SJ0606-2016 版

成都信息工程大學
Chengdu University of Information Technology

# 教学实习报告

实习单位：成都信息工程大学

实习时间：2024.5.4 至 2024.6.4

学　　院：网络空间安全学院

专　　业：信息安全

学生姓名：杨佳倪 学号：2022132006

2024 年 06 月 04 日

成都信息工程大学 教务处制

一、实习目的

RSA 算法是应用最广泛的公钥密码算法。

1977 年，RSA 算法由 MIT 的罗纳德 • 李维斯特（Ron Rivest）、阿迪 • 萨莫尔（Adi Shamir）和伦纳德 • 阿德曼（Leonard Adleman）共同设计，于 1978 年正式发布，以他们三人的首字母命名。

在这之前所用的对称加密方式只采用一个密钥，知道加密密钥就可以知道解密密钥。但是由于双方需要事先约定加密的规则，就导致没有办法安全地交换密钥，建立安全的传递通道。

但是 1976 年出现的非对称加密算法的思想就可以解决密钥的交换和存放问题。它使用两个密钥，一个用来加密消息和验证签名，叫公钥，另一个用来解密，叫私钥，加解密双方是不平等的。这种新的构思是由美国计算机科学家 Whitfield Diffie 和 Martin Hellman 提出的，被称为 Diffie-Hellman 密钥交换算法，RSA 算法就是受到它的启发产生的，是这种构思的具体实现方式，既可以用来加密，解密，也可以用于密钥交换。

通过本次实习，需要学习如何调用 openssl 库等相关的编程知识，深入认识到函数和多文件编程逻辑的重要性，对编程思想进行体会，养成良好的编程习惯。使用 C 语言开发出一个对大文件的 RSA 加解密系统，锻炼自己的编程能力，并且能满足用户对数据的高效、准确、便捷的加解密要求。

通过老师的指导，我的文档撰写能力得到很好的提升，能够对文字、图片实现更好的排版，符合格式要求；条理清晰，能够将自己的想法和编程逻辑通过文字传达出来。在系统设计期间，学习到课堂上没有的知识，积累实践经验，增强动手能力和解决实际问题的能力。

二、实习单位及岗位介绍

实习单位：成都信息工程大学

岗位介绍：软件开发工程师是一种专业技术岗位，负责设计、编码、测试和维护软件应用程序和系统。他们是现代科技行业中至关重要的角色之一，通过技术和创新为用户提供高质量的软件解决方案。

作为软件开发工程师，主要职责包括以下几个方面：

1） 软件需求分析和设计：与客户或团队成员合作，理解并分析软件需求，确定系统的功能和特性。根据需求，设计软件系统的架构、模块和数据库结构，确保满足用户需求和系统的可扩展性。

2） 编码和开发：利用编程语言和开发工具，将设计转化为具体的代码。编写高质量、可维护的代码，实现软件的各项功能和特性。

3）软件测试与调试：编写测试计划和测试用例，执行各类测试，包括单元测试、集成测试和系统测试，以验证软件的正确性和稳定性。

4） 版本控制和文档编写：使用版本控制工具管理软件的源代码，确保团队成员间的协作和代码的可追溯性。

5） 持续学习和技术更新：软件开发工程师需要持续学习和掌握最新的技术和工具，跟随行业的发展趋势。了解新技术和编程语言，掌握前沿的开发框架和平台，不断提升自己的技术水平和解决问题的能力。

三、实习内容及过程

1.选题为基于 RSA 算法的文件加密和解密工具

2.需求

完成一个基于 RSA 算法的文件加密和解密工具功能要求：

1）实现 RSA 公钥和私钥产生。要求私钥的长度至少 1024 比特。

2）用 RSA 公钥对中英文文件加密

3）用 RSA 私钥对中英文文件解密

算法实现要求：
（1） 可自行编写 RSA 算法，也可以调用编译器或者加密包自带接口完成算法 RSA 算法。
（2） RSA 算法私钥长度和模数 n 至少 1024 比特长度，即要求实现大数计算（建议可直接调用编译器大数库实现）
（3） 编程语言不限，可选择 C、C++、Java、Python 等任意一种编程语言实现

3.总体设计

针对以上要求，应该设计一个实现基于 RSA 算法的文件加密和解密工具，该系统提供对中英文文件加解密的功能，达到大数的计算需求通过外部导入大数库 openssl，保证系统的实现。

4. 编程实践

在编程的过程中，感受到了数据结构和编程逻辑的重要性，有了结构才能将好的思想付诸实践。同时经过查询资料了解到栈的一些运用方法，比如栈的顺序存储结构,栈是计算表达式的经典应用。对用户注册登录系统的编程实现也是出于对系统安全性的考量，保障了数据的相对安全。

5.文档撰写

通过老师的指导，我的文档撰写能力得到很好的提升，能够对文字、图片实现更好的排版，符合格式要求；条理清晰，能够将自己的想法和编程逻辑通过文字传达出来。

四、实习总结及体会

工具设计期间，学习到很多课堂上没有的知识，还积累了很多实践经验，增强了动手能力和解决实际问题的能力。在此之前，对于 C 编程技术或是其他的编程知识都只是略知皮毛，尽管编了些程序，但都是功能较小、容易实现的设计，对知识没有深入了解。在短短的几个月时间里，作者认真学习了 C 语言调用 openssl 库实现 RSA 加解密等相关的编程知识，初步认识到函数和编程逻辑的重要性，对编程思想有了进一步的体会，养成了一些良好的编程习惯。系统虽然完成，但是距离优秀仍存在一定差距，用 C 编程设计系统也需要继续学习。希望自己能不断学习和实践，争取以后做得更好。