解决方案：豫龙软件产（股）权交易系统解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/170/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_170922.htm 一、产（股）权交易系统整体架构 产（股）权交易系统采用的编程语言为BORLAND DELPHI7语言和C 语言，语言应用平台为WINDOWS 2000和UNIXWARE711，数据库为非常优秀和优化的ORACLE8i，安装在UNIXWARE711操作系统上。为了更方便的对交易系统的管理和设置交易参数，交易系统的前台管理模块采用在WINDOWS2000操作平台上的DELPHI7语言编写；为使交易系统更加稳定、安全和具有很高的运行速度，后台交易撮合系统采用在UNIXWARE711操作平台上的C语言编写。整个交易系统采用C/S/S三层架构，即后台交易撮合、中间件及前台管理和委托。交易系统的交易数据是通过INTERNET传送客户端，交易数据包括委托指令、数据查询、成交回报、行情信息及客户的出入金数据等，这些数据在INTERNET上以明码的方式传输是非常不完全的，为使数据更安全，要把交易数据加密。下面主要介绍一下中间件和加密算法。为解决分布异构问题，我们采用了中间件技术。中间件是位于平台(硬件和操作系统)和应用之间的通用服务，这些服务具有标准的程序接口和协议。针对不同的操作系统和硬件平台，它们可以有符合接口和协议规范的多种实现。中间件具有如下的一些特点：1、满足大量应用的需要2、运行于多种硬件和OS平台3、支持分布计算，提供跨网络、硬件和OS平台的透明性的应用或服务的交互4、支持标准的协议5、支持标准的接口产（股）权交易系统采用面向消息的

中间件（Message-Oriented Middleware）和交易处理中间件，这样可以大幅度提高连接信息的吞吐量和交易撮合速度。证券交易所和期货交易所都采取的这两中间件技术。加密算法主要有以下几种：1、公开密钥算法
（RSA(Rivest-Shamir-Adelman)是使用最多的公开密钥算法，能够被应用在加密和数字签名中。）2、隐秘密钥算法3、块密码模式4、密文暗码函数（如MD4、MD5）5、随机数字发生器（如RC4、RC5） 产（股）权交易系统采用IDEA (International Data Encryption Algorithm)加密算法，这个算法被认为非常安全。这是目前世界上最好的公开的加密算法，这也是一种比较新的算法，在已经使用过的这些年里，没有关于这种算法的弱点的报告，尽管有无数人对其进行了分析和攻击。 本系统采用国际上认可的公开加密算法并与随机加密结合的加密方式进行加密。对于来往交换的数据我们采用了著名加密算法"IDEA加密算法"的变异64位分组加密算法，它的加密内核是基于"IDEA"的，但它的外部采用了"循环模余异或"的加密算法.整个加密算法采用64位分组16位模余，密钥长度达128位，加密轮数为8轮.变异说明:数据处理前要初始化128位的密钥生成加密密钥数组和解密密钥数组加密过程:1.对要加密的数据与初始密钥进行循环异或运算.2.再用IDEA对数据进行8轮加密运算.3.再对数据与初始密钥的模16值进行异或运算 解密过程为加密过程的逆序3,2,1步.安全性分析: 本加密算法密钥长度为128位---比DES长两倍多。假定采用穷举法进行攻击是有效的，那么，为获取密钥需要2的128次方(等于10的38次方)加密运算.设计一个每秒可以测试10亿个密钥的芯片，并采用10亿个芯片来并行处理，它将花费10的13次方

年.IDEA算法在4轮以上就对差分密码分析免疫了.所以对8轮以上的变异的IDEA算法任何密码分析都是无效的.二、产（股）权交易系统模块组成和功能#61548.（2）交易结算结算主要负责系统数据计算及各种报表的生成打印。交易结算菜单包括数据查询（成交、委托、资金、交易所收益情况、交易统计）、数据结算（数据结算、结算日期管理）、打印报表（日报、月报）会员手续费的按月返还。各类资金及成交情况查询、预览、打印。此程序实现对每日交易后的数据进行清算。对股权交易的资金结算。当日结算后的没有被股权占用的资金可以在第二天通过银证转帐进行出金。#61548.（4）登记托管登记托管：对要进行交易的企业的基本资料的常规操作（基本信息的录入、查找、修改、删除、预览、打印）。对产（股）权的基本量化转换，对进行托管的产（股）权进行TP化及分类、并进行相应的产（股）权编码，基本信息的录入、查找、修改、删除、预览、打印等基本操作；登记托管办理会员的注册，输入会员的基本资料；投资人的注册，输入投资人的基本资料；可以批量开户、会员转让、交易过户等。#61548.（6）撮合系统后台撮合系统是交易系统各模块中最核心的部分。它对会员及投资人的申报和查询操作指令进行解释执行。负责把动态行情和成交回报信息传送到行情播发和成交监控。