesistel 结构，其分组长度为 64 位，有效长度为 54 位，剩余的为奇偶校验位。[1]DES 函数是整个 DES 的核心，函数由四部分组成，分别为拓展的换比特盒、增加密钥、一组换字盒和一个直接换比特盒。DES 算法对明文进行一连串的排列和替换操作来对其加密，加密数据的关键就是从已有的 16 个初始子密钥函数，每个子密钥按顺序对数据执行一系列位操作，总共重复 16 次。除了以子秘钥的相反顺序处理加密数据之外，还可以使用相同的过程来进行解密加密数据。

3.2 AES 算法

AES 算法有三种类型的密钥，一般 AES 算法为 AES-128 密钥，密钥的长度为 128bit，分组的长度为 128bit，通常的加密轮数为 10 次。AES 算法加密涉及到四种操作：字节替换，行移位，列混淆和密钥加。[2]解密过程就是分别为对应的逆操作。因为操作的每个步骤都是可逆的，所以可以以相反的顺序解密算法以恢复明文，加密和解密过程中的每一轮密钥都是从初始密钥扩展派生的。

3.3 RSA 算法

RSA 算法的密码体质是理论上迄今为止最成熟，最完善的公钥密码，是现代非对称密码的典型代表。[3]RSA 算法的步骤大致是密钥生成，加密算法和解密算法。

(1)产生两个不同的质数 m，n 计算 p=m*n；

(2)用欧拉函数计算 r=φ(p)=φ(m)φ(n)=(m-1)(n-1)；

(3)选取一个小于 r 并且和 r 互为质数的整数 e；

(4)求出整数 e 有关于 r 的模反元素 d；

(5)取(p,e)是公钥，(p,d)是私钥，p 和 e 都会公开，私钥中的 d 泄露的话加密就失去了意义；

(6)最后是进行相应的加密运算和解密运算;

ci=(bi)emod p

bi=(ci)dmod p

可以将明文 bi 加密成密文 ci 或者将密文解密成明文。

4.数据加密技术在校园网信息安全中的使用

4.1 在教务系统中的应用

高校教务系统是学校处理教学相关事宜的综合管

理系统，教务系统在高校所有系统中一直处于核心地位。[4]学生对课程表，最终成绩查询和一些考试查询的查询都是在教务管理系统上进行的，因此教育管理系统的安全性至关重要。但是由于系统应用软件本身就存在安全性方面的漏洞以及校园网络运行的环境中存在有些许的安全隐患，会对教务系统数据的完整性造成严重的威胁。在教务管理系统中运用数据加密技术，对相关教学任务以及老师学生需要查询的资源等进行相应的数据加密，对校园网外的教务系统网络请求访问进行身份验证识别和过滤网站中垃圾信息，这样能够很好地防止由于系统软件的本身漏洞以及网络攻击带来的危害。

4.2 在图书馆系统中的应用

由于计算机网络的不断发展，数字信息资源正日益取代传统的纸质信息资源。图书馆系统管理着大量的电子图书，图书馆的地位在校园中尤为重要。传统的图书馆管理系统大多只能对电子图书进行大致分类进行集中管理，通常每名学生都被授权访问电子图书馆，图书馆系统在接受请求访问上的安全性不高，一些电子图书资源还很容易受到黑客的盗取和病毒的攻击。因此在图书馆管理系统中融入数据加密技术也显得尤为重要，对特定信息资源进行数据分类分组加密，它可以提高图书馆管理系统的整体安全性，也便于管理人员为系统的日常运行和定期维护提供可靠性。伴随着计算机技术的飞速发展，软件数量不断增加，有关计算机信息盗取事件时发，为了避免这种情况的发生，可以将数据加密技术运用到图书馆管理系统中对相关软件进行加密，为信息安全提供强有力的保障。

4.3 在网络数据库系统中的应用

网络数据库管理平台它的安全级别一般可以定义在 C1 级别或者是 C2 级别。[5]网络数据库通常使用网络操作系统作为管理载体，通常使用 Windows 服务器或 Windows NT 作为管理数据库的操作系统。但这些系统软件安全性能相对较低，在运行中由于病毒故障或软件故障，易导致软件瘫痪；在传输信息的过程中，很容易被黑客拦截。数据库网络中存储着大量学生和老师的个人信息以及学校存放的各类文件，显然这些操作系统的安全性是满足不了的。因此，在网络数据库中融入数据加密技术可以对这些数据文件起到很好的保护作用，充分的利用数据加密技术不但可以防止一些不法分子盗取学校信息进行倒卖，它还保持了计算机内部系统的稳定性。

5.结论

随着网络信息技术的发展，网络技术在高校中的应用也越来越广泛，成为了学生学习和老师工作便捷的工具。但是，校园网络技术的应用过程中仍存在许多安全问题。例如计算机病毒、木马病毒、数据库资源泄露、系统遭到攻击和网络通信遭黑客拦截等，利用数据加密技术保障网络安全，为校园网络营造一个安全的环境，也有助于推动全国高校网络安全的长期发展。

参考文献

[1]詹鹏伟，谢小姣.DES 与 AES 算法实现及其在图像加密中的效率探究[J].网络安全技术与应用，2018(09):41-42.
[2]王方鑫.基于 AES 算法的研究[J].民营科技,2018(12):189.
[3]兰海兵，程胜利.RSA 算法及其实现技术的改进研究[J].交通与计算机，2006(01):95-97.
[4]徐卫克.高校教务系统的数据处理和分析[J].电子技术与软件工程，2019(03):156-157.
[5]张鑫，金双.浅论计算机网络信息安全中数据加密技术[J]. 山东工业技术，2019(05):146.

作者简介

第一作者：贾梦飞（1999-），男，汉，河南省信阳市，本科，四川大学金城学院，研究方向：电子商务
第二作者（通讯作者）：鲍正德（1989-），男，汉，黑龙江省哈尔滨市，研究生，四川大学锦城学院，研究方向：电子商务。
第三作者：李晨曦（1998-），男，汉，贵州省贵阳市，本科，四川大学锦城学院，研究方向：大数据技术开发