编号：_____

桂林电子科技大学
GUILIN UNIVERSITY OF ELECTRONIC TECHNOLOGY

毕业设计(论文)开题报告

题　　目：文件加解密安全管理系统

学　　院：计算机与信息安全学院

专　　业：信息安全

学生姓名：王光汉

学　　号：1300340125

指导教师单位：计算机与信息安全学院

姓　　名：姚罡

职　　称：

题目类型： ☐理论研究 ☐实验研究 ☐工程设计 ☐工程技术研究 ☑软件开发

2017 年 9 月 18 日

开题报告填写要求

1．开题报告作为毕业设计（论文）答辩委员会对学生答辩资格审查的依据材料之一。此报告应在指导教师指导下，由学生在毕业设计（论文）工作前期内完成，经指导教师签署意见审查后生效。

2．开题报告内容必须用黑墨水笔工整书写，或按教务处统一设计的电子文档标准格式打印，禁止打印在其它纸上后剪贴，完成后应及时交给指导教师签署意见。

3．学生查阅资料的参考文献应在 5 篇及以上（不包括辞典、手册），开题报告的字数要在 1000 字以上。

4．有关年月日等日期的填写，应当按照国标 GB/T 7408—94《数据元和交换格式、信息交换、日期和时间表示法》规定的要求，一律用阿拉伯数字书写。如“2010 年 9 月 20 日”或“2010-09-20”。

1．毕业设计的主要内容、重点和难点等

主要内容：

基于 AES 与 RSA 加解密算法融合的文件加解密。加密时用 RSA 公钥加密 AES 秘钥，用 AES 算法加密文件数据。解密时使用私钥解密 AES 秘钥，再通过 AES 秘钥与 AES 解密算法解密数据。从而解决 RSA 明文长度限制于加解密效率问题以及秘钥交换问题。

本系统要实现的主要功能包括 3 个方面，各个模块的功能说明如下：

1、文件加密模块

2、文件解密模块

3、用户私钥对生成模块

重点：

加解密算法协议设计与加密生成文件格式设计

难点：

多线程加解密。

2．准备情况（查阅过的文献资料及调研情况、现有设备、实验条件等）

查阅文献:

[1]罗云锋,熊伟,许庆光. 一种基于属性加密的数据保护与访问控制模型[J]. 网络安全技术与应用,2017,(09):53-56. [2017-09-18].

[2]杨迪,叶鹏,方镇林. 透明加解密在电子文件可信保管中的应用[J]. 电子科学技术,2017,04(04):147-150. [2017-09-18]. DOI：10.16453/j.issn.2095-8595.2017.04.033

[3]李春杰,史正乐,高慧敏,颜智润. 移动智能终端的个人隐私保护系统的开发设计[J]. 计算机应用与软件,2017,34(06):217-220+256. [2017-09-18].

[4]赵萍. 保护文件传输中 DES 加密算法在数据安全中的应用[J]. 黑龙江科技信息,2017,(14):176. [2017-09-18].

[5]程旋,何成万. PDF 中隐私数据的保护方法[J/OL]. 软件导刊,2017,16(04):194-196. (2017-04-28)[2017-09-18]. http://kns.cnki.net/kcms/detail/42.1671.TP.20170428.1629.122.html

[6]孙晓红,曾昭虎,聂旭. 文档安全技术在油田知识管理系统中的应用[J]. 信息系统工程,2017,(04):66. [2017-09-18].

[7]余彩霞,姚晔. 基于多级安全加密的电子文件流转中的访问控制研究[J]. 档案学通讯,2017,(02):58-63. [2017-09-18]. DOI：10.16113/j.cnki.daxtx.2017.02.014

[8]张通明,关建峰. 面向文本的标识分组加解密模式[J]. 网络与信息安全学报,2017,3(03):43-50. [2017-09-18].
[9]武旭方,胡晓勤. 一种信息防泄密系统的设计与实现[J]. 现代计算机(专业版),2017,(07):72-74. [2017-09-18].
[10]李进豪. 基于多语言的实用简易加解密算法的研究与实践[J]. 现代计算机(专业版),2017,(04):48-52. [2017-09-18].

调研情况:

通过调研，我们发现传统的使用文件加解密系统中存在以下问题：

（1）文件加密传输需要事先共享秘钥（AES）；

（2）文件加解密效率低加密位长有限（RSA）；

（3）不利于在网络上进行文件安全传输。

现有设备:

1、计算机：Intel® Core™ II×2 245 i3-3217U CPU:1.8GHz RAM:6GB。

2、操作系统：Linux mint 17.03

3、软件：Qt creator5.9, Openssl-dev 1.0.2。

实验条件：

具备软、硬件开发平台及测试条件。

3、实施方案、进度实施计划及预期提交的毕业设计资料

实施方案：

1、查找资料，查阅文献，熟悉开发工具，学习 Qt creator 的使用以及 Qt API、Openssl API 的使用；

2、完成需求分析和可行性分析；

3、加密文件格式设计，完成系统概要设计与详细设计；

4、编码及测试；

5、撰写毕业设计论文。

进度实施计划：

第 1 周：查阅相关资料,编写开题报告；

第 2～3 周：确定技术方案，翻译英文资料；

第 4～6 周：完成系统的基本框架，实现基本功能；

第 7～10 周：完善界面，丰富系统功能；

第 11～14 周：完善系统设计，撰写毕业设计论文；

第 15～16 周：毕业设计答辩。

预期提交的毕业设计资料：

1、毕业设计开题报告一份；

2、英文翻译材料一份（包括不少于 4 万字符的英文原文和译文）；

3、毕业论文一份（二万汉字以上，附中英文摘要，其中英文摘要 300~500 单词）；

4、本系统软件及源程序清单一套。

指导教师意见

指导教师（签字）： 2015 年 1 月 16 日
开题小组意见
开题小组组长（签字）： 2015 年 1 月 19 日
院（系、部）意见
主管院长（系、部主任）签字： 2015 年 1 月 20 日