学校编码：10384　　分类号＿＿＿＿密级＿＿＿＿

学号：X2014230005　　UDC＿＿＿＿

厦门大学

工 程 硕 士 学 位 论 文

基于 DES 和 RSA 混合加密的即时通信系统的设计与实现

Design and Implementation of Instant Messenger Based on DES and RSA Hybrid Encryption

张驰

指导教师姓名：　吴 清 锋　教 授

专 业 名 称：　软　件　工　程

论文提交日期：　2017 年 04 月

论文答辩日期：　2017 年 05 月

学位授予日期：　2017 年 06 月

指 导 教 师：＿＿＿＿＿＿

答辩委员会主席：＿＿＿＿＿＿

2017 年 04 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

随着计算机网络和移动互联网的发展，即时通信系统（Instant Messenger,即 IM）在人们生活工作中扮演着越来越重要的角色，政府、企业都需要使用即时通信软件来提高工作效率，降低运作成本。最早的即时通信软件能够实现互联网、局域网内的信息沟通、文件传输等功能。随着时代的发展，即时通信软件的功能越来越丰富，可以进行语音、视频聊天，群聊天以及分享心情等等。但是对软件安全性能的关注并没有跟上，用户信息遭到泄露，对即时通信行业造成不良影响，应引起我们的重视。不少企业开始加强对即时通信安全性的研究和开发。本论文就是着眼于此，对安全的 IM 系统进行设计与实现，以供学习借鉴。

论文主要介绍了即时通信系统的发展、运行原理和存在的问题，在此基础上设计并实现一款基于 DES 和 RSA 加密技术的混合加密策略的即时通信系统。该系统可在不影响用户使用的前提下，形成良好的加密策略保证用户信息的安全。通过这种方式，旨在提高用户在网络中传输聊天消息和账号密码信息的安全性。通过加密的手段可以帮助用户抵御嗅探技术窃取用户信息，增加截取信息破译的难度，提高在网络上传递信息信的安全性。系统分为客户端和服务器端，利用 Socket 网络编程技术和加密技术，具体包含：注册与登录模块，好友添加和删除模块，群聊天和服务器管理等功能模块。该系统注重功能的简洁和信息的安全性，把信息安全视为用户的首要保障和迫切需要。

论文遵循软件工程的规范，设计实现该系统。本论文的主要研究内容包括：

1、对现有即时通信系统的功能和发展趋势进行研究，学习如 QQ、MSN 等软件的优势和思路，加深对即时通信原理和功能的理解。

2、对系统进行可行性分析、功能分析和非功能分析等，以用例图、流程图等形式提出对象化需求分析，在研究加密的基础上，提出加强系统安全性的构想和设计方案。

3、利用 Spring、JDBC 等技术设计并实现本系统所需的方法、接口、界面、数据库等各功能模块。

4、搭建模拟局域网和客户机/服务器模式的系统环境，设计测试方案对系统进行功能测试和非功能测试，确定软件的功能是否实现，发现程序设计中完整性、安全性、稳定性等问题。

关键词：即时通信；DES 加密；RSA 加密

ABSTRACT

With the development of computer and Internet, Instant Messenger (IM) plays an increasingly important role in people's lives. The government and enterprises need Instant Messenger to improve work efficiency and reduce costs. The earliest Instant Messenger can connect to the Internet, support information communication, file transfer and other functions. As time flows, IM got more and more functions, such as voice communication, sharing moods , group chat and so on, but the measures on security did not keep up. Users' information was often compromised, which brought bad influence to the IM companies. Because of this situation, the dissertation focuses on how to improve the security of IM on design and implementation.

The dissertation mainly introduces the development of IM system, operating principle and the existence problems. The theme of the dissertation is to design and implement an IM system based on hybrid encryption with DES and RSA. It can provide a good encryption strategy to ensure the security of user information without affecting the user's use. In this way, to improve the security of user chat messages and account information through the network. By the way of encryption, it can help users avoid sniffing technology which steals user information through the Internet. Encryption also increases the difficulty of interception of information deciphering, improving the security of information during Internet transmission. The system is divided into two parts, Client and Server. It uses Socket network programming technology and encryption technology, including: registration and login module, friends add and delete modules, group chat modules, server management and other functional modules. The system focuses on the simplicity of the function and the security of information. It regards information security as the primary guarantee and urgent need for users' concern.

The dissertation follows the method of software engineering to design and implement the system. The main contents of this dissertation include:

1. Finding out the functions and development trend of existing Instant Messenger, studying the advantages and principles of existing IM system, such as QQ, MSN.

2. Carrying out feasibility analysis, function analysis and nonfunctional analysis of

the system. Using UML case diagram and flow chart for requirements analysis to build a demand model. To put forward the idea and design of security IM system on the basis of learning Encryption.

3. Using Spring Bean, JDBC, network programming and other technology to design and implement the IM system which includes interfaces, databases, encryption and other functional modules.

4. A simulation test environment for C/S system testing was built. Test plan for functional testing and non-functional testing was put forward. To make a conclusion about whether the function of the software is up to the requirements analysis and to find out the programs of integrity, security, stability and other issues.

Keywords: Instant Messenger; DES encryption; RSA encryption

目 录

第一章 绪论 1

1.1 研究背景与意义 1

1.2 国内外安全现状 2

1.2.1 IM 软件技术现状 2

1.2.2 IM 软件开发现状 4

1.3 研究目标与系统特点 7

1.4 论文组织结构 8

第二章 系统需求分析 10

2.1 系统建设目标分析 10

2.2 系统的可行性分析 10

2.2.1 市场可行性 11

2.2.2 技术可行性 13

2.2.3 经济可行性 14

2.2.4 操作可行性 14

2.2.5 社会可行性 15

2.3 系统功能需求调研 15

2.4 系统功能需求分析 17

2.4.1 客户端主要功能 17

2.4.2 服务器端主要功能 18

2.4.3 用例图 19

2.4.4 数据流图 23

2.5 接口需求分析 24

2.5.1 服务器接口需求分析 24

2.5.2 客户端接口需求分析 25

2.6 非功能需求分析 26

2.7 本章小结 30
第三章 系统设计 32
3.1 系统设计的目标和任务 32
3.1.1 系统设计的目标 32
3.1.2 系统设计的任务 33
3.2 系统框架设计 33
3.2.1 局域网总体框架设计 33
3.2.2 广域网总体架构设计 35
3.2.3 即时通信系统技术框架 38
3.3 功能模块设计 42
3.3.1 通信功能模块的划分 42
3.3.2 系统功能模块详细设计 43
3.4 系统接口设计 50
3.4.1 内部模块接口设计 51
3.4.2 外部接口设计 52
3.4.3 数据库接口设计 52
3.5 数据库设计 53
3.6 本章小结 56
第四章 系统实现 57
4.1 系统的实现环境 57
4.2 系统功能实现 57
4.2.1 系统服务器端功能的实现 57
4.2.2 系统客户端功能的实现 59
4.3 加密模块的实现 64
4.4 本章小结 64
第五章 系统测试 65
5.1 测试环境与测试工具 65
5.2 测试方案 65

5.3 功能测试 66
5.4 性能测试 69
5.5 测试结论 72
5.6 本章小结 74
第六章 总结与展望 75
6.1 总结 75
6.2 展望 76
参考文献 77
致 谢 78

CONTENTS

Chapter 1 Introduction 1
1.1 Research Background and Meaning 1
1.2 Security Condition at Home and Abroad 2
1.2.1 IM Software Technology Situation 2
1.2.2 IM Software Development Situation 4
1.3 Research Objectives and System Characteristics 7
1.4 Organizational Structure of Dissertation 8
Chapter 2 System Requirements Analysis 10
2.1 System Construction Target Analysis 10
2.2 System Feasibility Analysis 10
2.2.1 Market Feasibility 11
2.2.2 Technical Feasibility 13
2.2.3 Economic Feasibility 14
2.2.4 Operational Feasibility 14
2.2.5 Social Viability 15
2.3 Research on System Function Requirement 15
2.4 System Functional Requirements Analysis 17
2.4.1 Client-side Main Function 17
2.4.2 Server-side Min Functions 18
2.4.3 Use Case Diagram 19
2.4.4 Data Flow Diagram 23
2.5 Interface Requirements Analysis 24
2.5.1 Server Interface Requirements Analysis 24
2.5.2 Client Interface Requirements Analysis 25
2.6 Non-functional Requirements Analysis 26
2.7 Smmary 30
Chapter 3 System Design 32
3.1 System Design Goals and Tasks 32
3.1.1 Instant Messaging System Design Goals 32

3.1.2 Instant Messaging System Design Tasks 33
3.2 System Frame Design 33
3.2.1 Overall Framework Design of Local Area Network 33
3.2.2 Overall Architecture Design of Wide Area Network 35
3.2.3 Instant Messaging System Technology Framework 38
3.3 Functional Module Design 42
3.3.1 Division of Communication Function Modules 42
3.3.2 System Function Module Detailed Design 43
3.4 System Interface Design 50
3.4.1 Internal Module Interface Design 51
3.4.2 External Interface Design 52
3.4.3 Database Interface Design 52
3.5 Database Design 53
3.6 Summary 56
Chapter 4 System Implementation 57
4.1 System Implementation Environment 57
4.2 System Function Implementation 57
4.2.1 Implementation of System Server Function 57
4.2.2 Implementation of System Client Function 59
4.3 Implementation of Encryption Module 64
4.4 Summary 64
Chapter 5 System Testing 65
5.1 Test Environment and Test Tools 65
5.2 Test Program 65
5.3 Function Test 66
5.4 Performance Testing 69
5.5 Test Discussion 72
5.6 Summary 74
Chapter 6 Conclusion and Prospect 75
6.1 Conclusion 75
6.2 Prospect 76
References 77

Acknowledgements.....78

第一章 绪论

1.1 研究背景与意义

即时通讯软件（即 Instant Messenger, IM）最早是由以色列人首先提出构想并予以实现。在 1996 年，三名以色列人决定开发一种使人与人在互联网上能够快速直接交流的软件，他们为新软件取名 ICQ[2]。通过 ICQ 软件，用户可以在互联网上聊天、传递文件，这也成为所有即时通信软件最基础的应用。随后他们成立了公司，向注册用户提供互联网即时通讯服务。

随着 ICQ 的发明和使用，即时通信如雨后春笋一般迅速发展壮大，各种即时通信软件也迅速出现，用户人群不断扩大，逐渐从年轻的计算机爱好者到广大青少年人群，如今已经遍及各个年龄层、不同职业的人群[1]。国内著名的即时通信软件有：腾讯 QQ，阿里旺旺，飞信等，他们逐渐发展成熟并受到用户的广泛欢迎。**腾讯 QQ** 由于发展的早，并且能够抓住青年用户的兴趣点，因此获得了最大的市场份额，并且扩大到各个年龄层[7]。**阿里旺旺**借助淘宝，对使用淘宝的买家和卖家更多地注册和使用阿里旺旺即时通信软件，阿里旺旺借助对交流信息可以进行保存，作为消费者和卖家维护自身权益的证据，因此具有和淘宝广泛的黏连性，离开淘宝，阿里旺旺则失去生命力。**飞信**则主要是中国移动的手机号码进行注册的用户，飞信借助移动公司的网络，能够向用户手机群发短信，提供了计算机端与手机端的连接和信息传递，曾经风靡一时受到广泛使用。移动即时通信软件则以微信、陌陌、易迅等为代表，成为新兴即时通信软件的发展趋势，随着移动即时通信软件的迅速普及，传统的基于计算机的互联网络即时通信软件用户规模受到很大影响，使得大家对计算机即时通信软件的使用迅速减少，成为微信等移动即时通信软件的陪衬。微信的出现成为即时通信软件行业的一次重要革命，具有快速的消息传递，随时随地的朋友动态分享，便捷的添加好友，与手机和 QQ 号进行申请和发现好友迅速吸引了年轻用户的注意，并且迅速扩大了使用人群。之后又加入了微信支付，微信红包等实用功能，使得用户忠诚度不断升高，并且在如今保持着长盛不衰的发展态势，一跃成为我国最大的即时通信软件。其模仿者如

陌陌、易迅等移动即时通信软件也拥有许多使用者，但与微信相比，依然难以撼动微信的领军地位。

但是，在新的竞争环境下，现代企业、单位的交流节奏越来越快，内部的工作协调与交接需要快速完成，对沟通的形式有更丰富的需求。为了应付瞬息万变的市场需求，计算机即时通信软件等即时通信技术在企业和单位逐渐兴起[3]。它比电子邮件更快捷，比手机、电话具有可记录性，费用低，数据形式多样。它们需要在工作场所内部搭建局域网，为了便于工作的沟通交流，也会设计关于局域网即时通信系统，如企业即时通信系统、图书馆即时通信系统、医院即时通信系统等。工作中使用的即时通信系统，一方面跟上了信息社会的发展需要，另一方面也产生了即时通信软件的安全性问题。与此同时，QQ、MSN、阿里旺旺、飞信等他们的隐私保护也成为我们需要关注的课题。

随着我国进入“互联网+”时代，互联网的作用渗透到工作、生活的各个方面，有许多人会通过即时通信软件作为文件传输，交流工作的必备工具，其作用涵盖的范围也越来越广，还有承担着交流商业沟通、工作联系、公关拓展等多方位功能，其随之而来的，信息的安全性和账号的安全性愈加重要，除了在我们使用即时通信软件时提高安全意识，更要在技术上和软件设计上提高即时通信软件的安全性能，保护用户的隐私。

1.2 国内外安全现状

在信息化浪潮席卷全球的今天，我们常用的即时通信工具如 QQ、Skyep 等，给每个人提供了即时有效的信息交换。但信息安全技术应用的不足，对提高即时通信软件的服务水平、业务创新和提升核心竞争力等方面产生严重制约。对于在数据传输、身份验证等方面缺少安全措施的现状，用户常常对使用即时通信软件有很多担忧。

1.2.1 IM 软件技术现状

调查显示，随着即时通信软件使用用户数量的增加，即时通信更容易受到黑客的攻击，在 2003 年就出现了“我爱你”、“MSN 窃贼”、“JITUX”等病毒专门针对 MSN 用户，QQ 则出现了“QQ 尾巴”等病毒。日益爆发的病毒和黑客攻击表

明，即时通信软件的安全措施还未跟上时代的发展。

电子前沿基金会与 ProPublica、普林斯顿大学信息技术中心合作，推出“通讯软件安全性记分卡”项目，为几十个最流行的即时通信应用程序进行安全性打分，包括 Skype、QQ 等等。安全性打分基于 7 类得分，包括：安全性规范及文档；代码的安全性（即通过第三方审查）；密钥泄露是否会导致用户历史信息遭泄密；是否加密传输消息；短信或通话是否泄露联系人信息；服务提供商不能读取用户消息等七类。表现良好的是有加密通信应用有 Cryptocat 等。苹果短信应用得到了 5 分，而脸书聊天、Skype 等打分为 2 分左右。QQ 得分也不太理想。

网络专家认为，如今即时通信软件的信息安全受到三方面威胁：1、用户密码被窃取；2、计算机中木马，聊天记录被窃取；3、实时聊天信息被嗅探窃取。在腾讯 QQ 使用中，两个用户甲、乙之间的通信，服务器会给甲和乙分发一个密钥，甲和乙之间发送消息都使用这个密钥进行加密，这个密钥只有甲乙知道，所有，他们之间的通信内容也只有甲、乙能够获得。其他人即使监听到了甲、乙之间发送的消息，也只能获取到加密的乱码，无法知道具体聊天内容。根据以上分析，腾讯 QQ 对消息进行加密使用的是对称密钥，而且对密钥是进行临时分配，也提高了即时 QQ 软件的安全性能。但是，如果密码被黑客获取，则 QQ 用户在聊天时发送的信息内容也会受到破译，对水平较高的黑客来说，依然能够获得聊天的内容。

即时通信软件的泄密事件也不断出现。2013 年，国内知名安全漏洞监测平台乌云公布称，腾讯 QQ 群关系数据遭泄露，泄露数据达 7000 多万个，涉及 12 亿个部分重复的 QQ 号。可以说，即时通信软件成为黑客攻击对象具有必然性。同时，即时通信技术特性也导致其在安全性方面具有先天的弱点。即时通信的主要特点是通过 P2P 进行数据交换，两台终端设备的直接交换信息，也容易使病毒更加便捷的传播[4]。缺少服务器的中转和过滤，也使得网络监管对数据交换的监控难度在增加，造成了黑客攻击和病毒传播的范围和速度大大增加。

即时通信软件受到攻击造成的主要影响有，作为通信软件，即时通信普遍存在安全漏洞，在信息技术发展和使用范围扩大的情况下，攻击即时通信软件的利益驱动使得黑客攻击和针对有关软件的病毒影响危险性增大，给用户和使用单位造成不同程度的损失，轻则隐私泄露，重则系统瘫痪。即时通信的信息传播方式