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

西安理工大学 计算机科学与工程学院,西安 710048
Xi'an University of Technology,School of Computer Science and Engineering,Xi'an 710048,China
E-mail:xiaozhuoyh@126.com

WANG Shang-ping,XIE Xiao-zhuo,ZHANG Ya-ling,et al.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.Computer Engineering and Applications,2008,44(24):208-211.

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

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
DOI:10.3778/j.issn.1002-8331.2008.24.063 **文章编号:**1002-8331(2008)24-0208-04 **文献标识码:**A **中图分类号:**TP393.08

1 引言

计算机网络的飞速发展,正影响并改变着人们的生存观念和生活方式,使很多领域发生了天翻地覆的变化。基于计算机网络的考试系统将带来考试方式的革命。网络考试体系彻底改变了传统的考试方式,传统的考试方式需要运用交通运输方式发放和提交试卷,手续繁琐、缓慢及效率低下,网络考试使得考试变得便利、高效,实现了自动化、网络无纸化并且可以节省大量的人力物力。但是,在提供很多方便的同时,新的问题伴随而生。

在网络化全国大学生数学建模竞赛考试中,存在这样几个问题。首先是试题发放,因为竞赛需要在全国范围内同时展开,有成千上万的参赛队参赛,参赛队需要在第一时间同时从网络服务器下载试题,而现在的题目又都含有大量的数据(全国大学生数学建模竞赛试题的数据有的多达几兆),因此,每年都会发生服务器拒绝服务, 很多队伍在很长时间不能及时得到试题,影响到竞赛的公平性。如何高效、安全可靠同时提供试题,是一个首先需要解决的问题。第二个问题是试卷的收交问题,即需要按时确保每个队伍在规定的时间同时交卷,因为竞赛试题难度大,时间紧张,很少有提前交卷,因此如何解决瞬时大量的试卷安全高效提交,是需要解决的第二个问题。第三个问题是竞赛中的身份认证问题,如何有效地管理和识别身份是一个重要的问题;第四个问题是试卷的完整性问题,即试卷在网络提交到最后的阅卷结束,如何防止试卷被修改,防止恶意的篡改,保证竞赛结果的公平性这也是一个重要的问题。

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60273089)。
作者简介:王尚平(1963-),男,博士,教授,研究方向为密码理论与网络安全;谢小琢,硕士,研究方向为数据与网络信息安全;张亚玲,博士,副教授,研究方向为网络安全、协同设计;牛鹏超,硕士,研究方向为数据与网络信息安全。
收稿日期:2007-10-25 **修回日期:**2008-01-24

这些问题可以规约为如何保证信息的机密性、真实性、完整性和不可否认性。

本文针对全国大学生数学建模竞赛系统中试题集中发放、答题试卷集中收交及身份认证和答卷完整性等安全问题,提出了基于 PKI 的相应解决方案。用数据加密技术实现了试题集中发放问题,数字签名、数字证书及时间戳技术实现试题答卷在收交和评阅过程中的时间认证、完整性、不可否认性及评阅中可能出现的作弊等安全问题。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。

2　相关知识[4,6]

PKI 是"Public Key Infrastructure"的缩写,意为"公钥基础设施"。简单地说,PKI 技术是以公开密钥密码学为理论技术基础的一整套网络信息安全技术设施与服务,内容包括数字证书、公钥密码技术、认证中心、证书和密钥的管理、安全代理软件、不可否认性服务、时间戳服务、相关信息标准、操作规范等。PKI 体系结构如图 1 所示。PKI 体系结构包括以下 5 个部分:

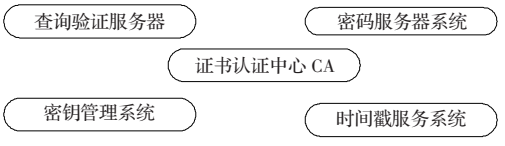

图 1　PKI 体系结构

(1)查询验证服务器提供证书发布、证书状态在线查询服务;

(2)密码服务系统提供加解密、签名及签名验证服务;

(3)证书认证中心 CA 是证书业务服务系统的核心业务节点和基本单元,主要提供身份证书的签发和发布服务。它是权威机构,是可信的;

(4)密钥管理系统负责向 CA 中心提供密钥服务,包括密钥的产生、登记、分发、注销、归档及恢复等服务;

(5)时间戳服务系统提供精确可信的时间戳,保证处理数据在某一时间(之前)的存在性及相关操作的相对时间顺序,为业务处理的抗抵赖性和可审计性提供有效支持。

3　全国大学生数学建模竞赛安全系统分析及解决方案

全国大学生数学建模竞赛安全系统主要涉及到网上试题集中发题的问题、网上答卷集中提交问题、竞赛中的身份认证和答卷评阅中的完整性四个问题,具体分析情况如下:

3.1　网上集中发题的问题

传统的做法是数模竞赛比赛开始时,全国有成千上万个队同时在指定的时间从网上下载比赛试题,这样一来服务器难于处理,会出现拒绝服务现象。为了避免此种现象,本系统采用的方案是:提前将试题用高级加密算法 AES 加密[3],将试题密文提前在网上公布,供各参赛队伍提前下载,参赛队提前下载安全客户端(解密)软件,等到比赛开始时候,网上公布解密密钥,解密密钥非常的短,一般为 128 bit,这样参赛队比赛开始后,获取密钥,利用密钥本地解密,及时得到竞赛试题。系统采用智能客户端模式实现了安全客户端软件。

3.2　网上集中提交试题问题

数模竞赛结束时,传统的做法是各学校集中提交书面打印文档到各省指定的学校,这样遇到很多问题,同一个都市,交卷时间相差数小时,外地的(远离省会城市的)是通过特快专递,时间是看特快专递的时间,而这个实际并不可靠。利用传统的网络方法把试卷同时上传到竞赛中心服务器又会遇到拒绝服务问题。本系统为了避免上述现象并且保证每个队能够在规定的时间前,比如说比赛结束几个小时之内,把答案提交到服务器,又确保提交的答卷是比赛结束时间以前的文档。系统的解决方案是竞赛结束时先对这个文档加盖时间戳,具体做法是参赛队伍在比赛结束时,利用安全客户端软件提供的哈西算法(SHA-1)计算文档的信息摘要,这样以参赛学校为单位,将每个参赛队伍的答卷的信息摘要汇总,及时提交到服务器,由服务器加盖时间戳,并对时间戳进行数字签名。同时将该签名保存在服务器,并下发给各参赛队伍。这样比赛结束后,各队都不能修改答卷,否则以后提交的答卷作废。这样也可以使参赛队伍,在比赛结束的几个小时之内提交答卷,并确保提交的文档是没有被修改的文档。服务器端可以对提交的文档利用签名进行验证。

3.3　竞赛中的身份认证

系统中的身份认证模块实现需要实现客户端与服务器的双向身份验证。因传统的网络认证模式无法确保客户端与服务器之间的相互认证以及安全通信,为了避免攻击者冒名发布试题或提交试卷必须要实现服务器对客户身份的认证,同时为了防止攻击者恶意破坏,客户端也需要对服务器进行认证并且实现安全通信。

方案的前提是首先各竞赛队伍和竞赛中心服务器各携带身份信息到证书认证中心 CA 申请公钥证书。证书认证中心 CA 首先审核用户身份资料是否合法和准确,审核通过之后分别产生私钥和公钥,将私钥返回用户,证书认证中心利用公钥给用户颁发公钥证书,然后将公钥证书发布到查询验证服务器和密钥管理系统。

双方进行通信的具体流程是[6]:(1)首先客户端产生一个随机数 n_1,将随机数 n_1 发送给服务器,本地保留随机数内容;(2)服务器用其证书的私钥对随机数 n_1 进行签名,然后在本地产生随机数 n_2,本地保留随机数 n_2 内容,之后将其对随机数 n_1 的签名值、服务器公钥证书和随机数 n_2 一块发送给客户端;(3)客户端接收到服务器发送过来的签名值、服务器公钥证书和随机数 n_2;(4)客户端查询验证服务器证书的有效性,如果该证书有效,利用服务器公钥证书对得到的随机数 n_1 的签名值进行验证签名,如果验证失败退出,否则客户端对服务器的身份认证通过;(5)客户端用其证书的私钥对随机数 n_2 进行签名,然后将客户端对随机数 n_2 的签名值和客户端公钥证书一并发送给服务器;(6)服务器得到客户端发送过来的签名值和客户端公钥证书。服务器端查询验证客户端公钥证书。如果该公钥证书有效,利用得到的客户端公钥证书对客户端发送过来的对随机数 n_2 签名值进行验证签名,如果验证签名失败退出,否则服务器对客户端的身份认证通过;(7)双向身份认证结束,客户度与服务器双方进行正常通信。

3.4　答卷的完整性

在竞赛中,试题答卷的保管和评阅过程中都可能会发生答卷被替换、修改和恶意篡改等舞弊行为,为防止这种现象发生,本系统采用时间戳方案解决试卷的完整性问题。具体做法是:竞赛结束时,用客户端软件先计算答题试卷的 Hash 值,然后用这个 Hash 值向时戳服务器请求时间戳,客户端软件系统保存

返回的时间戳,并对答卷利用客户端私钥进行数字签名。最后将答卷、数字签名连同时间戳一起提交到服务器端数据库,数据库端在数据入库时验证签名和时间戳的正确性。组委会在必要时可以验证签名及时间戳,这样确保答卷是竞赛结束前已存在,无论在提交还是评阅过程中都无法换改。

4 系统具体设计及实现

4.1 系统结构图

微软.NET的CAPICOM组件封装了加密体系模型(CryptAPI)的一些复杂操作,利用ActiveX和COM对象进行加密和数字签名,能够实现B/S模式客户端加密和数字签名。很多应用系统在实现Web系统加密及数字签名时都选择CAP ICOM组件,依靠它能方便地获取客户数字证书及其私钥的特性。但是利用CAP ICOM组件开发存在一些弊端:首先,客户需要手动注册CAP ICOM.DLL,这为系统的部署带来诸多不便;其次,CAPICOM的实施需要在客户端下载安装ActiveX控件,而其本身存在着安全隐患[7]。

为了解决上述问题,本文采用智能客户端架构,综合应用数字证书、加密和数字签名技术,开发了试题文件的加密、数字签名和提供时间戳服务的客户端软件,并且实现了客户端与服务器之间的相互认证,确保了传输信息的机密性、完整性以及不可否认性。系统结构如图2:本系统主要由客户端(数模竞赛组委会客户端、参赛队客户端)、数模竞赛中心服务器、时间戳服务器和数字认证服务器组成。

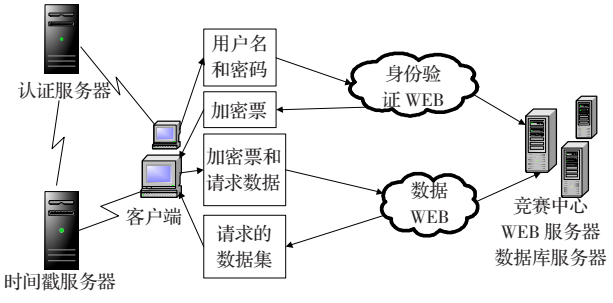

图2 数模竞赛系统结构图

4.2 安全实现原理

4.2.1 试题加密/数字签名实现原理

为了保证试题的机密性,使用对称加密算法加密试题,加密密钥以及初始化向量暂保存本地安全位置;实施数字签名与传统不同,在此是对试题的密文文档进行签名,依此来确保参赛队下载试题之后得到密钥之前,试题是保密的。加密与数字签名实现原理如图3所示。

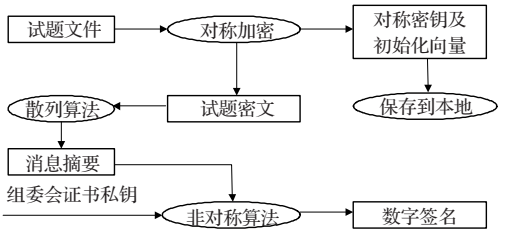

图3 试题加密/数字签名实现原理

4.2.2 试卷时间戳和签名实现原理

竞赛结束时,为保证试卷的完整性并且提高实施时间戳请求及数字签名的速度,首先对试卷进行散列运算,形成数字摘要。为防止存放和评阅过程中舞弊行为的发生,确保试卷在答题结束之前已存在,参赛队须对计算得到的试卷电子文档的信息摘要向时间戳服务器请求时间戳。最后为了保证试卷的不可否认性,对试卷的数字摘要实施数字签名。试卷时间戳、签名实现原理如图4所示:

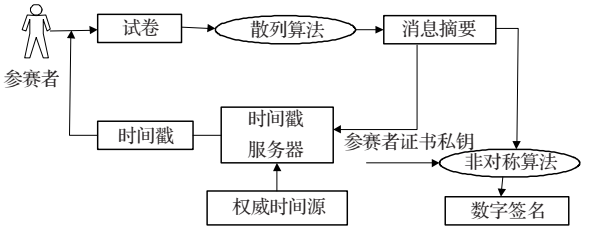

图4 试卷时间戳、签名实现原理

4.3 系统安全工作流程

4.3.1 符号说明

为了使得系统的形式化描述更加清晰,将定义以下符号来对系统工作方式及流程进行形式化的描述:

P_i:代表第 i 个参赛队;

O:代表竞赛组织委员会,简称组委会;

Q:代表竞赛试题;

A_i:代表第 i 个参赛队的答题试卷

T_i:代表文件 i 的时间戳;

S_W:代表竞赛中心服务器;

S_T:代表时间戳服务;

$SmartClient$:代表加解密智能客户端软件;

Key:代表加解密的对称密钥;

$E_{key}(m)$:表示用 key 对消息 m 加密;

$D_{key}(c)$:表示用对密文 c 解密;

$Cert_i$:代表主体 i 的x509v3证书;

PK_i:代表包含在主体 i 的x509v3证书中的公钥;

SK_i:代表通信方 i 对应于公钥 PK_i 的私钥;

$Hash:\{0,1\}^* \rightarrow \{0,1\}^l$ 代表哈西函数;

$Sign_{sk_i}(m)$:代表通信方 i 对消息 m 的签名;

$Verify_{pk_i}(m,\sigma)$:代表用通信方的公钥 pk_i 验证消息 m 的数字签名 σ。

4.3.2 工作流程图解及描述

系统安全的简化工作流程如图5所示:

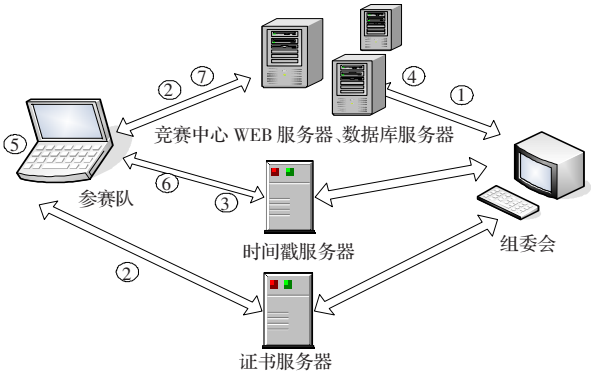

图5 系统工作流程图

其中相关过程描述如下:

(1)$O\rightarrow S_W$:$E_{Key_Q}(Q)$,$Sign_{Sk_O}(E_{Key_Q}(Q))$,$O$ 对称加密试题,并本地安全保存对称密钥 Key_Q,然后对试题密文进行签名,最后把 $E_{Key_Q}(Q)$,$Sign_{Sk_O}(E_{Key_Q}(Q))$提交到 S_W Web 服务器上,并在网上提前公布供下载。

(2)$P\leftarrow S_W$:$E_{Key_Q}(Q)$,$Sign_{Sk_O}(E_{Key_Q}(Q))$*SmartClient*,$Cert_O$,$P$ 从网上下载 $E_{Key_Q}(Q)$,$Sign_{Sk_O}(E_{Key_Q}(Q))$及加解密安全智能客户端软件 *SmartClient* 和组委会 O 的 x509v3 证书 $Cert_O$:

$Verify(Cert_O)=accept$

(3)p:$Verify_{pk_O}(E_{Key_Q}(Q),\sigma)=accept$,$\sigma=Sign_{Sk_O}(E_{Key_Q}(Q))$,$P$验证组委会 O 的 x509v3 证书的有效性,验证签名 $\sigma=Sign_{Sk_O}(E_{Key_Q}(Q))$ 的正确性,正确后保存 $E_{Key_Q}(Q)$文档并安装 *SmartClient* 软件,否则退出。

(4)$O\rightarrow S_W$:Key_Q,比赛开始时,网上公布 $E_{Key_Q}(Q)$的解密密钥 Key_Q。

(5)$P\leftarrow S_W$:Key_Q P:$Q=D_{Key_Q}(E_{Key_Q}(Q))$;$P$ 下载解密密钥 Key_Q,在 *SmartClient* 中利用 Key_Q 对 $E_{Key_Q}(Q)$解密得到试题 Q 并开始答题。

以上所述步骤属于试题集中发放过程,在这一过程中,主要运用了对称加密,数字证书及数字签名技术。下面是竞赛结束后试卷集中提交的过程:参赛队的答卷为 A。

(6)$P\leftrightarrow S_T$:$Requst(T_A)$,$Responce(T_A)$,P 计算试卷信息摘要 $HASH(A)$,然后用 $HASH(A)$向 S_T 发送 $Requst(T_A)$,S_T 响应 $Responce=Sign_{sk_{S_T}}(Hash(A),T_A)$返回 P,P 保存 T_A 和 $Responce=Sign_{sk_{S_T}}(Hash(A),T_A)$。

(7)$P\rightarrow \begin{matrix} S_W:A,T_A,Sign_{Sk_P}(A,T_A) \\ Sign_{sk_{S_T}}(Hash(A),T_A) \end{matrix}$,$P$ 把给 S_W 数据库服务器。

最后,组委会分发试卷给评卷员进行评卷。如果组委会对评阅中可能出现的舞弊需要查处,可以查阅服务器的数据库进行签名验证,哈西值比对,杜绝作弊行为。

试卷提交过程中主要运用了时间戳服务、对称加密和签名等技术。

5 结论

本文主要从全国大学生数学建模系统的试题发放和试卷提交过程中存在的难点问题和安全需求出发,经过分析、研究,提出了一套安全的解决方案,并在此基础上利用 B/S 和智能客户端模式相结合的模式实现了系统。此系统使得数模竞赛在网络方式下可以方便、快速、安地的运行,但这也只解决了试题发放和试卷提交两部分功能,要使系统得以完善,还需要做到阅卷过程中的很多管理流程,其中包括密封试卷,回避、计分和排序等很多实际工作。

参考文献:

[1] [美]William Stallings.Crytography and network security:principle and practices[M].4 版.北京:清华大学出版社,2006:21-56.

[2] Adams C,Cain P,Pinkas D,et al.Internet X.509 public key infrastructure Time Stamp Protocol(TSP),RFC3161[S].2001-08.

[3] 呼玮,石志寒,徐海龙.高级加密标准 Rijindael 算法研究与实现[C]//中国通信学会青年工作委员会.通信理论与技术新进展:第十一届全国青年通信学术会议论文集,中国四川绵阳,2006.

[4] 关振胜.公钥基础设施 PKI 与认证机构 CA[M].北京:电子工业出版社,2002:1-92.

[5] 邹建锋,周山峰,项细威.C# 企业级开发案例精解[M].北京:人民邮电出版社,2006:25-26.

[6] 周琦,郑学风.基于 PKI 体系结构的双向身份认证模型[J].电子科技,2005(3):36-37.

[7] 张璐,张景,井浩,等.网络采购系统中安全机制的研究与实现[J].计算机应用,2007,27(2):318-323.

(上接 196 页)

局部特征的人脸识别中,由于待识别脸像中嘴部开合变化很大(与该测试者的其它样本相比),基于局部特征的方法识别效果较差,而基于全局的方法得出了正确的结果。将基于局部特征和全局特征的方法进行融合可以得到更好的识别效果。

参考文献:

[1] Chellapa R,Wilson C L,Sirohey S.An human machine recognition of faces[J].Proceeding of The IEEE,1995,83(5):705-740.

[2] Zhou D L.A study of human face recognition[D].Xi'an:Northwestern Polytechnical University,2001.

[3] Tian Y,Tan T,Wang Y H.Do singular values contain adequate information for face recognition[J].Pattern Recognition,2003,36(6):649-655.

[4] Foley D H,Sammon J W.An optimal set of discriminant vectors[J].IEEE Trans Compute,1975,24(3):281-289.

[5] Duchene J,leclercq S.An optimal transform for discrimination and principal component analysis[J].IEEE Trans on Pattern analysis and machine Intelligence,1998,10(6)978-983.

[6] Belhumeur P,Hespanha J,Kriegman D.Eigenface vs.Fisherfaces:Recognition using class specific linear projection[J].IEEE Transaction on Pattern Analysis and Machine Intelligence,1997,19(7):711-720.

[7] Turk M,Pentland A.Eigenfaces for Recognition[J].Journal of Cognitive Neuroscience,1991,3(1):71-86.

[8] Cevikalp H,Discriminative common vectors for face recognition[J].IEEE Transactions on Pattern Analysis and Intelligence,2005,27(1).

[9] Zhao W,Chellappa R,Rosenfeld A,et al.Face recognition: a literature survey[R].Computer Vision Laboratory,University of Maryland,Technical Reports CAR2TR2948,2000.

[10] 陈伏兵.人脸识别中鉴别特征抽取若干方法研究[D].中国优秀博士论文,2006.

[11] 周德龙,高文,赵德斌.基于奇异值和判别式 KL 投影的人脸识别[J].软件学报,2003,14(4).

[12] 王蕴红,范伟,谭铁牛.融合全局和局部特征的字空间人脸识别算法[J].计算机学报,2005,28(10).