摘　要

计算机网络技术的发展和应用便利了社会、生活的方方面面，而无纸化考试更作为一个具有广泛前景的应用领域变革了传统的考试方式。随着无纸化考试系统的研究与发展，以互联网技术为基础的无纸化考试系统也同样需要面对由互联网络带来的信息安全问题，因而对无纸化考试系统的应用层通信安全机制展开全方位的研究便具有较大的理论价值和现实意义。

在探讨了无纸化考试系统的应用层通信安全机制所涉及的相关技术以及无纸化考试系统的体系架构和安全需求的基础上，从设计原则、各模块功能的实现上进行了详细的分析与论述。阐述了无纸化考试系统的应用层协议模型的设计，探讨了身份认证模块的构成和工作流程，给出了数据加密模块的加密策略。这些分析和设计构成了无纸化考试系统的应用层通信安全机制实现的基础。

在无纸化考试系统应用层通信安全机制详细设计的基础上，给出了各功能模块中核心内容的具体实现。讨论了通信服务器和考场管理客户端中的应用层协议处理流程，阐述了身份认证模块及其子模块的功能实现，论述了数据加密策略的算法实现细节。

实际应用结果表明，所建立的应用层通信安全机制能够为无纸化考试系统提供良好的安全通信保障，并具有较好的普适性和可扩展性，对增强类似应用系统的安全性具有一定的参考价值。

关键词：无纸化考试，信息安全，应用层通信，身份认证，密码体制

Abstract

Development and application of the computer network technology makes convenience in all aspects of our society and life, and paperless examination as a widely prosperous subject field has changed the traditional examination method. Along with the research and development of paperless examination system, the paperless examination system based on the Internet technology has to face the information security problems brought by Internet, hence it is with great value and practical significance to do the research of the communication in application layer omnidirectionally.

Based on the analysis of relevant technologies about the communication in application layer, the system architecture and the security requirement of paperless examination system, the design principle and the implementation of functional modules are particularized. The design of the application layer protocol model of paperless examination system is expounded, while the composition and workflow of the identity authentication module and the encryption strategy of the data encryption module are discussed. These analysis and design constitute the implementation foundation of the security mechanism about communication in application layer for paperless examination system.

On the basis of the detailed design of the security mechanism about communication in the application layer for paperless examination system, the specific implementation of the core for every functional model is presented. The processing workflow for the application layer protocol of communication server and examination manager client are discussed. And then the functional implementation of the identity authentication module and its sub-modules are described, while the implementation details about the algorithm of encryption strategy is expounded.

The practical application indicates that the security mechanism of communication in

the application layer can provide an well security guarantee for paperless examination system, and it has great universality, good expansibility and certain reference value to enhance the security requirements of similar application systems.

Key Words: Paperless Examination, Information Security, Communication in Application Layer, Identity Authentication, Cryptography

独创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除文中已经标明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到，本声明的法律结果由本人承担。

学位论文作者签名：

日期：　　年　　月　　日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，即：学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权华中科技大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本论文属于　　保　密 □，在_____年解密后适用本授权书。

　　不保密 □。

（请在以上方框内打“v”）

学位论文作者签名：　　指导教师签名：

日期：　　年　　月　　日　　日期：　　年　　月　　日

1 绪论

1.1 课题研究背景

互联网技术的迅速发展，使其以前所未有的深度和广度渗透到社会生活的各个方面，传统的信息交互方式已然被基于互联网技术的新方式所延伸或取代。电子邮件、电子商务、电子政务、即时通讯和网络游戏等互联网技术应用极大地丰富和便利了人们的日常生活，而无纸化考试、网上阅卷等此类计算机辅助系统的使用更是颠覆了相关的传统工作模式，带来了成本、效率上的显著改善。然而，在互联网技术发展的同时，针对互联网传输信息进行的窃取、截取、伪造、篡改、重放、冒充等恶意行为越来越普遍，并给社会带来了直接或者间接的经济损失。因此，互联网的信息安全问题亦成了必须被面对和解决的重要问题。

信息安全的内涵伴随着其发展与应用在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防守）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。信息安全是一个综合、交叉学科领域，它要综合利用数学、物理、通信和计算机诸多学科的长期知识积累和最新发展成果，进行自主创新研究，加强顶层设计，提出系统的、完整的解决方案。与其他学科相比，信息安全的研究更强调自主性和创新性，自主性可以避免“陷门”，而创新性可以抵抗各种攻击，适应技术发展的需求[1]。

无纸化考试系统将整个考试工作（试题导入、试题管理、试卷生成、试卷管理、考试管理以及试卷评定等）全过程电子化、信息化和无纸化，从而克服了传统的笔试考试的许多弊端，并且降低了成本、提高了效率。然而，考试过程本身的公平、公正性以及试题答案的安全、保密性仍然必须被保证，而这些需求的实现正是信息安全领域所涉及和研究的范畴。因此，结合信息安全相关技术与无纸化考试系统特点进行无纸化考试系统的应用层通信安全机制的研究便具有了重要的意义和价值。

1.2 国内外的研究现状

1.2.1 无纸化考试的发展现状

随着计算机及通信技术为代表的信息技术的发展，各种各样的无纸化考试系统也应运而生，但整个考试流程仍然是相同的，即：命题、考生报名、考生登录、获取试题、开始考试、提交试卷、系统评分[2-4]。由于各种考试系统都有很强的针对性，各个系统的考试模式是不一样的，根据考试系统的模式可以分为两大类：单机模式和网络模式，而网络模式又可分为B/S模式和C/S模式。

（1）单机模式：考试在单机上进行，又分两种方法。第一种方法，将整个系统（包括系统管理和考试系统）都安装在单机中，有多少机器考试就要安装多少次系统。这种方法的缺点是需要重复安装，而且对系统安全性和成绩回收都有较高的要求，考务工作量以及系统升级维护工作量都相当大，而优点则是保持了系统的完整性。全国计算机等级考试的单机版就是这样进行。第二种方法，将系统管理模块安装在管理员的一台专用计算机中，由它来生成考卷。将已经生成的考卷和考试系统安装在考试计算机中。这时，通常用一块软盘存储考试系统和相关考卷。考生的答卷就存放在软盘中，考生考完以后，收回软盘，再由管理员的专用计算机进行改卷。这种方法无论从考务工作量、信息安全和成绩回收上都存在重大缺陷，但其优点是考试组织比较灵活，管理人员不需要特别严格的培训，地域范围广。因此，这种方法还大量存在于一般的中、小型考试。例如，有些地方的成人考试，高校学生计算机考试常采用这种方式。

（2）网络模式：考试通过互联网（Internet）和局域网（LAN）进行。有C/S[5]和B/S [6]模式。C/S模式主要由客户应用程序、服务器管理程序和中间件三个部分组成。在服务器上安装考试服务器端的软件及数据服务器，为学生分配考试试题，在客户机上安装客户端软件，考生在客户机上考试，从服务器上获取试题，数据保存在数据服务器上。C/S模式具有较强的交互性，在C/S中，客户端有一套完整应用程序，在出错提示、在线帮助等方面都有强大的功能，而且C/S模式提供了更安全的

存取模式，全国计算机等级考试网络版、NIT等都采用这种方法。B/S模式是一种以Web技术为基础的系统平台模式，它把传统C/S模式中的服务器部分分解为一个数据服务器与一个或多个应用服务器（Web服务器），从而构成一个三层结构的客户服务器体系。B/S采用点对多点、多点对多点这种开放的结构模式，并采用TCP/IP这一类运用于Internet的开放性协议，其安全性只能靠数据服务器上管理密码的数据库来保证。世界范围内的“微软认证”考试就是采用这种方式进行。

无纸化考试代表着未来考试方式的改革与发展方向，使教师从出题、制卷、组织监考、阅卷判分、试卷分析等费时费力的传统考试方式中解脱出来，极大地提高考试及办公的自动化水平和管理水平，降低规模考试的成本，提高工作效率，促进教学与考试的规范统一，并使考试更加高效、公平与合理。

1.2.2 信息安全的发展现状

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因为偶然的或者恶意的原因而遭到破坏、更改或泄露，系统连续可靠正常地运行，使信息服务不中断。信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都属于信息安全的研究领域[7-8]。

现代信息系统中的信息安全的核心问题是密码理论及其应用，其基础是可信信息系统的设计与评估。总的来说，目前在信息安全领域所关注的焦点主要有以下五个方面。

1.2.2.1 密码理论与技术

密码理论与技术主要包括两部分，即基于数学的密码理论与技术（包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash函数、身份识别、密钥管理、PKI技术等）和非数学的密码理论与技术（包括信息隐形、量子密码、基于生物特

征的识别理论与技术等）[9]。

目前，基于数学的密码理论与技术主要有 DES、TEA、RSA、IDEA、DSA 等密码算法。而对非数学的密码理论与技术主要有图像叠加、数字水印、潜信道、隐匿协议等信息隐藏技术，识别手形、指纹、语音、视网膜、虹膜、脸形、DNA 等生物特征识别技术，基于单光子量子信道中测不准原理、基于量子相关信道中 Bell 原理以及基于两个非正交量子态性质的量子密码技术。

1.2.2.2 安全协议理论与技术

安全协议的研究主要包括两方面内容，即安全协议的安全性分析方法研究和各种实用安全协议的设计与分析研究。安全协议的安全性分析方法主要有两类，一类是攻击检验方法，一类是形式化分析方法，其中安全协议的形式化分析方法是安全协议研究中最关键的研究问题之一，它的研究始于 20 世纪 80 年代初，目前正处于百花齐放，充满活力的状态之中[10]。

目前已经提出了大量实用的安全协议：电子商务协议、IPSEC 协议、TLS 协议、SNMP 协议、PGP 协议、PEM 协议、S-HTTP 协议和 S/MIME 协议等。实用安全协议的安全性分析特别是电子商务协议、IPSEC 协议和 TLS 协议是当前协议研究中的另一个热点。

1.2.2.3 安全体系结构理论与技术

安全体系结构理论与技术主要包括安全体系模型的建立及其形式化描述与分析，安全策略和机制的研究、检验和评估系统安全性的科学方法和准则的建立，符合这些模型、策略和准则的系统的研制（比如安全操作系统和安全数据库系统等）[11]。

目前，美国已研制出达到 TCSEC 要求的安全系统（包括安全操作系统、安全数据库、安全网络部件）多达 100 多种，但这些系统仍有局限性，还没有真正达到形式化描述和证明的最高级安全系统。英、法、德、荷四国针对 TCSEC 准则只考

虑保密性的局限，联合提出了包括保密性、完整性和可用性概念的“信息技术安全评价准则”（ITSEC）[12]，但是该准则中并没有给出综合解决以上问题的理论模型和方案。近年来六国七方（美国国家安全局和国家技术标准研究所、加、英、法、德、荷）共同提出“信息技术安全评价通用准则”（CC for ITSEC）。CC 综合了国际上已有的评测准则和技术标准的精华，给出了框架和原则要求，但它仍然缺少综合解决信息的多种安全属性的理论模型依据[13]。

1.2.2.4 信息对抗理论与技术

信息对抗理论与技术[14]主要包括：黑客防范体系，信息伪装理论与技术，信息分析与监控，入侵检测原理与技术，反击方法，应急响应系统，计算机病毒，人工免疫系统在反病毒和抗入侵系统中的应用等。

该领域正在发展阶段，理论和技术都很不成熟。目前看到的成果主要是一些产品（比如 IDS、防范软件、杀病毒软件等），攻击程序和黑客攻击成功的事件。美国在网络攻击方面处于国际领先地位，有多个官方和民间组织在做攻击方法的研究。其中最著名的研究黑客攻击方法的组织有：CIAC（计算机事故咨询功能组），CERT（计算机紧急响应小组）和 COAST（计算机操作、审计和安全技术组）。他们跟踪研究最新的网络攻击手段，对外及时发布信息，并提供安全咨询。

1.2.2.5 网络与安全产品

网络安全是信息安全中的重要研究内容之一，研究内容包括：网络安全整体解决方案的设计与分析，网络安全产品的研发等[15]。网络安全包括物理安全和逻辑安全。物理安全指网络系统中各通信、计算机设备及相关设施的物理保护，免于破坏、丢失等。逻辑安全包含信息完整性、保密性、非否认性和可用性。它是一个涉及网络、操作系统、数据库、应用系统、人员管理等方方面面的事情，必须综合考虑。

解决网络信息安全问题的主要途径是利用密码技术和网络访问控制技术。密码技术用于隐蔽传输信息、认证用户身份等。网络访问控制技术用于对系统进行安全

保护，抵抗各种外来攻击。目前市场上比较流行而又能够代表未来发展方向的安全产品大致有以下几类：防火墙、安全路由器、虚拟专用网（VPN）、安全服务器、电子签证机构—CA 和 PKI 产品、用户认证产品、安全管理中心、入侵检测系统（IDS）、安全数据库以及安全操作系统。

1.3 课题研究的意义、内容及目标

1.3.1 意义和内容

无纸化考试系统的重要信息（考生、考场、试卷及答案等）如何在广域网中安全的传输，是保证无纸化考试系统的公平性、安全性和可靠性的重要环节，因此应用层通信安全机制的研究成为该系统的重要部分。在对无纸化考试系统的应用层协议进行设计，对登录用户进行身份认证以及对其网络传输数据采用加密策略的基础上，构建一种基于应用层通信安全的机制，并探讨与之相适应的实现技术。

主要内容包括以下几个方面：

（1）无纸化考试系统的应用层协议设计。

（2）身份认证技术。

（3）加解密技术。

（4）一个能满足无纸化考试系统基本需求的应用层通信安全机制的设计与实现。

1.3.2 目标

本研究课题所实现的应用层安全通信机制应达到以下目标：

（1）应能为无纸化考试系统的广域网信息传输提供安全、可靠的信息传输平台。

（2）应具有高效性，不影响网络信息的传输以及无纸化考试系统的运行性能。

（3）应具有较好的普适性和可扩展性，可方便地应用于其他的类似系统中。

2 相关技术基础

本章将分析无纸化考试系统应用层通信安全机制所涉及的相关技术。阐述互联网的体系结构模型；讨论身份认证技术；探讨对数据进行加密解密的相关技术。

2.1 网络体系结构模型

计算机网络是一个非常复杂的系统，通信双方必须保证通信工作的协调一致。为便于复杂的计算机网络设计，国际标准化组织 ISO 提出了开放系统互连基本参考模型 OSI/RM，简称 OSI[16]。OSI 试图使全世界的计算机网络都遵循这一标准，然而由于种种原因，真正得到广泛应用的却是 TCP/IP 网络体系结构。

2.1.1 OSI 参考模型

OSI 参考模型如图 2.1 所示。该参考模型定义了七个层次。

图 2.1　OSI 参考模型

（1）应用层（Application Layer）

规定了用户级别地对话规则，包括事务服务、文件传送、远程作业和电子邮件等一些进行通信任务的处理规则。

（2）表示层（Presentation Layer）

提供了应用层实体之间的通信所使用的信息表示形式，即信息的语法与语义，包括对各种数据类型和数据结构的表示方法、数据编码以及数据的加密和压缩等。

（3）会话层（Session Layer）

会话服务是面向连接的服务。它是高层实体间的会话连接，包括会话的控制、同步、释放，同时它还管理高层实体间的数据交换方法。

（4）传输层（Transport Layer）

在高层实体之间提供了透明的数据传输，以及出错时的恢复处理，使得这些实体（一般指进程）无需考虑进行可靠和有效的数据传输的具体方法。

（5）网络层（Network Layer）

对数据进行分组，提供网络结点间的路由选择等，当跨网络传送数据时对其中可能出现的不同寻址方式、分组长度和协议进行处理。

（6）数据链路层（Date Link Layer）

提供点到点的数据传输，并提供了建立、保持和释放点的连接功能。

（7）物理层（Physical Layer）

该层实现系统通信媒体的物理接口，规定物理链路的参数，如信号的幅度，宽度，链路的电气和机械等特性等。

2.1.2 TCP/IP 模型

TCP/IP 协议又被称为 DoD 模型[17]，是一个抽象的分层模型。在此模型中，所有的 TCP/IP 网络协议都被归类到四个抽象的“层”中。

（1）应用层

应用层提供给利用 TCP/IP 协议进行通讯的程序，与 OSI 参考模型应用层、表示层以及会话层的功能基本相同。

（2）传输层

传输层提供应用进程之间的数据传输。包括：传输控制协议（TCP），提供面向连接的可靠的、完整性检查的数据传输以及拥塞控制和流控制；用户数据报协议

（UDP），它提供无连接的、不可靠的传输。

（3）网络层

IP 协议是这层最重要的协议，它是一个无连接的协议，没有提供可靠性、流控制、或错误恢复，但它提供了路由功能，负责将信息传送到其目的地。除了 IP 协议外，还有 ICMP、IGMP、ARP 和 RARP 等网络层协议。

（4）网络接口层

网络接口层也即OSI模型中的数据连接层及物理层，是网络连接的接口。TCP/IP在这层并没有制定任何具体协议，可以利用几乎所有的可用的网络接口，如 IEEE 802.2、X.25、ATM、FDDI 以及 SNA 等。

图 2.2 给出了 TCP/IP 模型的层次结构以及每层对应的具体协议。

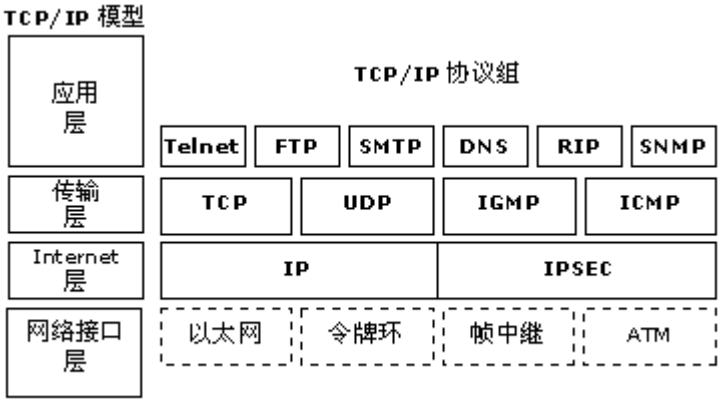


图 2.2　TCP/IP 模型四层结构

2.2 身份认证技术

2.2.1 身份认证的概念

身份认证又称作识别（Identification）、实体认证（Entity Authentication）、身份证实（Identity Verification）等，它是在通信用户之间进行的一个用户对另一个用户进行识别以证明其身份的过程。身份认证是计算机系统的用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的手段。

2.2.2 身份认证的方式

一般来说，身份认证有三种方式：根据约定的口令进行身份认证[18-21]、采用智能卡进行身份认证[22-25]以及基于生物特征的方式。

（1）基于口令的认证

系统事先保存每个用户的用户名和口令，口令通常经加密后保存到口令文件中，系统根据用户输入的信息与口令文件的对比来判断用户身份的合法性。这种方法简单但不安全，用户口令一般比较容易受到口令猜测攻击，如果口令文件被窃，还容易受到字典式攻击等。动态口令机制是对基于口令的身份认证方式的改进，用户登录系统时系统随机提示一条信息，用户根据这一信息连同其个人化信息共同产生一个口令，系统也使用同样的信息和方法产生口令并进行比较来判断用户身份的合法性。基于口令认证的优点是不需要附加硬件设备，且容易实现；缺点则是用户与服务器之间要经过数次通信才能完成一次识别过程，且本地存放的口令信息具有一定的安全隐患。

（2）基于智能卡的认证

基于智能卡的身份识别方法，其原理是在智能卡上存储用户的个人秘密信息。用户首先输入身份识别 PIN 码，智能卡认证 PIN 码，待确认后，计算机就从智能卡中读取用户的秘密信息并发送到远程服务器，服务器根据收到的信息对用户的身份进行认证。这种认证方式的安全保证是基于智能卡的物理安全性的—智能卡难以伪造，也难以直接读出其中的数据。

（3）基于生物特征的认证

这种认证方式是根据人的生理特征如指纹、脸型、声音等特性来进行身份认证[26]，它需要使用诸如指纹阅读器，脸型扫描器，语音阅读器等价格比较昂贵的硬件设备。同时，要求验证双方通过直接而非网络的方式交互，所以该类方法并不适用于在 Internet 或者无线应用等分布式的网络环境中。

2.2.3 静态身份认证和动态身份认证

从身份认证的基本原理上来说，身份认证可以分为静态身份认证和动态身份认证[27]。

2.2.3.1 静态身份认证

静态身份认证是指用户登录系统验证身份过程中，输入系统的验证数据是固定不变的。符合这个特征的身份认证方法即称为静态身份认证。静态身份认证主要可以分为单因子静态身份认证和双因子静态身份认证。

（1）单因子静态身份认证

静态口令是一种单因子静态认证方法[28]。当用户需要访问系统资源时，系统提示用户输入用户名和口令，系统采用加密方式或明文方式将用户名和口令传送到认证中心，和认证中心保存的用户信息进行对比，若验证通过，系统允许该用户进行随后的访问操作，否则拒绝用户的进一步访问操作。

静态口令身份认证一般用于那些安全性要求不太高的场合，如 PC 机的开机口令、Unix 系统中用户的登录、Windows 用户的登录等。

（2）双因子静态身份认证

双因子静态身份认证，即在单一的记忆因子（固定口令）认证基础上结合第二物理认证因子，这里的物理认证因子包括智能卡、条码卡和指纹等[29-30]。用户在登录业务终端上输入 ID 和口令，待确认后，再通过专用设备（磁条读写器、IC 读写器、指纹仪等）将第二物理认证因子的数据读入并发送到认证中心进行验证，业务终端再根据认证中心返回的认证结果，决定用户的后继操作。

双因子静态身份认证是对单因子静态身份认证的一个改进，因为有了第二物理认证因子，使得认证的可靠性得到指数递增。

2.2.3.2 动态身份认证

动态身份认证是指用户登录系统验证身份过程中，输入系统的验证数据是动态

变化的，符合这个特征的身份认证方法称为动态身份认证。动态身份认证目前主要有时间同步机制身份认证和挑战/应答机制身份认证。这两种身份认证方法都是基于智能令牌实现的，时间同步机制身份认证基于时间同步令牌实现，挑战/应答机制身份认证基于挑战应答令牌实现[31-32]。

2.3 密码体制与加解密技术

2.3.1 对称密钥加密体制

对称密钥加密体制，即加密密钥等于解密密钥，或由其中一个很容易推出另一个[33]。对称密钥算法要求发送者和接收者在安全通信之前商定一个密钥。若用 M 表示明文、C 表示密文、E 表示加密算法、D 表示解密算法、k 表示密钥，则对称密钥算法的加密和解密过程可表示为：加密，Ek(M)=C；解密，Dk(C)=M。

对称密钥算法可分为两类：一类是只对明文中的单个位（有时对字节）运算的算法称为序列算法或序列密码[34]；另一类算法是对明文的一组位进行运算，这些组位称为分组（典型分组长度为 64 位、128 位、256 位），相应的算法称为分组算法或分组密码[35]。对称密钥算法具有加密速度快、安全强度高等优点，但也存在着明显的缺陷，包括：

（1）进行安全通信前需要以安全方式进行密钥交换。这在某种情况下是可行的，但在某些情况下会非常困难，甚至无法实现；

（2）密钥规模复杂。例如，A 与 B 两人之间的密钥必须不同于 A 和 C 两人之间的密钥。那么在拥有 1000 个用户的团体中，A 需要保持至少 999 个密钥，而对于该团体中的其它用户，此种情况同样存在。这样，该团体一共需要将近 50 万个不同的密钥。则可推出拥有 n 个用户的团体则需要 $n^2/2$ 个不同的密钥[36]。

2.3.2 公开密钥加密体制

为了解决对称密钥体制中密钥的管理问题，1976 年，Diffie 和 Hellman 在“密

码学的新方向”一文中提出了一种密钥交换协议，允许在不安全的媒体上通讯双方交换信息，安全的达成一致的密钥。在此基础上，很快出现了非对称密钥密码体制，即公开密钥加密体制。在公开密钥加密体制中，加密密钥不同于解密密钥，加密密钥是公开的，而解密密钥是非公开的，这一对密钥被分别称为公开密钥（Public key）和秘密密钥（Private key）[37]。

采用公开密钥加密体制进行安全通信的步骤如下（假设 A 向 B 发送秘密信息）：

（1）A 查找 B 的公钥。因为公钥的公开不会影响到通信的保密性，B 可以将自己的公钥公布在公共数据库，由其它人取用，或以普通电子邮件等方式通过非安全信道发送给 A；

（2）A 采用公钥加密算法以 B 的公钥作为加密密钥对原始信息进行加密；

（3）A 通过非安全信道将密文发送给 B；

（4）B 收到密文后使用自己持有的私钥对其解密，还原出明文[38]。

利用公开密钥密码技术进行安全通信，有以下优点：

（1）通信双方事先不需要通过保密信道交换密钥；

（2）密钥持有量大大减少：在 n 个用户的团体中进行通信，每一用户只需要持有自己的私钥，而公钥可放置在公共数据库上供其他用户取用，这样整个团体仅需要拥有 n 对密钥，就可以满足相互之间的安全通信的需求；

（3）公开密钥密码技术还解决了对称密钥密码技术无法或很难提供的服务：如与哈希函数联合运用可生成数字签名，可证明的安全伪随机数发生器的构造，零知识证明等。

非对称密码技术的主要缺点是：解密速度慢、资源消耗大[39]。

2.3.3 混合密钥加密体制

关于对称密钥密码技术和公开密钥密码技术的讨论表明：前者具有加密速度快、运行时占用资源少等特点，后者在密钥交换上具有优势。因此，通常把这两者结合起来实现最佳性能。即用公开密钥密码技术在通信双方之间传送对称密钥，而用对称密钥来对实际传输的数据加密解密，这就是混合密钥加密技术[40]。

若 A 向 B 发送保密信息，具体步骤为：

（1）A 生成一随机的对称密钥，即会话密钥；

（2）A 用会话密钥加密明文；

（3）A 用 B 的公钥加密会话密钥；

（4）A 将密文及加密后的会话密钥传递给 B；

（5）B 使用自己的私钥解密会话密钥；

（6）B 使用会话密钥解密密文，得到明文。

用户可以在每次发送保密信息时都使用不同的对称密钥，从而增加密码破译的难度。而且即使某次会话的密钥被破译了，也只会泄漏该次会话的信息，不会影响到其它密文的传递，这使得信息的传输更加安全[41]。

2.3.3 哈希（Hash）函数

Hash 函数是一种将任意长度的消息压缩到某一固定长度的消息摘要的单项函数，主要用于数字签名和消息的完整性检测。数字签名时，当签名者想签一个消息 x 时，首先构造一个消息摘要 z = h(x)（h 是 Hash 函数），然后计算签名 y = Sigk(z)[42]。检测数据完整性时，计算数据的 Hash 值，并与已经保存的原 Hash 值进行比较，如果相等，则数据是完整的，没有被改动；否则，数据已经被改动过[43]。

目前已经设计出了大量的 Hash 函数，诸如，Rabin Hash 方案、Merkle Hash 方案、N-Hash 算法、MD4 算法、MD5 算法、SHA 等。

2.4 小结

本章主要论述了无纸化考试系统的应用层通信安全机制所需涉及的相关技术。阐述了网络体系结构模型，包括 OSI 基本参考模型和 TCP/IP 模型，详细讨论了身份认证技术，并在最后对整个通信安全机制的核心问题——加解密技术进行了深入的探讨。

3 无纸化考试系统的应用层通信安全机制

本章将先对无纸化考试系统的体系架构和安全需求进行介绍、分析，然后在相关技术分析的基础上，讨论无纸化考试系统的应用层通信安全机制的设计原则以及各功能模块划分，并详细阐述各功能模块的设计思想。

3.1 无纸化考试系统及其安全需求

3.1.1 无纸化考试系统的体系架构

本无纸化考试系统采用了三层 C/S 体系架构，即表示层、应用服务层和数据服务层。

三层 C/S 体系架构指的是将数据处理过程分为三部分：第一层是表示层（也即客户端层、用户界面层），提供用户与系统的友好访问；第二层是应用服务层（也叫中间层），负责业务逻辑的实现；第三层是数据服务层（又称数据源层或数据库管理系统层），负责数据信息的存储、访问及其优化。由于业务逻辑被提取到应用服务层，大大降低了客户端负担，因此也被称为瘦客户（Thin Client）结构。三层结构在传统的二层结构的基础上增加了应用服务层，将应用逻辑单独进行处理，从而使得用户界面与应用逻辑位于不同的平台上，两者之间的通信协议由系统自行定义。通过这样的结构设计，使得应用逻辑被所有用户共享。

数据服务层位于数据库系统中，而应用服务层位于通信服务器中（其中，应用层又划分为数据访问子层、业务逻辑子层和通信子层），考场管理客户端和其下级的考试客户端则共同组成表示层。

无纸化考试系统的体系架构如图 3.1 所示。

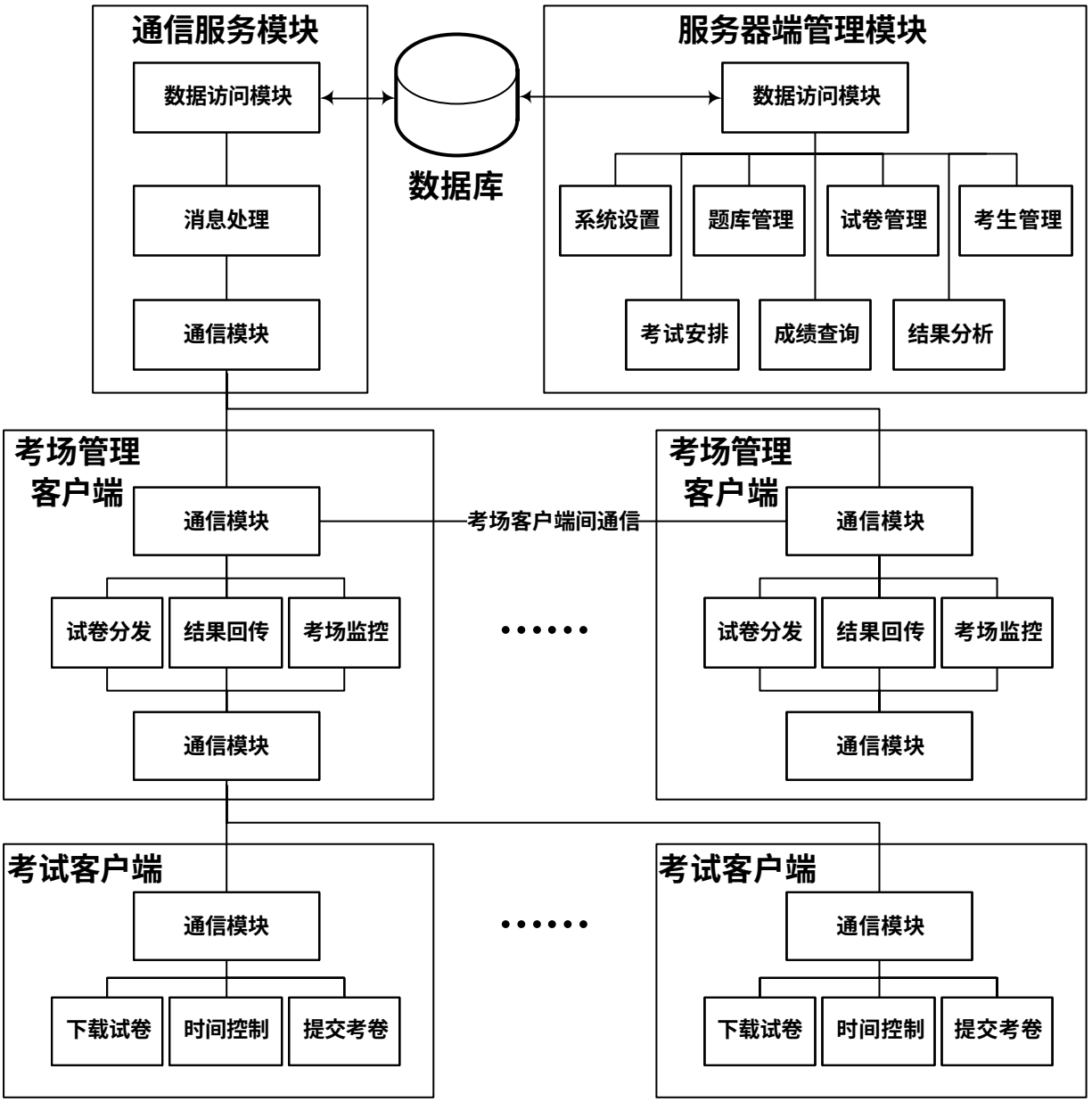


图 3.1　无纸化考试系统的体系架构

无纸化考试系统的拓扑结构如图 3.2 所示。应用服务层位于考试中心的一台服务器，数据服务层可以与通信服务器位于同一台服务器上，也可以位于另外一台服务器上，但最好位于同一局域网内，这是出于对性能以及安全方面的考虑。而表示层则可分布于广域网中，和应用服务层进行远程数据交互。

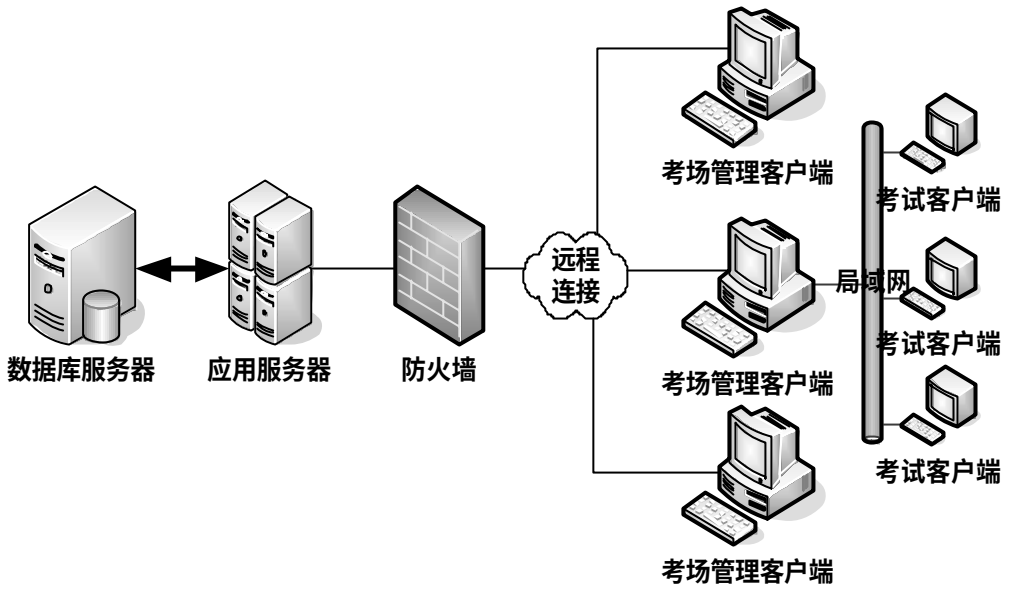


图 3.2　无纸化考试系统的拓扑结构

3.1.2 无纸化考试系统的安全需求

由上一节内容可知，无纸化考试系统是基于广域网通信的，通信服务器与考场管理客户端以及考场管理客户端之间（即应用服务层与表示层以及表示层之间）的信息交互是在广域网中进行的。通信服务器与考场管理客户端之间的交互信息包括：考场管理客户端登录信息、考场信息、传送的文件信息、试卷以及答案信息、评卷信息等。考场管理客户端之间的交互信息，仅仅是试卷以及答案信息，这主要是为了避免在同一时间段内多个考场管理客户端向通信服务器请求试卷以及答案信息，从而影响了通信服务器的性能，并增加了通信服务器的网络 I/O 负载，这种情况也使得各个考场管理客户端长时间处于对试卷以及答案信息的等待中，不利于考场管理客户端操作人员对整个考场考试过程的监督、管理。

广域网采用公网传输数据，因而在广域网上进行传输时，信息可能会被不法分子截取，所以广域网的信息传输是不安全、不可靠的。而无纸化考试系统在广域网中传输的信息都是敏感信息，属于保密级别，一旦这些信息被截取、篡改或者伪造，将会严重影响整个无纸化考试过程的公平性、公正性，并使得整个考试系统失去其作为测试、评估手段的意义。

综上所述，为了防止这些敏感信息在广域网的传递过程中被截取和利用，从而导致考试失去公平性，就必须提供一种通信安全机制，来保证无纸化考试系统的广域网通信安全。

3.2 设计原则

（1）符合安全需求的原则。无纸化考试系统的应用层通信安全机制要保证在广域网上发送和接收信息时：

①隐私性：除了发送方和接收方外，其他人是不可知悉的；

②真实性：传输过程中不被窜改；

③非伪装性：发送方能确信接收方不会是假冒的；

④非抵赖性：发送方不能否认自己的发送行为。

（2）协议设计采用简单和安全原则。把协议复杂性降至最低，可以提高信息处理的速度，减少协议中的冗余信息。加强协议本身的安全性，有利于提高整个应用层通信安全机制的安全性。

（3）保证该机制的高效性、易扩展性和可移植性。高效性是指，作为无纸化考试系统的广域网安全通信平台，不应该影响整个系统的性能（包括增加网络时延、服务器计算负载、网络 I/O 负载等）；易扩展性是指，由新需求和新问题所带来的新的功能要求，能够方便地加入其中，而不会导致整个结构上的改变；可移植性是指，不经过修改的或者经过少量的修改便可以被其他具有相同安全水平需求的系统所集成应用。

（4）采取模块化设计方法，利用功能模块的划分保证安全机制各部分的相对独立性，这不仅有利于降低整体复杂度，提高开发效率，而且更易于将来的维护和升级操作。

3.3 功能模块设计

3.3.1 应用层协议模型

3.3.1.1 协议功能需求及设计方式

由于 TCP/IP 协议的广泛性，无纸化考试系统是基于 TCP/IP 网络体系结构的。应用层是 TCP/IP 体系结构中的最高层，是为最终用户提供服务的。应用层协议的目的是为了解决某一类应用问题，而这些问题的解决往往是通过位于不同主机中的多个进程之间的通信和协同工作来完成的。

无纸化考试系统的应用层协议必须解决以下问题：

（1）基本信息传输

基本信息包括：考点、考场信息；考试中心时间信息；考场管理客户端拥有试卷信息；文件下载重定向地址；用户权限错误；考场号错误以及数据库异常等。

（2）文件传输

主要是考生信息文件、考试试卷以及答案文件的下载和考生考试结果信息文件的上传。

（3）用户登录

允许合法用户登录通信服务器，请求相关资源，防止非法用户获取这些敏感信息。

（4）其它

考场管理客户端之间的数据交互，包括身份确认和文件传输（考试试卷以及答案文件）。

目前而言，应用层上的协议设计可以分为两种方式：一种是基于 ASCII 码表示的命令/应答式协议模型；另一种则是采用类似底层协议（如 TCP、IP 协议等）的封包格式，在每个封包中定义不同的字段来表示各种有用的含义。第一种协议模型的优点是简单、易于理解，而其缺点正是由于其直观性、简单性导致的不安全性、

易破译性，即可以通过在网络上截取数据包并提取出应用层数据信息，再通过对ASCII码表示的字符串或者数字状态码的简单分析便能以较高的概率分析出协议规则。第二种协议设计方式的特点，正好与第一种相反，封包中字段的多少和字段长度的不一致导致了协议的相对复杂性，但是却增加了其安全性和不易破译性。无纸化考试系统的应用层协议采用的是第二种协议设计方法，以确保能在处于应用层通信安全机制中最核心的应用层通信协议上提供较好的安全性。

3.3.1.2 协议内容及格式

为了遵循协议设计简单性原则，协议数据包采用最少的字段划分。协议数据包格式如图3.3所示。

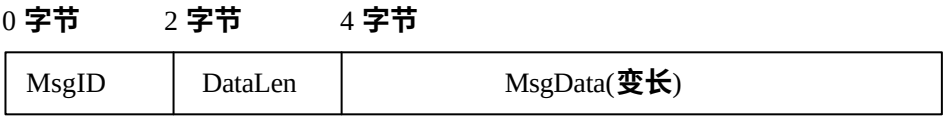


图3.3 协议数据包格式

协议数据包都具有以下字段：

（1）MsgID字段：协议类型，即消息ID，用来表示协议功能，占2个字节；

（2）DataLen字段：实际数据长度值，表示除去MsgID字段和DataLen字段后的实际数据长度，占2个字节；

（3）MsgData字段：实际数据，长度不定。

其中的第一个和第二个字段称为消息头部，结构定义如下：

```
typedef struct _msg_header
{
    WORD        nMsgID;         //协议类型，消息ID
    WORD        nDataLen;       //消息数据的长度
}MSG_HEADER;
```

以下将分类介绍详细的协议内容，表中“输入”表示信息从考场管理客户端发

送到通信服务器，而“输出”则表示信息发送方向相反。

（1）基本信息传输

基本信息传输涉及的协议内容如表 3.1 所示。

表 3.1　基本信息传输涉及的协议内容

输入\输出	MsgID	DataLen	MsgData	备注
输入	1001	0	无	请求考点、考场信息
输入	1002	0	无	请求考试中心的当前时间信息
输入	1003	不定	试卷名字符串序列	该序列以预先定义的分隔符分隔开每个试卷名字符串，分隔符定义为“;”
输出	2001	不定	考点、考场信息字符串序列	该序列以预先定义的分隔符分隔考点、考场信息字符串，分隔符定义为“,”和“;”
输出	2002	sizeof（CTime）	CTime 对象	发送考试中心当前的时间信息，作为调整考场管理客户端的时间的基准值
输出	2004	不定	文件重定向地址信息、验证信息和会话密钥信息	IP 地址占 4 个字节，验证信息包括
输出	2005	0	无	用户权限错误
输出	2006	0	无	考场号错误
输出	2007	不定	数据库异常描述字符串	描述数据库异常原因字符串

（2）文件传输的协议

文件传输涉及的协议内容如表 3.2 所示。

表 3.2　文件传输涉及的协议内容

输入\输出	MsgID	DataLen	MsgData	备注
输入	3001	不定	请求下载的试卷名字符串序列	该序列以预先定义的分隔符分隔开每个试卷名字符串，分隔符定义为“；”
输出	4001	Sizeof（PAPERFILE）	文件头部结构信息	文件信息
输出	4002	不定	信息序列、试卷文本和答案序列	文件内容

（3）用户登录

涉及的协议内容将在 3.3.2.1 节通信服务器身份认证模块中说明。

（4）其他

涉及的协议内容将在 3.3.2.2 节考场管理客户端身份认证模块中说明。

3.3.2 身份认证模块

身份认证模块，主要完成对登录用户身份的合法性确认工作，允许合法用户的数据传输，保证考试过程中的保密信息不会被以非法身份获得，避免对考试本身的公平性、公正性和有效性等造成不良影响或产生严重后果。

3.3.2.1 通信服务器身份认证过程

通信服务器身份认证过程采用了静态身份认证与动态身份认证相结合的双因子身份认证技术。双因子身份认证模块主要由三个子模块所组成：动态口令生成子模块、客户端代理子模块和认证子模块。

动态口令生成子模块通过对服务器端产生的一个随机登录令牌，然后以此登录令牌与登录用户的口令信息进行一种运算（这个运算过程使用的就是动态口令生成

算法），产生一个动态口令。

客户端代理子模块的主要功能是向认证子模块发出认证请求，将具体的身份认证信息发送给认证子模块，并通知用户验证结果。

认证子模块的主要作用是：

（1）验证用户口令的合法性；

（2）生成并向用户发送登录令牌。

这三个模块协同工作，无论什么时候考场管理系统需要登录通信服务器，其中的客户端代理模块就会启动一个会话过程，要求验证用户身份（这个会话过程是以一个 TCP 连接为实体）。如果用户提供的用户名、密码以及动态口令均正确，则允许与通信服务器进行数据交互，否则拒绝服务并关闭整个会话。

通信服务器身份认证模块的结构如图 3.4 所示。

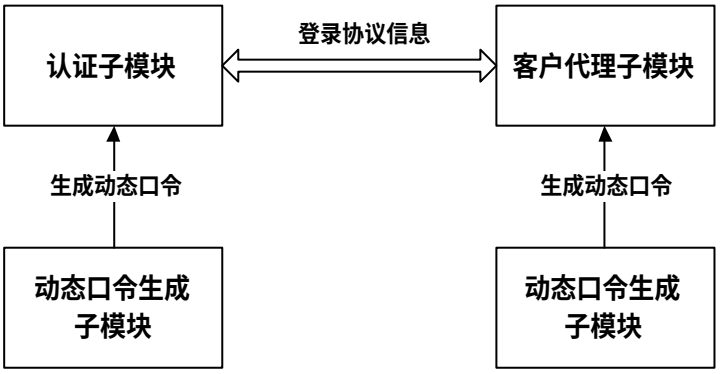


图 3.4　通信服务器身份认证模块的结构

在该身份认证模块中客户端代理子模块和认证子模块共享相同的动态口令生成算法，动态口令生成算法根据认证模块发送的 16 字节登录令牌生成动态口令。用户请求登录通信服务器时，客户端代理模块发送验证信息（用户名、密码以及动态密码）给通信服务器的认证模块。认证模块在接受到验证信息后，首先验证用户名、密码是否与用户信息数据库中信息匹配，如果匹配，再通过动态口令生成算法计算出当前的动态口令，如果用户提交的动态口令与之相等，则可以认定该用户为合法用户，接受用户的登录请求。

通信服务器身份认证模块的工作流程如图 3.5 所示。

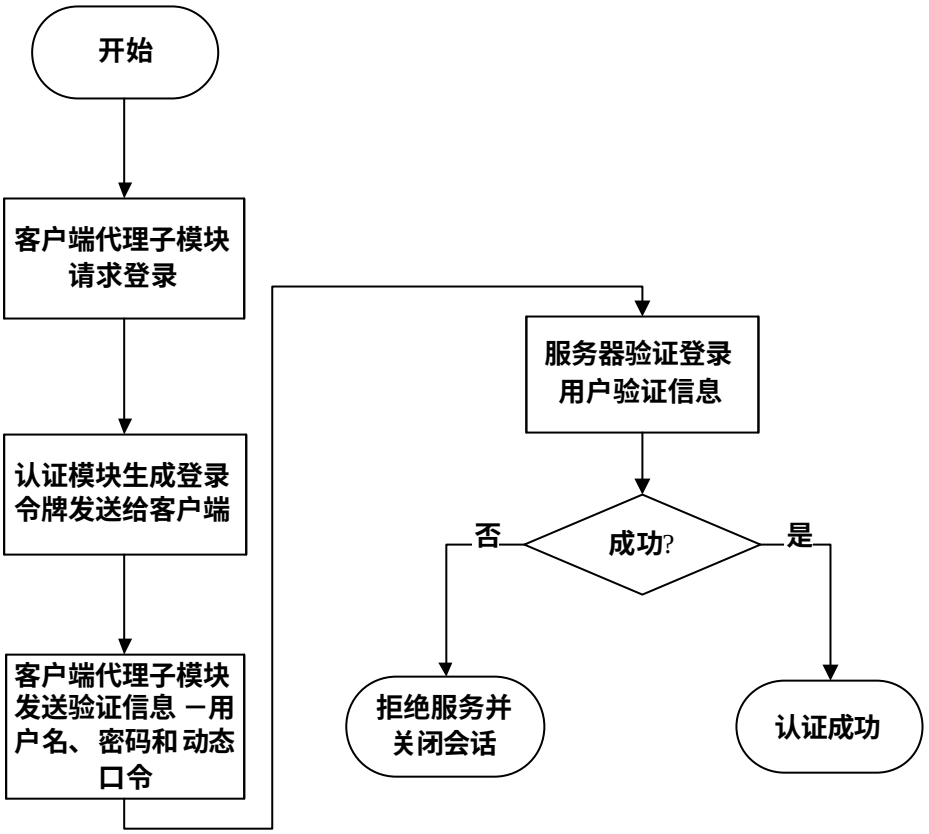


图 3.5　通信服务器身份认证模块的工作流程

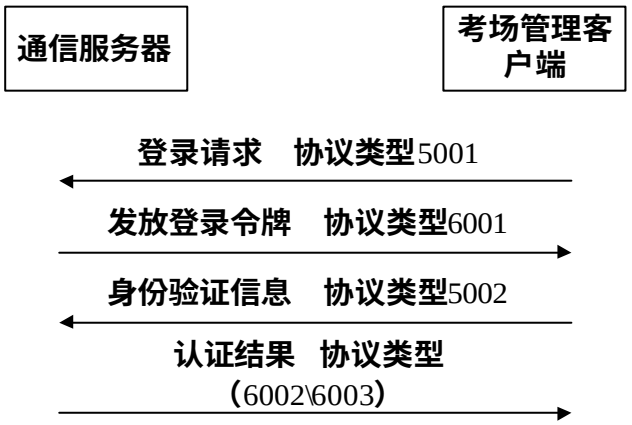
其中对用户名和密码的验证，并不是简单地进行明文对比。客户端代理模块发送给通信服务器认证模块的是把用户密码进行两轮 MD5 运算后的值作为密钥，再使用 TEA 加密算法（此处的 TEA 加密算法并不是标准的 TEA 加密算法，而是在第 3.3.3.1 节中介绍的修改的 TEA 加密算法，本文后面出现的 TEA 加密算法除了对标准 TEA 加密算法的介绍外都是指修改过的加密算法）对用户名进行加密运算所得的结果。所以，认证模块在验证用户名密码的时候，也是以这个密码密钥对客户端代理模块发送的这个结果值进行解密运算，如果和用户名一致，则表示用户名、密码正确。

通信服务器身份认证过程中涉及的协议内容如表 3.3 所示。表中“输入”表示信息从考场管理客户端发送到通信服务器，而“输出”则表示信息从通信服务器发送到考场管理客户端。

表 3.3　通信服务器身份认证过程中涉及的协议内容

输入\输出	MsgID	DataLen	MsgData	备注
输入	5001	不定	请求登录用户的用户名信息	无
输入	5002	不定	身份验证信息，包括 16 字节的动态口令和密码密钥 TEA 加密用户名的结果值	无
输出	6001	16 字节	随机登录令牌	使用该登录令牌生成动态口令
输出	6002	16 字节	随机生成的会话密钥	无
输出	6003	0	无	认证失败

通信服务器身份认证的基本过程如图 3.6 所示。



注：图中省略了TCP连接的三次握手过程

图 3.6　通信服务器身份认证的基本过程

3.3.2.2 考场管理客户端身份认证过程

考场管理客户端身份认证过程，采用单因子静态身份认证技术。请求数据的考场管理客户端从通信服务器获取被请求的考场管理客户端信息，包括其地址信息和口令信息，然后再与被请求考场管理客户端建立会话，发送口令给被请求考场管理客户端进行验证，验证成功则可进行数据的获取操作，否则拒绝并关闭会话。

考场管理客户端身份认证流程如图 3.7 所示。

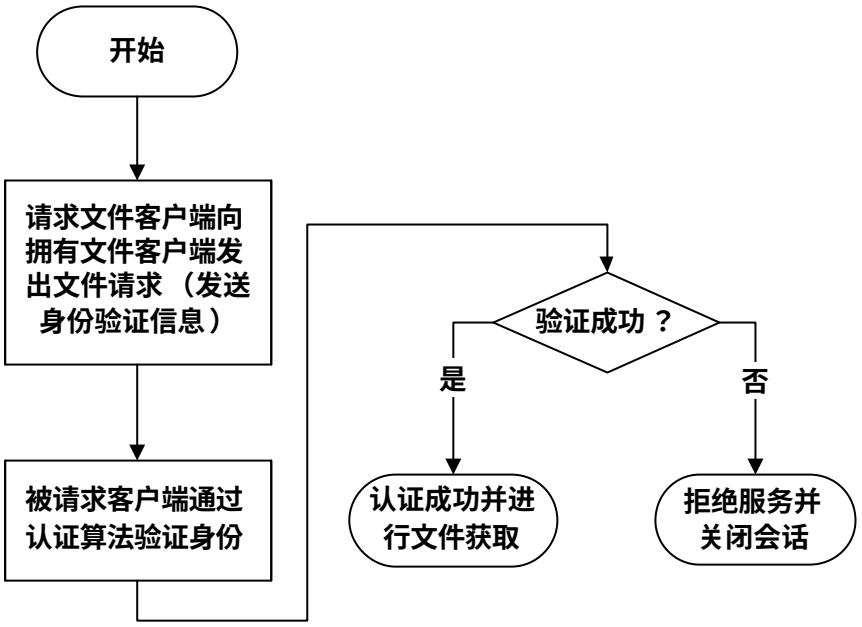


图 3.7　考场管理客户端身份认证流程

其中被请求的考场管理客户端所验证的口令信息，是通信服务器使用其密码密钥对其随机生成的会话密钥进行 TEA 加密的结果。而验证过程则是被请求考场管理客户端使用自己的密码密钥对请求考场管理客户端发送来的数据进行解密操作，并使用解密结果作为会话密钥（一次会话过程中使用的密钥）对请求考场管理客户端一并发送的测试数据进行 TEA 解密操作，这个测试数据被定义为被请求考场管理客户端登录通信服务器所使用的用户名。

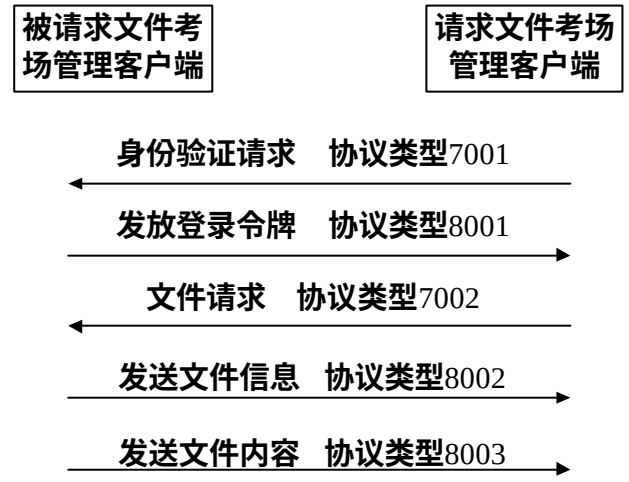
考场管理客户端之间信息交互涉及的协议内容如表 3.4 所示。表中“输入”表示信息从请求考场管理客户端发送到被请求考场管理客户端，而“输出”则相反。

表 3.4　考场管理客户端之间信息交互涉及的协议内容

输入\输出	MsgID	DataLen	MsgData	备注
输入	7001	不定	请求资源的验证信息和会话密钥信息	重定向下载文件时，请求拥有文件资源的考场管理客户端进行身份认证
输入	7002	不定	请求下载的试卷名字符串序列	该序列以预先定义的分隔符分隔开每个试卷名字符串，分隔符定义为“;”

输入\输出	MsgID	DataLen	MsgData	备注
输出	8001	0	无	身份认证成功，可以请求文件资源
输出	8002	Sizeof（PAPERFILE）	文件头部结构信息	文件信息
输出	8003	不定	信息序列、试卷文本和答案序列	文件内容

考场管理客户端身份认证的基本过程如图 3.8 所示。



注：图中省略了TCP连接的三次握手过程

图 3.8　考场管理客户端身份认证的基本过程

3.3.3 数据加密模块

有了应用层协议保证基本通信功能、身份认证机制确保合法用户访问资源，但是交互数据仍然是在广域网上进行传输的。如果数据仍以明文传输，只要通过在广域网中适当的网络节点上进行数据包捕获就能够获得这些敏感信息，从而进行一些破坏考试公平性、公证性及有效性的活动。

数据加密模块对整个会话期间的通信数据进行加密，以保证这些数据信息在被监听的情况下，很难由密文确定出明文或密钥，即具有高不可破译性和抗密码分析能力。

3.3.3.1 加密策略

对于所有的协议数据包，除去登录请求协议数据包（包括登录通信服务器的请求和考场管理客户端之间的身份认证请求）以及不附带实际数据的协议数据包不进行加密处理外，其余的协议数据包的数据部分都要进行加密处理（但是，消息头部，即 MsgID 字段和 DataLen 字段不进行加密）。对于登录通信服务器的协议数据包，除了发送登录用户验证信息的协议数据包使用登录令牌充当临时密钥进行数据加密外都使用密码密钥进行数据加密，而在双方都获得了会话密钥之后，则使用会话密钥进行数据的加密。

为了使加密过程快速、透明，即不影响通信服务器和考场管理客户端的运行效率，加密算法采用对称密钥算法。具体的数据加密策略是：采用 TEA 加密算法，结合填充、交织算法进行数据加密。TEA 加密算法（微型加密算法）是分组加密算法，它最初是由剑桥计算机实验室的 David Wheeler 和 Roger Needham 在 1994 年设计的。该算法使用 128 位的密钥为 64 位的信息块进行加密并产生 64 位的输出，它需要进行 64 轮迭代。该算法使用了一个神秘常数 δ 作为倍数，它来源于黄金比率，以保证每一轮加密都不相同。但 δ 的精确值似乎并不重要，这里 TEA 把它定义为 δ = 「$(\sqrt{5}-1)\times 231$」（也即 0x9E3779B9 的十六进制数）。这种算法的可靠性是通过加密轮数而不是算法的复杂度来保证的。TEA 加密算法是一种优秀的数据加密算法，虽然它比 DES 要简单得多，但却有很强的抗差分分析能力，加密速度也比 DES 快得多，而且对 64 位数据加密的密钥长达 128 位，安全性相当好。

该策略中使用 16 轮的迭代次数进行 TEA 加密，目的是为了减少加密所消耗的时间，但对其可靠性有一定的影响。在使用这个算法的时候，由于需要加密不定长的数据，所以使用了一些常规的填充算法和交织算法（也就是说，把前一组的加密结果和后一组的进行运算，产生新的结果）。

填充算法：原始字符串加上 8 个字节再加上填充字符数应该是 8 的倍数（即至少填充到 2 个字节）。填充后的字符串结构：第一个字节为填充字符数或上 0xA8，后面接着便是填充字节，然后是待加密的数据，最后是 7 个值为 0 的字节。其中填

充的字节采用随机生成的填充字符串。由于明文最后总会被添加 7 个值为 0 的字节，在解密后可以依照最后是否 7 个值为 0 的字节来判断是否正确的解密。

交织算法：第一个 64bits 块，按一般的 TEA 加密。下一个 64bit 块与上一组的加密结果异或生成待加密数据，加密后与上一组的待加密数据异或生成加密结果。

3.3.3.2 密钥生成及管理

该加密策略中的密钥即为 TEA 加密算法的密钥，它是一种对称密钥，长度为 128 位。在该加密策略中存在三种密钥，一种称之为密码密钥，第二种称之为会话密钥，最后一种称之为临时密钥。密码密钥在前面提到过，它是把用户密码进行两轮 MD5 运算后的值作为密钥，作用于用户身份认证过程中和会话密钥的获取过程中，因为通信服务器能够通过用户信息数据库得到用户密码，而用户本身亦知道密码，所以密码密钥是不需要协商的。会话密钥是通信服务器随机生成的，需要由通信服务器通过某种方式发给会话双方（例如，通信服务器与考场管理客户端之间的会话，由通信服务器发送密钥给考场管理客户端；而考场管理客户端之间的会话，则由通信服务器发给请求考场管理客户端，再转发给被请求考场管理客户端），它作用于通信服务器与考场管理客户端的一次会话过程，或者是考场管理客户端之间的一次会话过程，由此可知会话密钥只对每一次具体的会话有效。临时密钥是通信服务器认证模块发送的登录令牌，只在考场管理客户端发送登录用户的身份验证信息时用到。

3.4 小结

本章在探讨无纸化考试系统的体系架构和安全需求的基础上，从设计原则、各功能模块的设计上进行了详细的分析与论述。首先，阐述了无纸化考试系统的应用层协议模型的设计。其次，探讨了身份认证模块的构成和工作流程。最后对数据加密模块的加密策略进行了讨论。这些分析和设计构成了无纸化考试系统的应用层通信安全机制实现的基础。

4 无纸化考试系统的应用层通信安全机制实现

本章将在无纸化考试应用层通信安全机制分析与设计的基础上，具体阐述该机制中应用层协议处理模块、身份认证模块和数据加解密模块中核心内容的实现。限于篇幅，本章将不会详细讨论所有的实现细节，仅重点讨论其中涉及的关键技术的实现。

4.1 应用层协议处理模块的实现

针对上一章设计的应用层协议模型，在通信服务器和考场管理客户端中分别实现应用层协议处理模块，用来对具体的协议进行分拣并调用各自特定的功能模块进行处理。

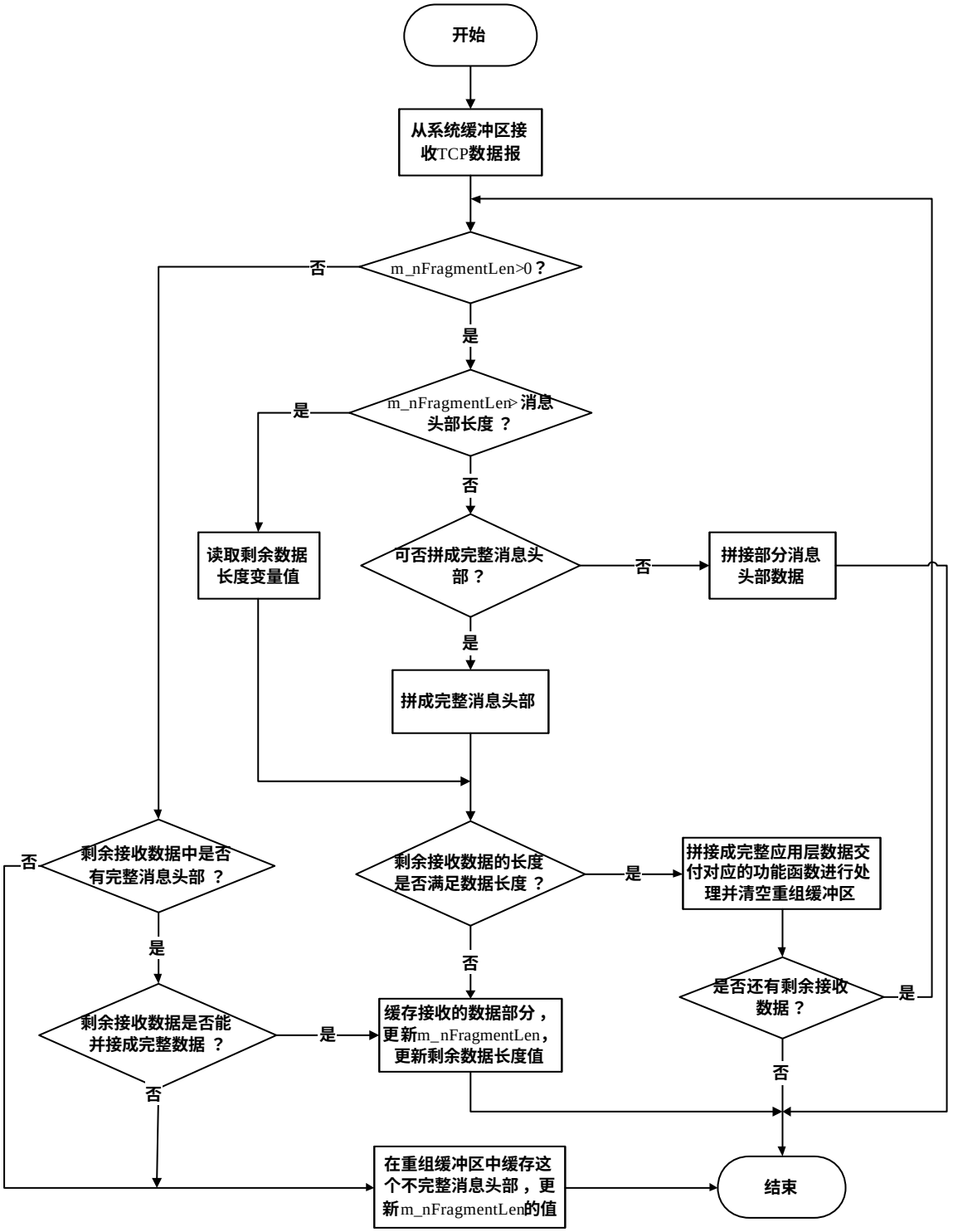
4.1.1 通信服务器应用层协议处理模块

通信服务器应用层协议处理模块主要处理考场管理客户端的登录请求、获取所有考点以及该考点考场个数信息的请求、下载所有考生信息文件的请求、获取当前考试试卷的请求、已下载试卷的反馈信息、重新从通信服务器下载试卷请求和上传考试结果文件信息以及内容的请求。该模块又分为应用层数据重组和应用层数据处理两个子模块。

（1）应用层数据重组子模块

由于通信服务器与考场管理客户端之间是以面向连接的 TCP 协议作为传输层协议服务于应用层的，而 TCP 协议定义了 TCP 数据报传输时的端到端的最大数据块的长度，即最大报文长度 MSS（这个值一般是 TCP 通信两端协商的）。若应用层传输的数据长度大于 MSS，则会被分段传输，所以通信服务器接收 TCP 数据报后必须对报文进行应用层协议数据包的重组，然后将完整的应用层协议数据包加入消息队列，以便进行后继的协议处理过程，这部分工作由应用层数据重组子模块来承

担。应用层数据重组子模块的工作流程如图 4.1 所示。



注：m_nFragmentLen**为重组缓冲区的缓冲数据长度值**

图 4.1　**应用层数据重组子模块的工作流程**

应用层数据重组子模块的重组算法比较复杂，这是由于接收的应用层协议数据包在理论上存在多种分段情况，算法必须考虑到每种可能情况并进行处理，算法如下：

①从系统缓冲区接收一段数据。

②检查重组缓冲区的缓冲数据长度 m_nFragmentLen 是否大于 0，大于 0 则转到步骤③，为 0 则转步骤⑥。

③如果有需要重组的协议数据包，再判断 m_nFragmentLen 的长度是否大于消息头部长度（MSG_HEADER 结构体长度），若大于则转步骤④，否则，转步骤⑧。

④拼接完整的消息头部，读取头部的数据长度信息并于剩余的接收数据长度作比较，如果剩余数据长度大于数据长度则转步骤⑤，否则转步骤⑨。

⑤拼接成完整的协议数据包，提交给数据处理模块，并清空重组缓冲区，置 m_nFragmentLen 为 0。判断是否还有剩余接收数据，若有则转步骤⑥，否则转步骤⑩。

⑥接收的数据长度是否大于消息头部长度，若大于则转步骤⑦，否则，转步骤⑧。

⑦读取消息头部的数据部分长度，与除去消息头部长度的剩余接收数据长度进行比较，若剩余接收数据长度大于协议数据包数据部分长度，则转步骤⑤，否则转步骤⑨。

⑧拼接不完整消息头部，更新 m_nFragmentLen 的值，并转入步骤⑩。

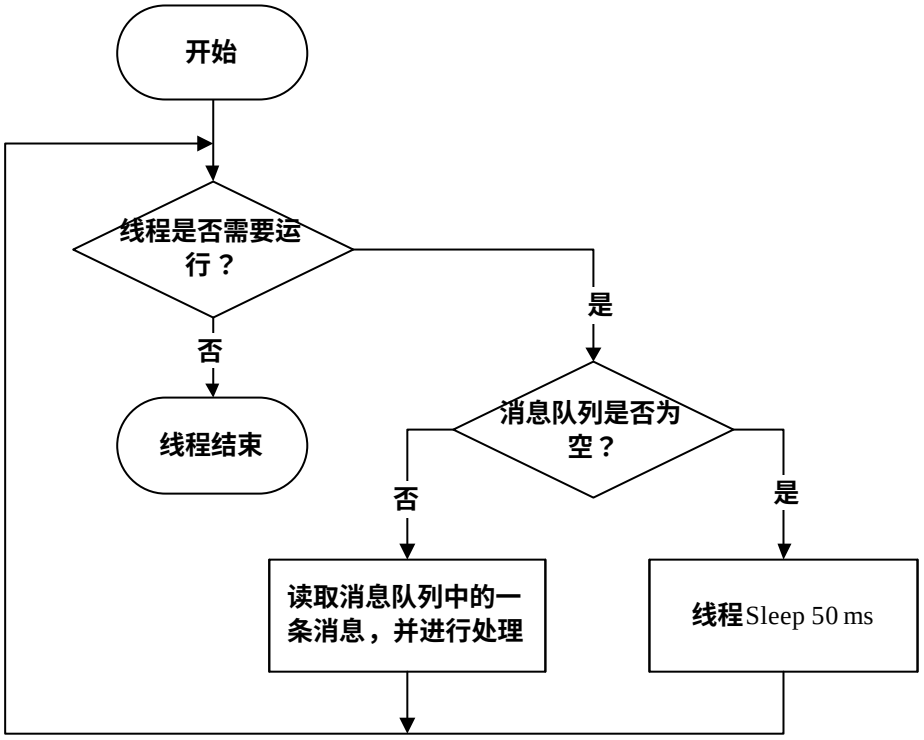
⑨拼接不完整的数据部分，更新 m_nFragmentLen 的值，并转入步骤⑩。

⑩结束。

（2）应用层数据处理子模块

应用层数据处理子模块以线程方式运行，循环查询消息队列中的应用层协议数据包，然后调用消息处理函数进行应用层数据处理，而这个数据处理过程则是根据不同的协议类型（消息 ID）交由各相应处理函数进行处理。线程启动后，循环检测线程运行标志。如果运行标志值为假，则退出循环并结束线程；如果为真，则测试消息队列是否为空，若不为空则取出消息队列中的一条消息进行处理，否则，调用

Sleep **函数进入等待状态，在处理完一条消息后或者等待时间到，则继续测试线程运行标志。应用层数据处理子模块线程的工作流程如图** 4.2 **所示。**



注：此处的消息队列中实际存放的是应用层数据包

图 4.2　**应用层数据处理子模块线程的工作流程**

应用层数据处理子模块处理功能的核心代码段给出如下：

```
pNode = g_RecvQueue.front(); //取出消息队列的指针
pMsgHdr = (PMSGHEADER)pNode->pchData; //转换为消息头部结构//类型
pMsgData = (LPTSTR)pMsgHdr + MSG_HEADER_LEN; //读消息数据部分
Decode(Sessionkey, pMsgData, iCipherLen, plaintext, iPlainLen) //对数据解密
switch( pMsgHdr->nMsgID ) //处理各种消息
{
    //考场管理系统要求获取所有考点以及该考点考场个数的信息
    case MANAGER_LOGON:OnTestSitesInfo();break;
    //考场管理系统登录消息
    case MANAGER_LOGON:OnManagerLogon(pMsgData);break;
```

```
…
//接收结果文件内容
case GET_PAPERFILES:OnSendResultFile(pMsgData, MsgHdr->nDataLen);
break;
default:break;
}
```

应用层数据处理子模块的数据处理流程如图 4.3 所示。从消息队列中取出一条消息数据；对消息数据进行解密操作（如果需要）；对解密后的数据提取消息头部信息；依次判断消息 ID 值（即协议类型）；根据消息 ID 值调用不同的功能函数。

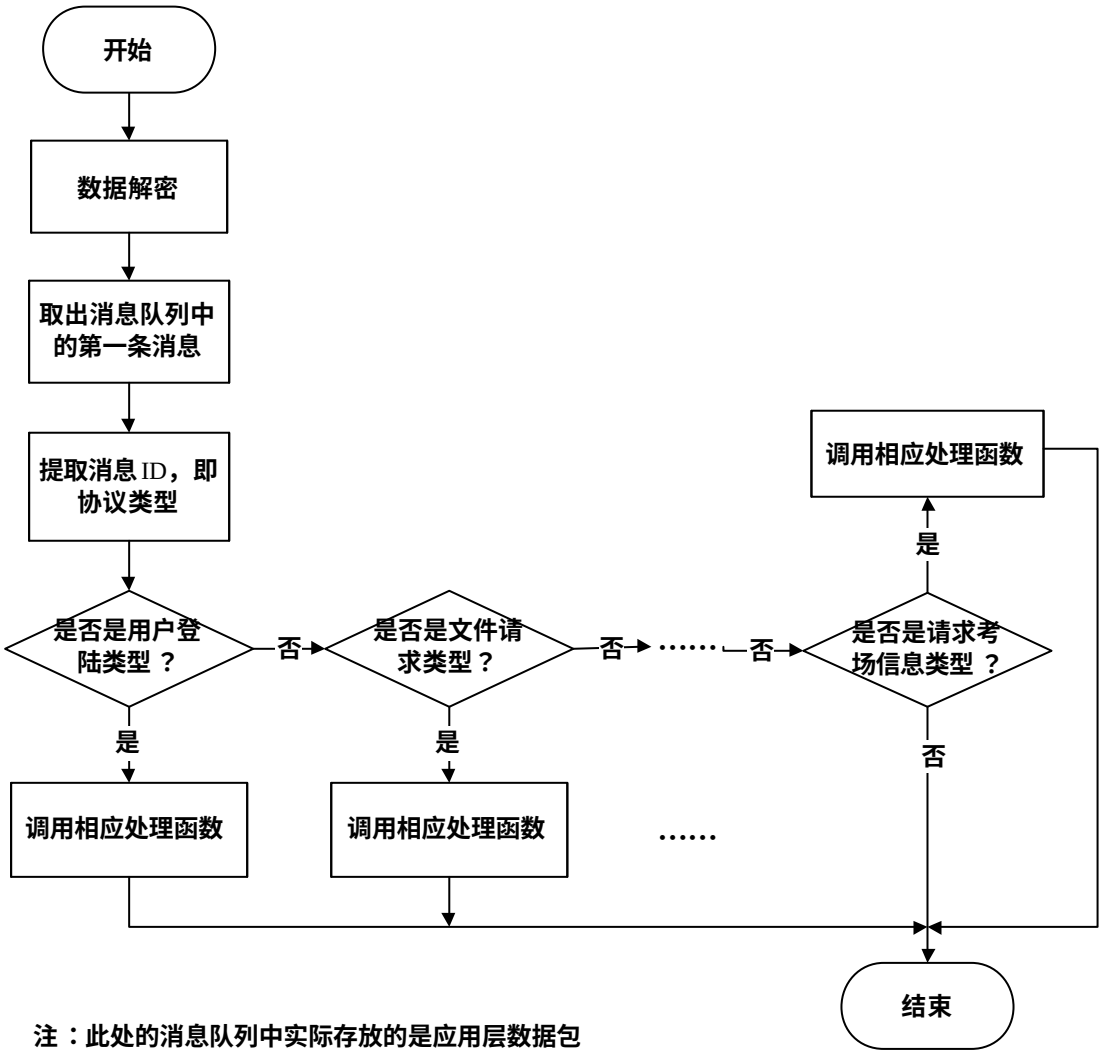


图 4.3　应用层数据处理子模块的数据处理流程

4.1.2 考场管理客户端应用层协议处理模块

考场管理客户端应用层协议处理模块的模块结构和各子模块的处理流程都与通信服务器应用层协议处理模块相同，所不同的只是具体的协议类型分拣和处理不同，因此此处不再作进一步讨论。

4.2 身份认证模块的实现

4.2.1 动态口令生成子模块

动态口令生成子模块的工作流程如图 4.4 所示。该子模块主要实现动态口令生成算法。

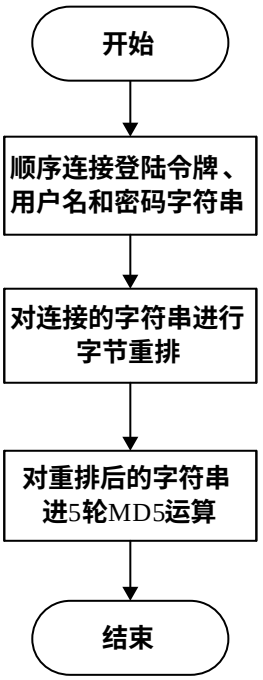


图 4.4　动态口令生成子模块工作流程

动态口令生成子模块对认证服务器生成的登录令牌（随机数值）、用户名和密码的字符串进行连接并进行字节重排运算，之后再对重排的数据进行 5 轮 MD5 哈希运算生成 16 字节的动态口令。字节重排是对字符串中每个字节重新进行排列，排列规则是以无符号字符值的大小交替排列，即第一个字节为最大无符号字符，第

二个字节为最小无符号字符，第三个字节为次大无符号字符，依此类推。

动态口令生成算法处理功能的核心代码段给出如下：

//链接登录令牌、用户名和密码字符串，通过内存拷贝实现

```
memcpy(pBuffer, plogtoken, iLogTokenSize);
memcpy(pBuffer+ iLogTokenSize, username.GetBuffer(0), username.GetLength());
memcpy(pBuffer+ iLogTokenSize + username.GetLength(), password.GetBuffer(0),
        password.GetLength());
ReArray(pBuffer, iBufferLen);//调用字节重排函数
MD5(pBuffer, iBufferLen, LOOP_TIME, pDynamicPassword);//调用 MD5 函数
```

其中，字节重排功能实现的函数原型为：

void ReArray(UCHAR pBuffer, int iBufferLen)，其中 pBuffer 是待重排的字符串缓冲区首指针，iBufferLen 为缓冲区的长度值。

字节重排函数的工作流程图如图 4.5 所示。

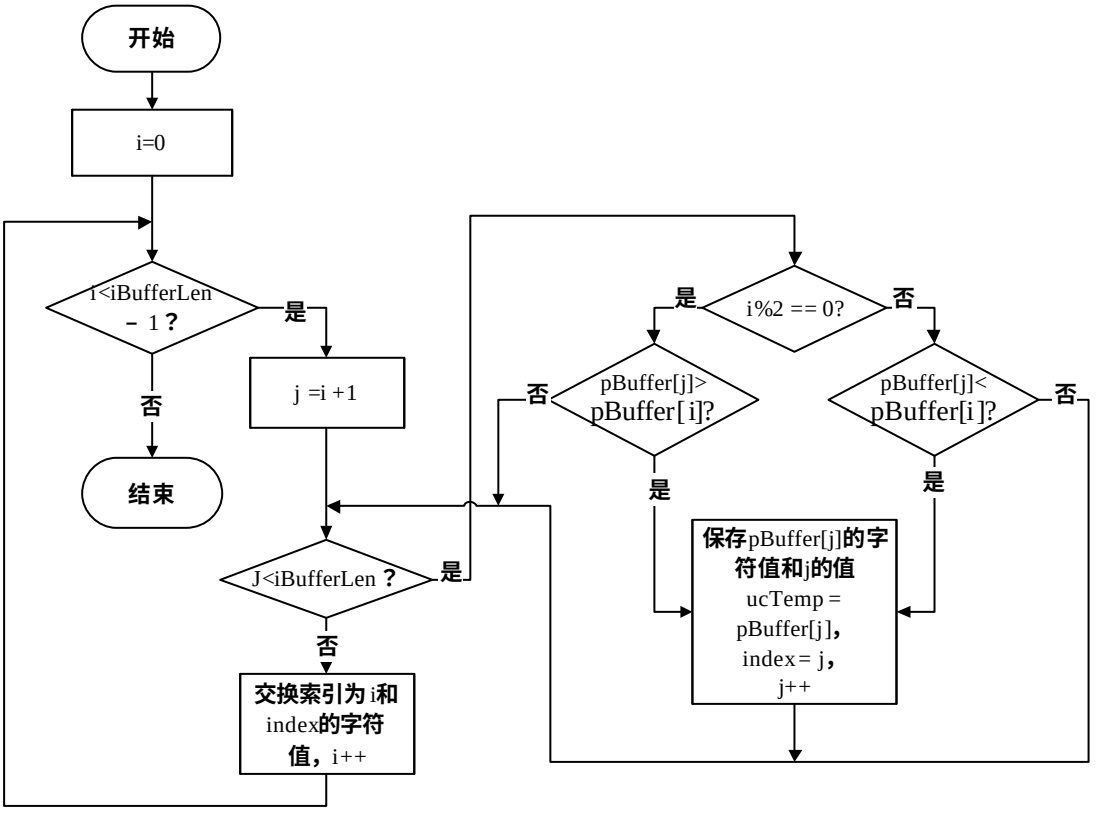


图 4.5　字节重排函数的工作流程

字节重排函数的实现思想：从第 0 个字符到第 n-2 个字符（设字符串长度为 n，字符串索引值从 0 开始），每次从包括该字符到最后一个字符的字符串中选择一个字符与该字符进行位置互换。互换规则是当该字符的位置索引是偶数时，选取最大字符值的字符进行位置互换，当该字符的位置索引是奇数时，选取最小字符值的字符进行位置互换。

MD5 哈希函数使用的是第三方函数库实现，MD5 算法的函数原型为：

void MD5(UCHAR pBuffer, int iBufferLen, int iLoop, UCHAR pResult)，其中 pBuffer 是待哈希运算的字符串缓冲区首指针，iBufferLen 为缓冲区的长度值，iLoop 为 MD5 运算次数，pResult 为哈希运算结果，因为结果长度固定为 16 字节，所以无需说明。其实现细节略去。

4.2.2 客户端代理子模块

客户端代理子模块负责处理：与通信服务器之间的登录类型的协议数据，包括向通信服务器发出登录请求，接收通信服务器发送的登录令牌并提交登录用户的验证信息（用户名、密码和动态口令）；与其他考场管理客户端的客户代理子模块之间的身份认证。

这其中最关键的部分是提交登录用户的验证信息以及客户代理子模块之间的身份信息。这些信息的生成方法在前述章节中已有详细说明，而登录用户验证信息的验证流程将在 4.2.3 节认证子模块中说明。在此仅给出客户端代理子模块间的身份验证信息的验证流程，如图 4.6 所示。

其中，提取登录用户验证信息的过程是：对解密后的数据取其前 24 个字节（因为会话密钥明文为 16 字节，经过 TEA 加密后，将会被填充为 24 字节数据），保存为待解密会话密钥（解密密钥为密码密钥），剩余数据保存为待解密的用户名密文信息。

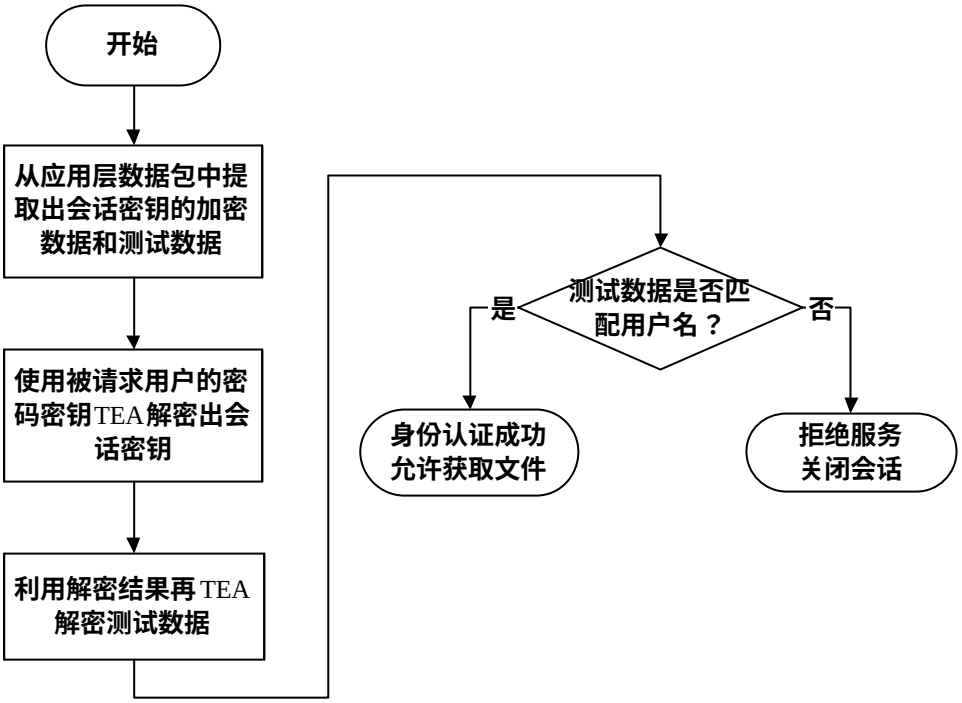


图 4.6　**客户端代理子模块间的身份验证信息的验证流程**

登录用户验证信息数据部分格式如图 4.7 **所示。**

注：SessionKey **和** Testing Data **都是** TEA **加密后的结果**

图 4.7　**登录用户验证信息数据部分格式**

4.2.3 认证子模块

认证子模块负责生成随机登录令牌并对客户端代理子模块发送过来的登录用户验证信息进行验证。登录用户验证信息的验证过程是：首先，根据用户信息数据库中的用户信息计算出密码密钥，并对客户端代理子模块提交的静态验证信息进行 TEA **解密，然后将解密结果与登录用户名进行对比；其次，通过调用动态口令生成子模块计算出动态口令信息，用以对比客户端代理子模块提交的动态口令信息。**

认证子模块的认证流程如图 4.8 **所示。**

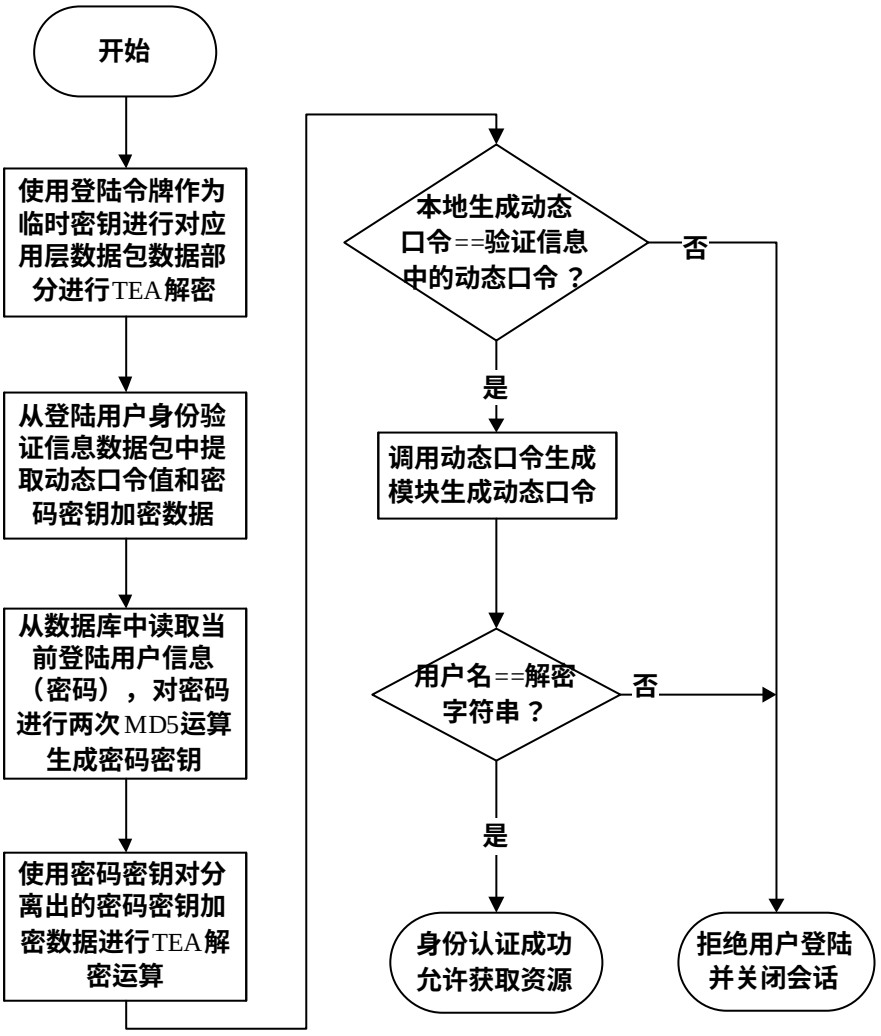


图 4.8　**认证子模块的认证流程**

提取登录用户验证信息的过程是对解密后的数据取其前 16 **个字节（因为生成的动态口令是一个** 16 **字节的字符串值），保存为动态口令数据（解密密钥为密码密钥），剩余数据保存为待解密测试数据，即登录用户的用户名。登录用户验证信息数据部分格式如图** 4.9 **所示。**

0 字节	24 字节
DynamicPassword	user name

注：user name **是** TEA **加密后的结果**

图 4.9　**登录用户验证信息的数据格式**

登录令牌生成算法流程如图 4.10 所示。

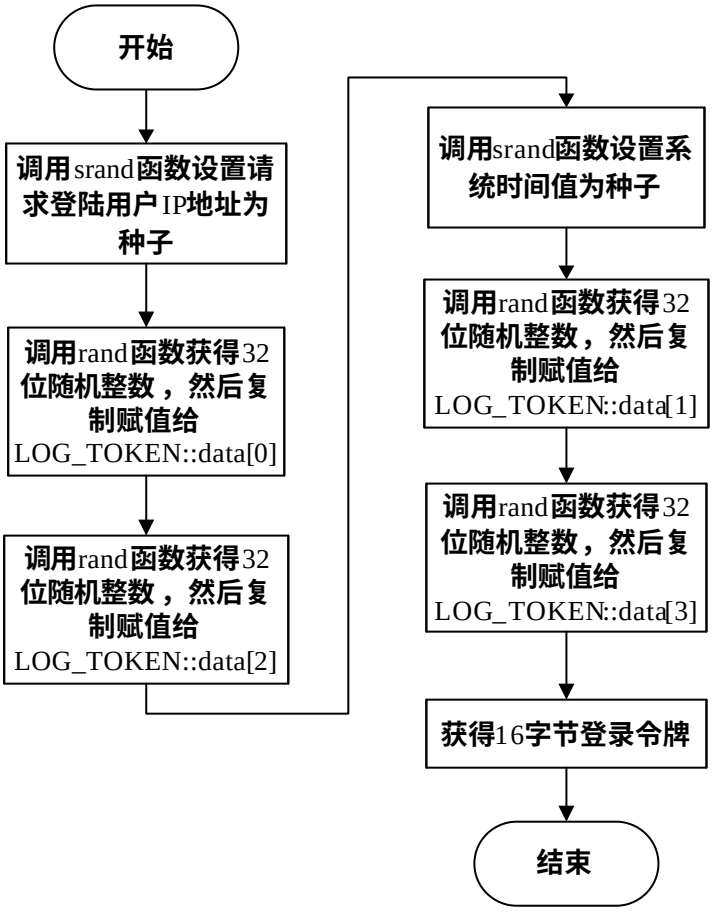


图 4.10　登录令牌生成算法流程

登录令牌的生成使用了一种简单的算法，使用 C/C++运行时函数库的伪随机数生成函数 rand 函数，进行四次随机数计算，调用 srand 函数设置随机数种子，前两次计算以请求登录用户的 IP 地址作为种子，而后两次计算以请求登录的时间（考试中心当前时间）作为种子，然后把这四个随机数交替填充在 LOG_TOKEN 随机令牌结构中。LOG_TOKEN 结构定义如下：

```
typedef struct log_token
{
    int data[4];
}LOG_TOKEN;
```

4.3 数据加密模块

数据加密模块包括加密、解密子模块和密钥生成模块。由于加密策略已在前述章节中进行了探讨，所以在 4.3.1 节和 4.3.2 节中只涉及各模块的工作流程图解以及算法实现。

4.3.1 数据加密模块的实现

数据加密流程如图 4.11 所示。

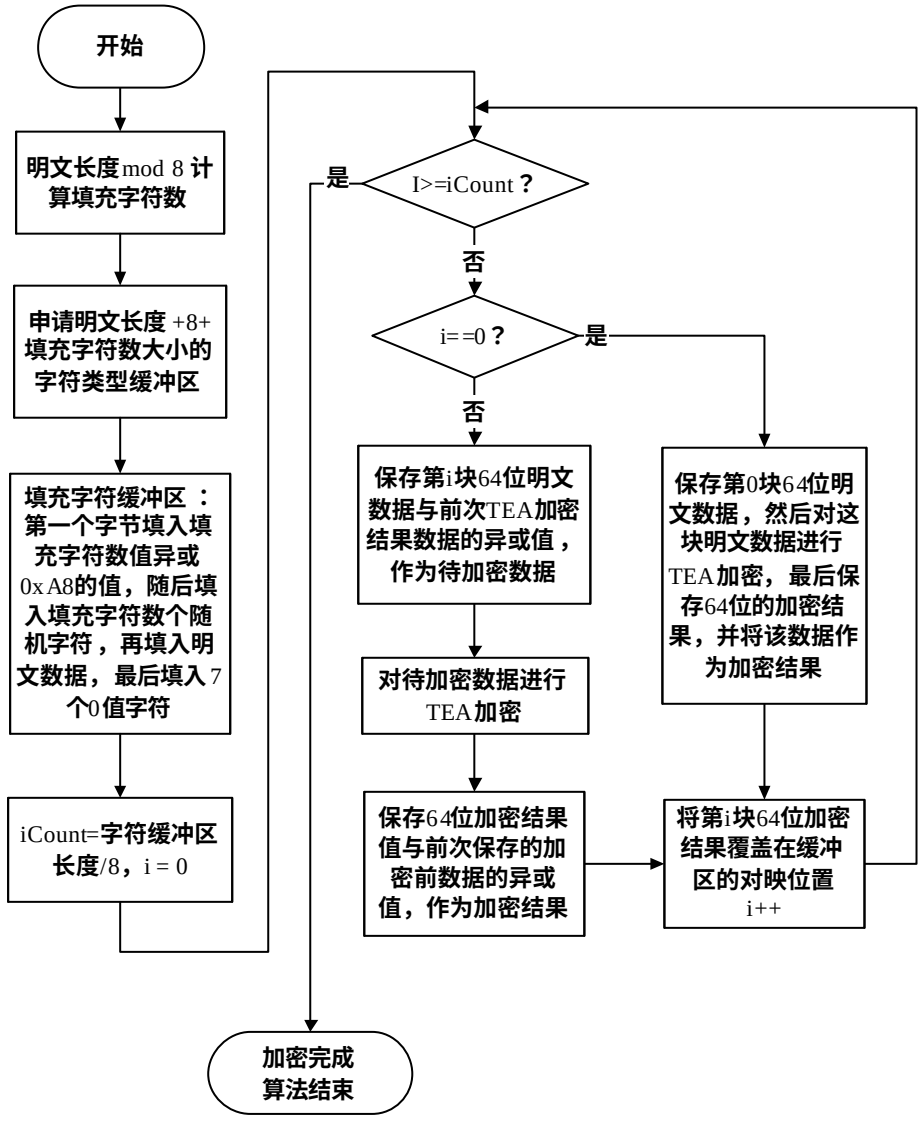


图 4.11　数据加密算法流程

该算法在调用 TEA 加密函数的前后进行了填充和交织运算。

TEA 加密算法流程如图 4.12 所示。

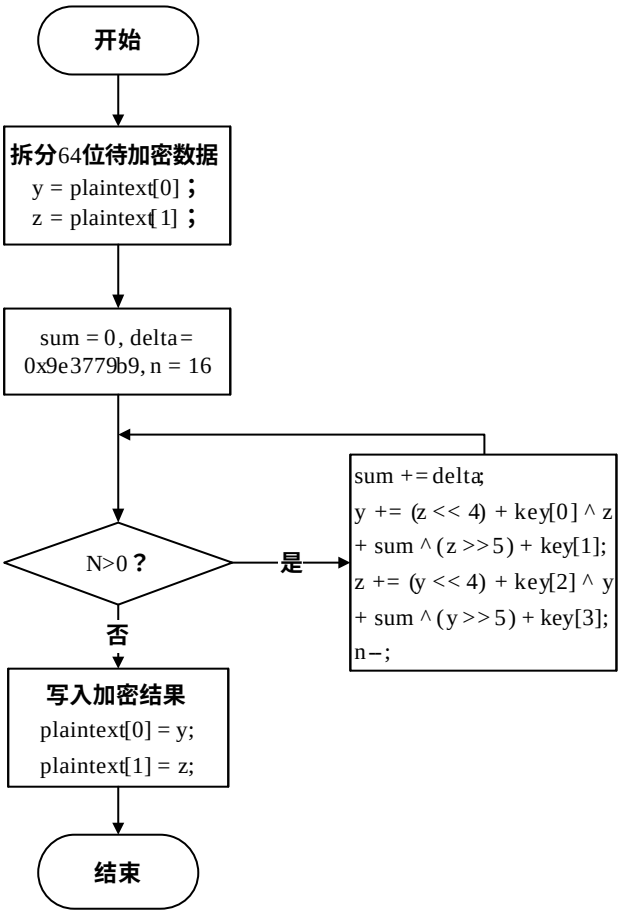


图 4.12　TEA 加密算法流程

TEA 加密算法的函数实现如下：

```
void TEAEncode (ULONG *plaintext, ULONG *key)
{
    ULONG y = plaintext[0], z = plaintext[1];
    ULONG sum = 0, delta = 0x9e3779b9, n = 16;
    while (n-->0)
    {
        sum += delta;
        y += (z << 4) + key[0] ^ z + sum ^ (z >> 5) + key[1];
```

```
        z += (y << 4) + key[2] ^ y + sum ^ (y >> 5) + key[3];
    }
    plaintext[0] = y,     plaintext[1] = z;
}
```

4.3.2 数据解密模块的实现

数据解密流程如图 4.13 **所示。**

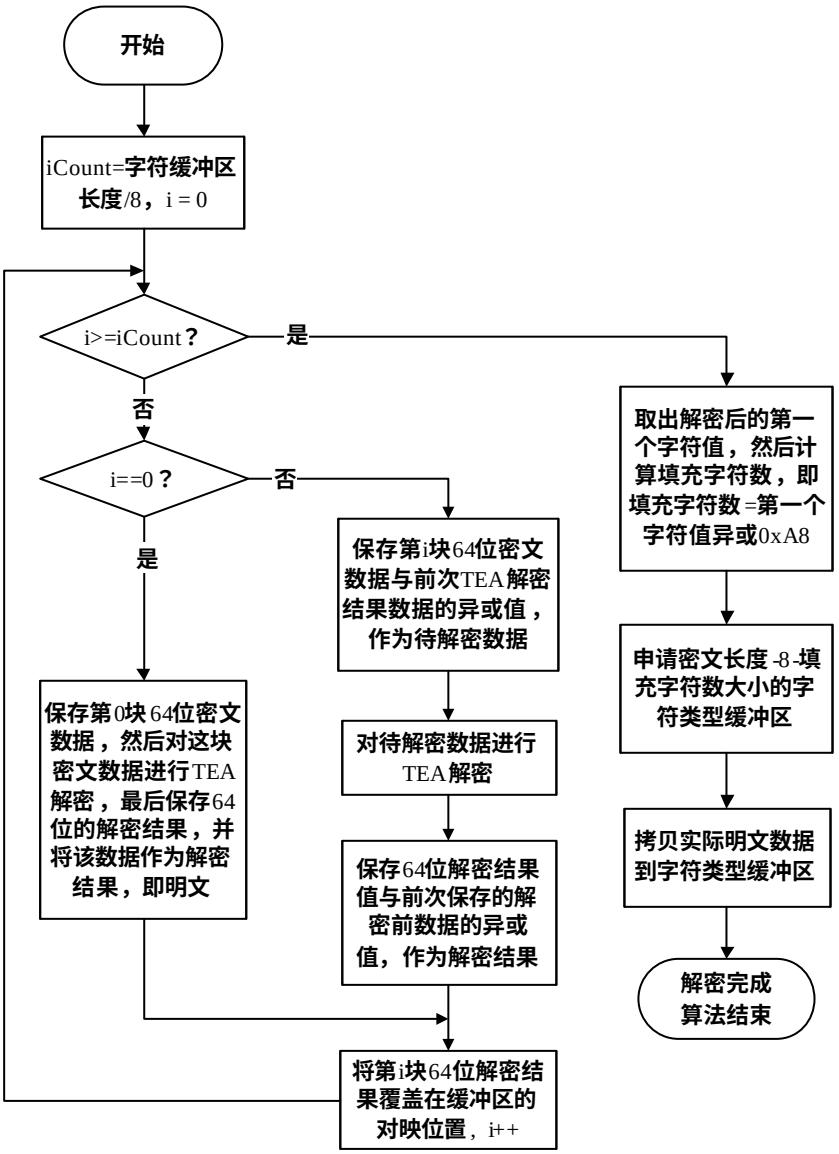


图 4.13　**数据解密算法流程**

该算法在调用 TEA **解密函数的前后进行了填充和交织运算。**

TEA **解密算法流程图如图** 4.14 **所示。**

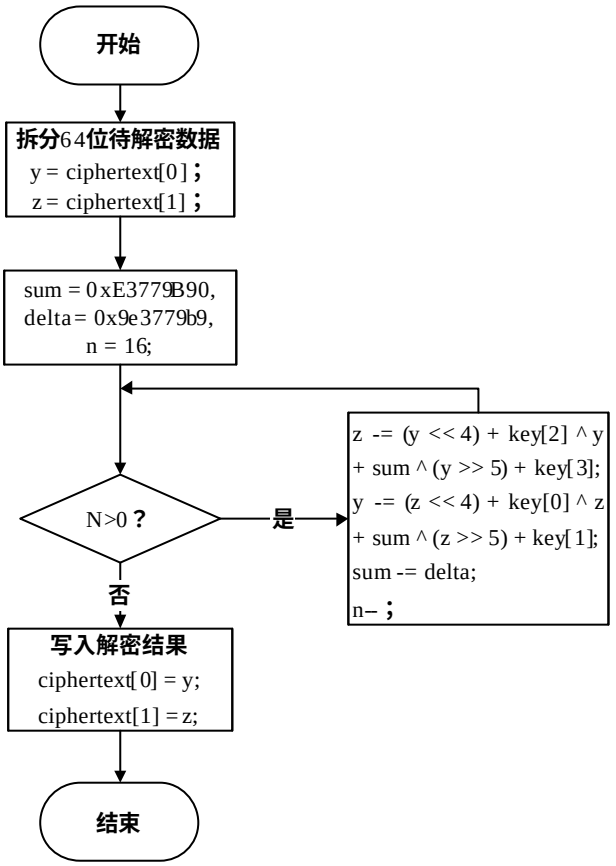


图 4.14　TEA **解密算法流程**

TEA **解密算法的函数实现如下：**

```
void TEADecodeFunc(ULONG *ciphertext, ULONG *key)
{
    ULONG y = ciphertext[0], z = ciphertext[1];
    ULONG sum = 0xE3779B90, delta = 0x9e3779b9, n = 16;
    while (n-- > 0)
    {
        z -= ((y << 4) + key[2]) ^ (y + sum) ^ ((y >> 5) + key[3]);
        y -= ((z << 4) + key[0]) ^ (z + sum) ^ ((z >> 5) + key[1]);
        sum -= delta;
```

```
    }
    ciphertext[0] = y, ciphertext[1] = z;
}
```

4.3.3 密钥生成模块的实现

由于通信服务器与考场管理客户端以及考场管理客户端相互之间的每一次会话，都需要一个会话密钥对传输的数据进行加、解密操作，而这个会话密钥的生成和管理是由通信服务器完成的，所以在通信服务器还实现了密钥生成模块。

该模块负责生成每一次会话的 TEA 加密算法的密钥，即一个 128 位的值。该模块复用了身份认证模块中的认证子模块的登录令牌的生成算法，生成一个 16 字节的随机数值作为会话密钥，详细说明请参考 4.2.3 节认证子模块。

将密钥类型定义为登录令牌类型：

```
typedef    LOG_TOKEN    SESSION_TEA_KEY;
```

4.4 小结

本章在无纸化考试系统应用层通信安全机制详细设计的基础上，给出了各功能模块中核心内容的具体实现。讨论了通信服务器和考场管理客户端中的应用层协议处理流程，阐述了身份认证模块及其子模块的功能实现，论述了数据加密策略的算法实现细节。

5 结束语

5.1 已完成的工作

（1）概要分析了国内外无纸化考试以及信息安全技术的发展现状和趋势，阐述了研究无纸化考试系统应用层通信安全机制的理论意义和实用价值。

（2）在对无纸化考试系统体系架构和其安全需求分析的基础上，针对应用层的协议模型、身份认证策略以及数据加密策略，设计并实现了一种无纸化考试系统的应用层通信安全机制，论述了该机制的设计原则以及各功能模块的详细描述。

（3）对无纸化考试系统的通信功能进行了适当的划分，给出了应用层协议的设计方法，说明了无纸化考试系统的应用层协议格式以及类型模型。在此基础上，实现了应用层协议处理模块。

（4）针对实际安全需求，为了有效保护合法用户的身份，讨论了身份认证模块的设计策略和实现技术，阐述了动态口令生成模块、客户端代理模块以及认证模块这三个子模块的设计和实现技术，并重点介绍了动态口令生成算法、登录用户信息验证算法以及登录令牌生成算法。

（5）讨论了数据加解密模块涉及的基本加密算法—TEA 加密算法和 MD5 哈希函数，给出了数据加密模块的加密策略和密钥生成及管理策略，并对这些策略的算法实现进行了详细描述。

实际应用结果表明，所建立的应用层通信安全机制能够为无纸化考试系统提供良好的安全通信保障，并具有较好的普适性和可扩展性，对增强类似应用系统的安全性具有一定的参考价值。

5.2 下一步的工作

（1）整个应用层通信安全机制还没有以最有效的方式集成在一起，可移植性

还不高。因此，下一步的工作需要对该机制中的各功能模块进行整合设计，设计并实现一种有效的体系结构，以提高可移植性。

（2）考场管理客户端之间的身份认证过程只是简单的使用单因子身份认证技术来进行单向身份认证，这种认证过程也存在着一定的安全隐患。因此，下一步的工作需要进一步深入研究身份认证技术，并采取一种第三方认证技术替代此种简单的单因子身份认证技术，以达到更高的安全性、可靠性。

（3）由于时间原因，身份认证模块的登录令牌生成算法以及数据加密模块的会话密钥生成算法共享了一种相对简单的随机数生成算法。这种算法本身的安全性是不够的，并且易于破解。因此，下一步的工作需要分别为两个模块设计出不同的、高可靠性、高可靠性以及不易破解的高性能随机数生成算法。

致　谢

在论文即将完成、两年的硕士学习阶段即将结束之际，回首走过的日子，我倍感荣幸，因为在这美丽的校园里遇到了许多极具才华的老师和学子。

首先，衷心感谢我的导师——德才兼备的陈晓苏老师。他为人开明，给我们创造了一个轻松的研究环境。同时，他治学严谨、知识渊博、观点新颖，使学生在学术上受益匪浅。感谢肖老师对我学习、工作上的指导，使我在理论和实践上都不断得到提高。感谢吴老师给我的鼓励和在为人处世上对我的教导，这对我的一生将产生重大影响。感谢刘辉宇老师和纪俊文老师，从他们那里我获取了不少宝贵的知识和经验。

感谢我项目研发中的伙伴：吴金华博士、张志广博士、熊兵博士、魏明、肖明、郭琦同学，他们经验丰富，认真负责，从他们身上我学到了许多专业知识。

感谢刘辉宇老师、吴金华博士、张志广博士、陈宁博士、余永升博士、魏明、肖明、卫怡、姚霞、李阳、刘忠文，他们在我论文写作过程中，给我提出了很多宝贵的意见和建议，给予了我巨大的帮助。

感谢魏明、肖明、卫怡、姚霞、李阳、刘忠文、宋方方、朱哲、李志成同学，感谢你们这两年来的友好、鼓励、支持和帮助。

特别感谢吴金华博士和张志广博士，在我的整个学习阶段里，他们给予了我许多慷慨无私的帮助，在我困惑不解的时候帮我指出方向。

永远感谢我的家人，他们对我精神上的鼓舞、殷切的期望和真挚无私的爱一直是我奋斗的力量源泉。

感谢所有关心和帮助我的人，是你们的支持使我走到了今天，谢谢你们。

参考文献

[1] 中国信息安全产品测评认证中心．信息安全理论与技术．第一版．北京：人民邮电出版社，2003．28～29

[2] 黄安健．实现无纸化考试的二项技术处理．上海应用技术学院学报，2003，3(1)：66～68

[3] 杨牧祥，王占波．考试系统网络版研究与应用．河北中医药学报，1999，14(4)：42～44

[4] 朱国华．网络考试软件的设计汪远征．郑州纺织工学院学报，1999，10(4)：57～60

[5] 李东红，董春丽，林红军等．多层次 Client/Server 结构及其应用．信息工程大学学报，2000，(4)：73～76

[6] 郑德庆，梁武，谭共志．基于浏览器/服务器结构的网络无纸化考试和管理系统．华南师范大学学报(自然科学版)，2002，(3)：22～25

[7] 谢冬青，李超，周洲仪．网络安全协议的一般框架及其安全性分析．湖南大学学报(自然科学版)，2000，27(12)：90～94

[8] Kluepfel H M. Securing a global village and its resources. IEEE Communications Magazine, 1994, 32(9): 82~89

[9] 张晓婷，孙祝广．国内外密码理论与技术研究现状及发展趋势．中国科技信息，2006，(14)：257～258

[10] Stillman, Rona B, Defiore et al. Computer Security and Networking Protocol: Technical Issues In Military Data Communications Networks. IEEE Transactions on Communications, 1980, 28(9): 1472~1477

[11] Eloff J.H.P, Eloff M.M. Information security architecture. Computer Fraud and Security, 2005, (11): 10~16

[12] Jahl C. The information technology security evaluation criteria. Software

Engineering, 1991, (13): 306~312

[13] **王强，杨政，王维宏．网格安全体系结构的研究与改进．科技信息(学术研究)，**2007，(9)：192～193

[14] **李俊成，宋君，祁雯等．信息对抗理论与技术研讨．吐哈油气，**2006，(3)：271～274

[15] **冯登国．国内外信息安全研究现状及发展趋势(摘编)．信息网络安全，**2007，(1)：9～11

[16] Day John D, Zimmermann Hubert. OSI Reference Model. Proceedings of the IEEE, 1983, 71(12): 1334~1340

[17] **郜宪林．**DoD TRM**与** TCP／IP **比较与分析．计算机工程与应用，**2001，37(20)：60～62

[18] Masashi Inoue, Akihiko Suyama. Application of a computer based education system for aged persons and issues arising during the field test. computer Methods and Programs In Biomedicine, 1999, 59(l): 55~60

[19] Erik Stubkjaer. World Wide Web and university education in remote sensing. ISPRS Journal of Photogrammetry and Remote Sensing, 1997, 52(6): 281~293

[20] Whelan, Paul E. Remote access to continuing engineering education (RACeE). Engineering Science and Education Joumal, 1997, 6(5): 205~211

[21] Doreen Radjenovic, F Layne Wallace. Computer-Based Remote Diabetes Education for School Personnel. Diatetes Technology &Therapeutics, 2001, 3(4): 601~607

[22] D.E.Denning, G.M.Sacco. Timestamps in key distribution protocols. Comm.ACM, 1981, 24(8): 533~536.

[23] T.C.Wu. Remote login authentication scheme based on a geometric approach. Comput Comm, 1993, 18(12): 959~963.

[24] **谭凯军，何晨，诸鸿文．基于矢积的远程口令鉴别方案．电子学报，**2000，28(2)：28～30

[25] M.S.Hwang, L.H.Li. A new remote user authentication scheme using smart cards. IEEE Transaction on Consumer Electronics, 2000, 46(l): 28~30.

[26] F.Leclerc, R.Plamondon. Automatic signature verification. International Journal on Pattern Recognition and Artificial Intelligence, 1994, 8(3): 643~660.

[27] **黄淑宽，林柏钢．常用的口令认证机制及其安全性分析．网络安全技术与应用，**2005，(6)：29～31

[28] **黄清，胡蓉．网络安全系统中的身份认证技术应用及其发展．中国现代教育装备，**2007，(1)：69～70

[29] **邢永明，乔佩利．基于双因子认证技术的统一身份认证的研究．现代制造技术与装备，**2006，(3)：62～65

[30] **杨立超．强双因子身份认证技术．同煤科技，**2003，(3)：45～46

[31] Yuan D, Fan Z P. A secure dynamic password authentic. cation scheme. Journal of Sichuan University, 2002, 39(2): 228~232

[32] **袁丁，范平志．远程动态口令鉴别方案．计算机应用研究，**2001，(7)：64～65

[33] **张述平，杨国明，时武略．数字加密技术与应用．福建电脑，**2006，(7)：44～45

[34] **李广彪，李东生．用序列密码进行网络加密．网络安全技术与应用，**2001，(12)：24～26

[35] **赵剑，杜钦生，王冰冰．分组密码发展现状．长春大学学报，**2006，16(12)：96～99

[36] **欧海文，李凤华，杨名华．对称密钥密码算法的类型测定及其安全性评估．北京电子科技学院学报，**2005，13(2)：35～36

[37] Odlyzko, Andrew M. Public key cryptography. AT&T Technical Journal, 1994, 73(5): 17~23

[38] **伍华健．公开密钥密码体系在网络安全中的应用研究．微计算机信息，**2006，(4)：14～16

[39] **李明，郝晓玲，张建．公开密钥基础设施体系及其缺陷分析．商业研究，**2006，(3)：101～104

[40] **阳光．两种密码体制的结合．福建电脑，**2005，(10)：132～132

[41] **章静，许力，林志伟．自组网中基于簇的混合密钥管理策略．计算机应用，**2006，26(6)：1328～1330

[42] **赵文清，姜波，王德文等．数字签名中哈希函数的分析与研究．计算机工程与应用，**2004，40(32)：155～157

[43] **黄智颖，冯新喜．哈希加密方案．通信技术，**2001，(7)：87～89

附录 英文缩写词

英文缩写	英文全称	中文译名
ARP	Address Resolution Protocol	地址解析协议
ASCII	American Standard Code II	美国标准码 2
ATM	Asynchronous Transfer Mode	异步传输模式
B/S	Browser /Server	浏览器/服务器
CC	Common Criteria	通用准则
CERT	Computer Emergency Response Team	计算机紧急响应小组
CIAC	Computer Incident Advisory Capability	计算机事故咨询能力
COAST	Computer Operations, Audit, and Security Technology	计算机操作、审计和安全技术
C/S	Client/Server	客户端/服务器
DES	Data Encryption Standard	数据加密标准
DNA	Deoxyribonucleic acid	脱氧核糖核酸
DOD	Department of Defence	美国国防部
DSA	Digital signature Algorithm	数字签名算法
FDDI	Fiber Digital Device Interface	光纤数字设备接口
IC	Integrated Circuit	集成电路
ICMP	Internet Control Message Protocol	因特网控制报文协议
ID	Identification	身份标识
IDEA	International Data Encryption Algorithm	国际数据加密算法
IDS	Intrusion Detection Systems	入侵检测系统
IEEE	Institute of Electrical and Electronics Engineers	电器电子工程师协会

英文缩写	英文全称	中文译名
IGMP	Internet Group Multicast Protocal	因特网组管理协议
I/O	Input/Output	输入/输出
IP	Internet Protocol	网络互联协议
IPSEC	Internet Protocol Security	因特网协议安全
ISO	International Organization for Standardization	国际标准化组织
LAN	Local Area Network	局域网
MD	Message Digest	消息摘要
MSS	Maximum Segment Size	最大分段长度
OSI/RM	Open Systems Interconnection Reference Model	开放系统互联参考模型
PC	Personal Computer	个人电脑
PEM	Privacy Enhanced Mail	私用强化邮件
PGP	Pretty Good Privacy	极好的保密性
PIN	Personal Identification Number	个人标识码
PKI	Public Key Infrastructure	公钥基础设施
RARP	Reverse Address Resolution Protocol	逆地址解析协议
RSA	Rivest , Shamir and Allemand	RSA 加密算法
SHA	Secure Hash Algorithm	安全散列算法
S-HTTP	Secure HyperText Transfer Protocol	安全超文本传输协议
S/MIME	Secure/Multipurpose Internet Mail Extensions	安全因特网邮件附件标准
SNA	system network architecture	IBM 系统网络体系结构
SNMP	Simple Network Management Protocol	简单网络管理协议
TCP	Transmission Control Protocol	传输控制协议

英文缩写	英文全称	中文译名
TEA	Tiny Encryption Algorithm	微型加密算法
TCSEC	Trusted Computer System Evaluation Criteria	可信计算机系统评估标准
TLS	Transport Layer Secure protocol	传输层安全协议
UDP	User Datagram Protocol	用户数据报协议
VPN	virtual private network	虚拟专用网络