计算机工程与应用 2008 44 (24): 208-211 ISSN: 1002-8331 CN: 11-2127/TP

工程与应用

基于PKI的网络考试安全机制研究及实现——全国大学生数学建模竞赛考试系统的研究与实现

王尚平, 谢小琢, 张亚玲, 牛鹏超

西安理工大学 计算机科学与工程学院，西安 710048

收稿日期 2007-10-25 修回日期 2008-1-24 网络版发布日期 2008-8-19 接受日期

摘要 针对全国大学生数学建模竞赛系统中试题集中发放、答卷集中收交及身份认证和答卷完整性等安全问题进行了分析，提出了基于PKI的相应解决方案。综合运用加密、数字签名、数字证书及时间戳技术实现了试题及答卷在发放和收交过程中的保密性、完整性、不可否认性及试卷评阅中可能出现的作弊等安全问题，用加密技术和时间戳技术解决试题集中下载和试卷集中提交中的时效性问题。最后基于B/S模式下实现加密与数字签名的问题，开发了试题加解密、数字签名和提供时间戳服务的智能客户端程序。

关键词 加密 数字签名 数字证书 时间戳 智能客户端

分类号

Research and realization of secure system of Internet exam in modeling based on PKI——research and realization of the system of China undergraduate mathematical contest

WANG Shang-ping,XIE Xiao-zhuo,ZHANG Ya-ling,NIU Peng-chao

Xi’an University of Technology，School of Computer Science and Engineering，Xi’an 710048，China

Abstract

Aiming at the four problems of downloading the contest paper simultaneously，submitting the answer papers simultaneously，validating the identity of players and validating the integrality in the China undergraduate mathematical contest in modeling，a corresponding PKI-based security solution is put forward with the help of comprehensive application of data encryption，digital signature，digital certificate and time-stamp technique to solve a series of security problems such as privacy，integrality，undeniability and cheat-preventing.At the same time，the time efficiency in the process of downloading and submitting test paper are solved with the help of encryption and time-stamp.Finally，concerning the problems of implementation of encryption and digital signature in B/S mode，it develops a smart client program for contest test with paper encryption，digital signature and time-stamp functions.

Key words encryption digital signature digital certificate time stamp smart client

DOI: 10.3778/j.issn.1002-8331.2008.24.063

通讯作者 王尚平 xiaozhuoyh@126.com