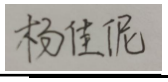
成 都 信 息 工 程 大 学
工 程 实 践 报 告

题目： 基于 RSA 算法的文件加密和解密工具

姓　　名：	杨佳倪
班　　级：	信息安全实验 221 班
学　　号：	2022132006
指导教师：	万武南
日　　期：	2024 年 6 月 4 日

作者签名： 

计算器系统的设计与实现

摘　要

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。

本设计从用户的需求出发，开发出来的一个操作简单、方便实用的 RSA 文件加解密工具。本文首先介绍 RSA 文件加解密工具的开发背景，并对加解密工具进行了较详细的需求分析；然后重点讨论该工具的设计与实现，包括总体设计，结构设计和功能模块详细设计；最后，通过测试与分析，说明该工具运行稳定、可靠，具有一定的实用价值。

关键词：RSA 文件加解密工具；openssl 库；多文件

目 录

1 引言 3
1.1 课题背景 3
1.2 本课题的研究作用 3
1.3 本文的主要工作 4
2 用户需求分析 4
2.1 系统目标 4
2.2 系统功能 4
2.3 开发环境及工具 4
2.3.1 运行环境及开发工具 4
2.3.2 底层实现技术介绍 4
3 结构设计 6
3.1 总体设计及介绍 6
3.2 系统功能模块及设计 6
3.2.1 详细结构设计 6
3.2.2 功能模块介绍 8
4 系统详细设计与实现 9
4.1 RSA 加解密算法设计与实现 ..... ……10
4.2 BASE64 编码解码设计与实现 ..... …..11
5 系统测试与分析 ..... ……..11
5.1 测试 ..... ……11
5.2 调试过程中遇到的主要问题 ..... …..12
结 论 13
参考文献 13

1 引言

1.1 课题背景

21 世纪，随着社会经济的迅速发展和科学技术的全面进步，人类社会已进入信息和网络时代。RSA 加解密在多方面有应用：1）信息安全是 RSA 加解密背景中的核心议题之一。RSA 算法是保护数据机密性和完整性的重要工具之一。研究人员和安全专家致力于改进 RSA 算法的安全性，发现潜在的漏洞并提出对策以应对各种攻击。2）网络通信：随着互联网的普及和网络通信的增加，RSA 加解密在网络安全中的应用愈加重要。在网页浏览、电子邮件传输、即时通讯等场景中，RSA 被用于加密通信内容，以确保数据在传输过程中的保密性。3）数字签名：RSA 不仅可以用于加密通信，还可以用于生成和验证数字签名。数字签名是数字证书的核心组成部分，用于验证数据的来源和完整性，广泛应用于电子商务、电子政务等领域。4）密钥管理：RSA 也用于密钥管理，包括密钥生成、交换和存储。在密钥交换过程中，RSA 能够安全地协商对称密钥，从而实现安全的通信。5）密码学研究：RSA 算法本身是密码学研究的重要内容之一。研究人员致力于分析 RSA 算法的数学基础，改进其性能和安全性，并探索基于 RSA 的新型密码学方案。

总的来说，RSA 加解密的课题背景涵盖了信息安全、网络通信、数字签名、密钥管理、密码学研究等多个领域，是当前信息安全领域中的重要议题之一。

1.2 本课题的研究作用

1.3.1

利用 RSA 算法是实现对文件的加解密工具。研究基于 RSA 算法文件加解密工具可以帮助实现信息传输的保密性，保证其在各种场景下都能够安全、可靠地完成加密传输任务。

1.3.2

应用到其他领域：研究 RSA 算法文件加解密工具可以应用到其他领域，进而推动其他领域的发展和进步。此外，研究 RSA 算法文件加解密工具还能推动 RSA 算法文件加解密工具的发展。研究 RSA 算法文件加解密工具可以推动计算器系统技术的发展和创新，从而不断完善和升级 RSA 算法文件加解密工具，以满足不断变化的加密需求。

1.3 本文的主要工作

基于用户对计算器系统的需求，通过一定时间的编码实现了该计算器系统所应有的功能。本文首先介绍计算器系统的开发背景，并对计算器系统进行了较详细的需求分析；然后重点讨论该系统的设计与实现，包括总体设计，系统功能设计和功能模块详细设计；最后，通过测试与分析，说明该系统运行稳定、可靠，具有一定的实用价值。

2 需求分析

2.1 系统目标

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

2.2 系统功能

系统功能主要是在加密前，读取文件内容并在屏幕打印出来；加密后，把密文内容在屏幕上打印出来。基于系统的安全性要求，实现了基于 RSA 算法的文件加密和解密工具，更好的保证用户数据的隐私性，使系统更加安全可靠。

2.3 开发环境及工具

2.3.1 运行环境及开发工具

运行环境：

（1）、Windows10 系统

（2）、vs2019 编译环境；

开发工具：C 语言；

2.3.2 底层实现技术介绍

（1）RSA 加解密

RSA 公钥算法由 Rivest、Shamir、Adleman 于 1978 年提出的，是目前公钥密码的国际标准。算法的数学基础是 Euler 定理，是基于 Deffie-Hellman 的单项陷门函数的定义而给出的第一个公钥密码的实际实现，其安全性建立在大整数因子分解的困难性之上。

RSA 算法的明文空间 M=密文空间 C=Zn 整数

1. 生成密钥

•秘钥产生算法Gen：

1）独立地选取两个大素数p_1和p_2。(各512bit的数)

2）计算$n=p_1\times p_2$，其欧拉函数值$\varphi(n)=(p_1-1)(p_2-1)$。

3）随机选一整数e，$1\le e<\varphi(n)$且gcd($\varphi(n)$, e)=1。(因而在模$\varphi(n)$下e有逆元)

4）计算$d=e^{-1} \bmod \varphi(n)$。

5）公钥为{e,n}，私钥为{d,n}。

(p_1, p_2不再需要，可以销毁)

8

2. 加密算法

•加密算法Enc：已知公钥{e,n}与明文M，计算密文

$C = M^e \bmod n$。

3. 解密算法

•解密算法Dec：已知私钥{d,n}与密文C，计算明文

$M = C^d \bmod n$

图 1-RSA 加解密原理

（2）生成一个 RSA 公钥/私钥对：

1）随计选择两个不相等的质数 p，q

2）计算它们的乘积 N=p*q

3）计算欧拉函数 Φ(N)=(p-1)(q-1)，N 的二进制长度作为密钥的长度，

4）随机选择一个加密密钥 e,这里 1<e<Φ(N),gcd(e, Φ(N))=1

5）根据以下公式求解得到解密密钥 d

6） mod Φ(N)，0≤d≤N

7）发布加密密钥：(e,N)

8）保密解密密钥：(d,N)

（3）base64 编码

加密后的数据通常是 二进制数据 ，如果直接将这些数据在网络中传输，那

么在传输过程中如果需要进行调试或者查看这些数据的时候，就会很不方便，因为二进制数据对人类来说是不可读的。而 Base64 编码可以将二进制数据转化为可读的 ASCII 字符集，这样就能在网络中方便地传输和查看了

3 系统总体结构设计

3.1 基本简介

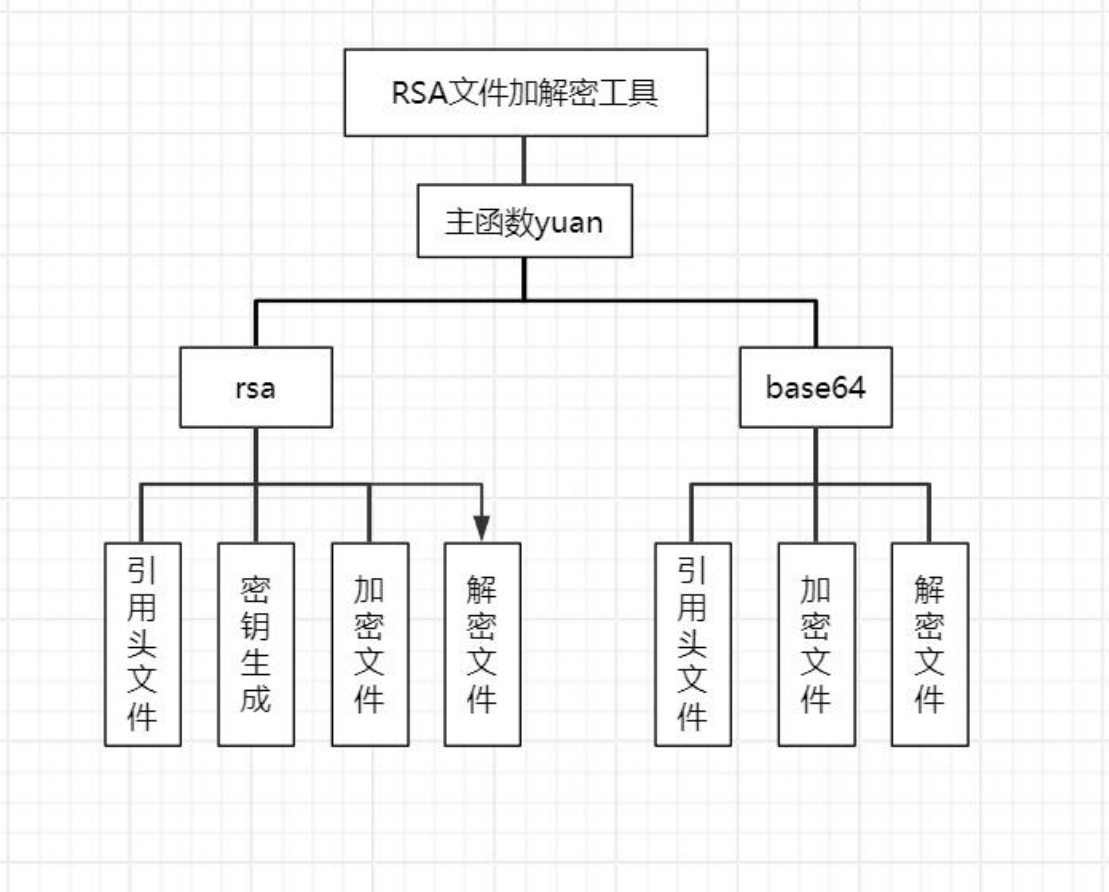


图 2-系统结构框图

3.2 系统功能模块及设计

3.2.1 详细结构设计

本题设计的核心是对 openssl 库的 调用，即如何调用 openssl 钟的 RSA 算法实现大文件加解密，具体实现方法如下：

甲方生成一对密钥并将其中的一把作为公钥向其它方公开,得到该公钥的乙方使用该密钥对机密信息进行加密后再发送给甲方，甲方再用自己保存的另一把 私钥 对加密后的信息进行解密。

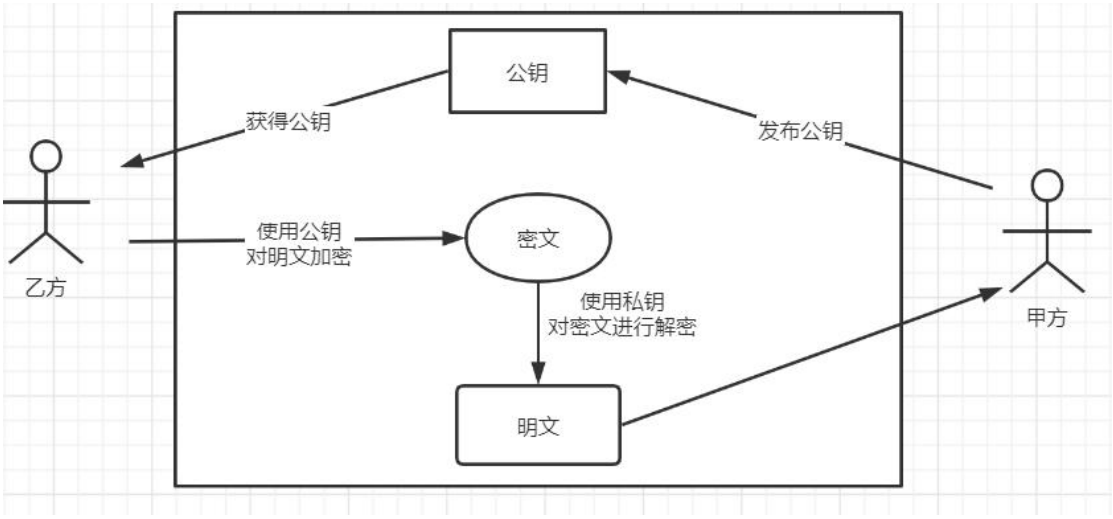


图 3-RSA 加解密流程示意图

RSA 加密算法的基本流程：

1）密钥

1.选择两个大素数：首先，选择两个足够大的素数 p 和 q。

2.计算模数 N：计算两个素数的乘积，即 N = p * q。

3.计算欧拉函数值：计算欧拉函数 φ(N) = (p-1) * (q-1)。

4.选择公钥指数 e：选择一个与 φ(N) 互质的整数 e，通常选择一个小的质数

5.计算私钥指数 d：计算 e 关于 φ(N) 的模反元素，即找到整数 d，使得 (e * d) mod φ(N) = 1。

6.生成密钥对：最终生成 RSA 密钥对，公钥为 (N, e)，私钥为 (N, d)。

2）加密

1.获取公钥：接收者将其公钥 (n, e) 分发给通信的发送者。

2.选择消息：发送者选择要发送的消息 M，确保消息的大小不超过模数 N。

3.加密消息：发送者使用接收者的公钥 (N, e) 中的公钥指数 e，将消息 M 加密为密文 C。

3）解密

1.获取私钥：接收者使用自己的私钥 (N, d) 来解密收到的密文。

2.解密密文：接收者使用私钥指数 d 对收到的密文 C 进行解密，恢复原始消息 M。

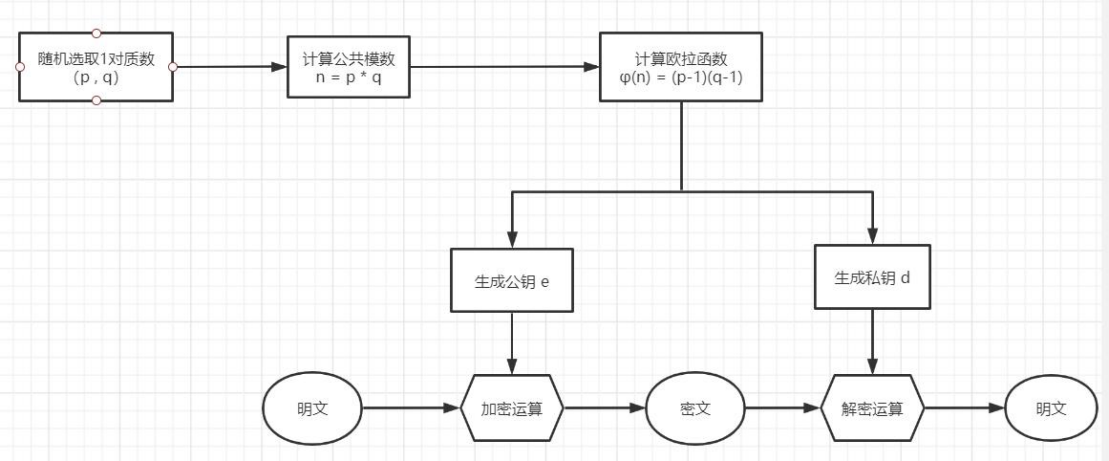


图 4-RSA 加解密详细流程

3.2.2 功能模块介绍

实现系统功能的关键主要是：用户输入的数据和运算符如何巧妙地分离和有机的结合，本系统在对输入的计算表达式进行输入判断之后，将所得算式分解，计算则用 if 分支语句分别实现了四则运算和三角反三角函数这两大功能。

功能编号	功能	备注
1	输入文件	显示文件内容
2	Base64 编码解码	相应二进制编码并且打印输出
3	打印加密后的文件内容	中/英文

表 1-功能实现框图

4　工具详细设计与实现

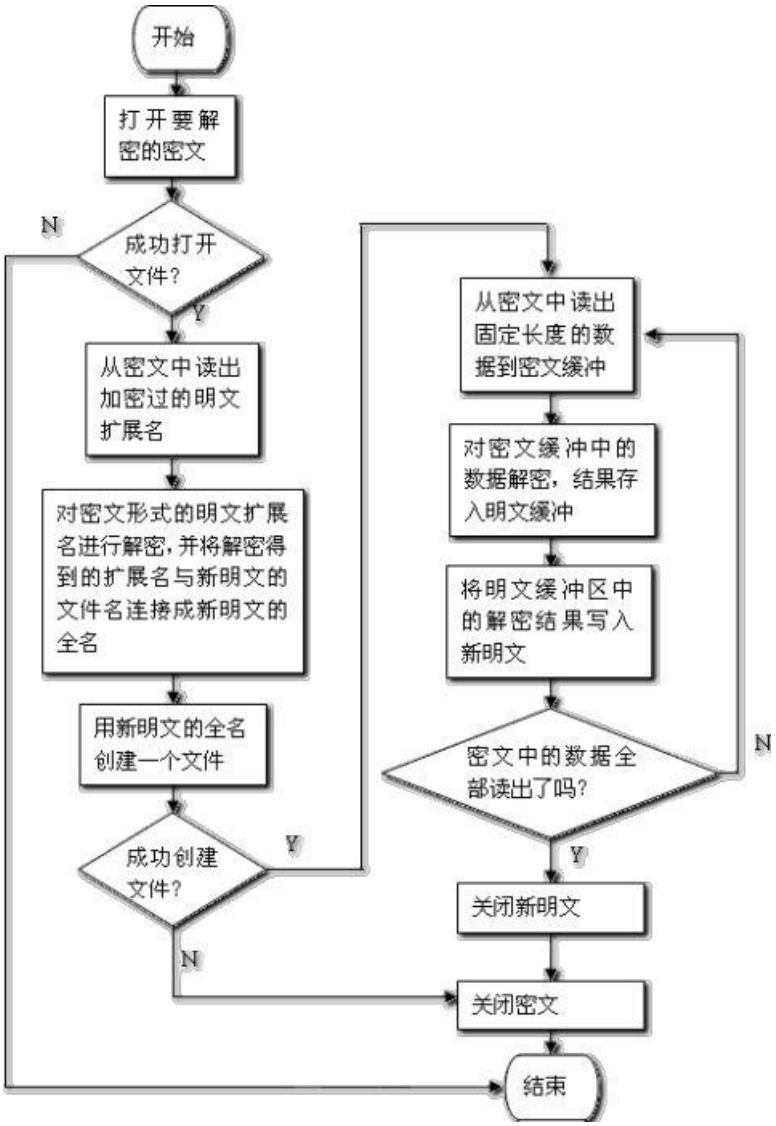
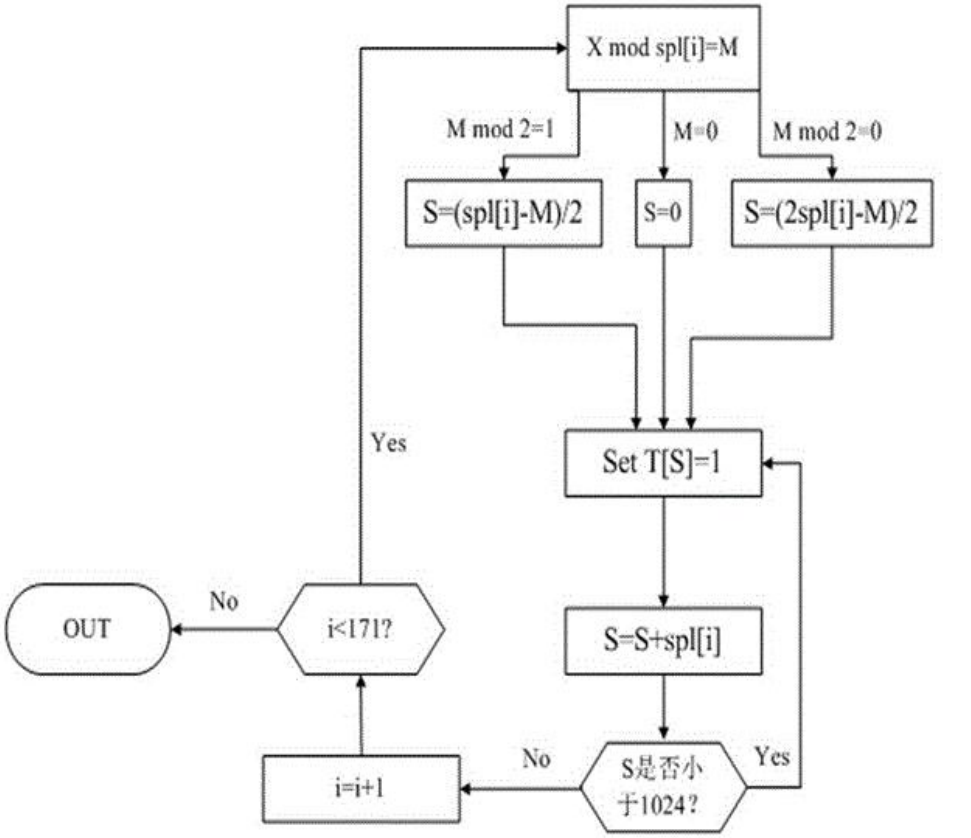
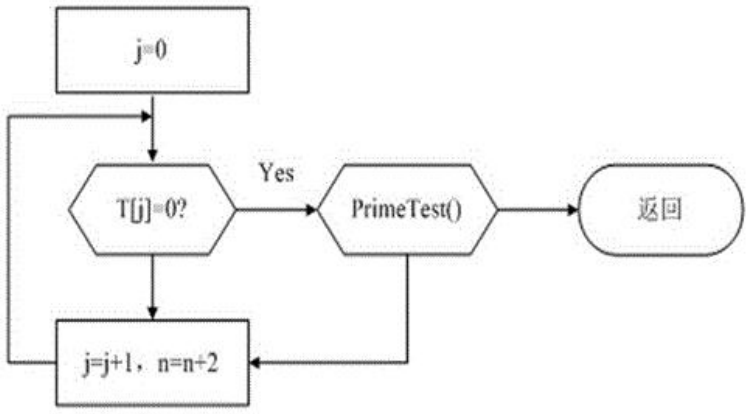


图 5-程序设计思路流程图

4.1 RSA 加解密算法设计与实现

1）密钥生成的快速算法





(1)X是一个1024位的随机数；
(2)spl是从3开始的小素数集；
（3）T[j]是标识数组，T[j]=1标示锁存数组不是素数；

图 6-RSA 密钥生成算法

4.2 base64 编码解码设计与实现

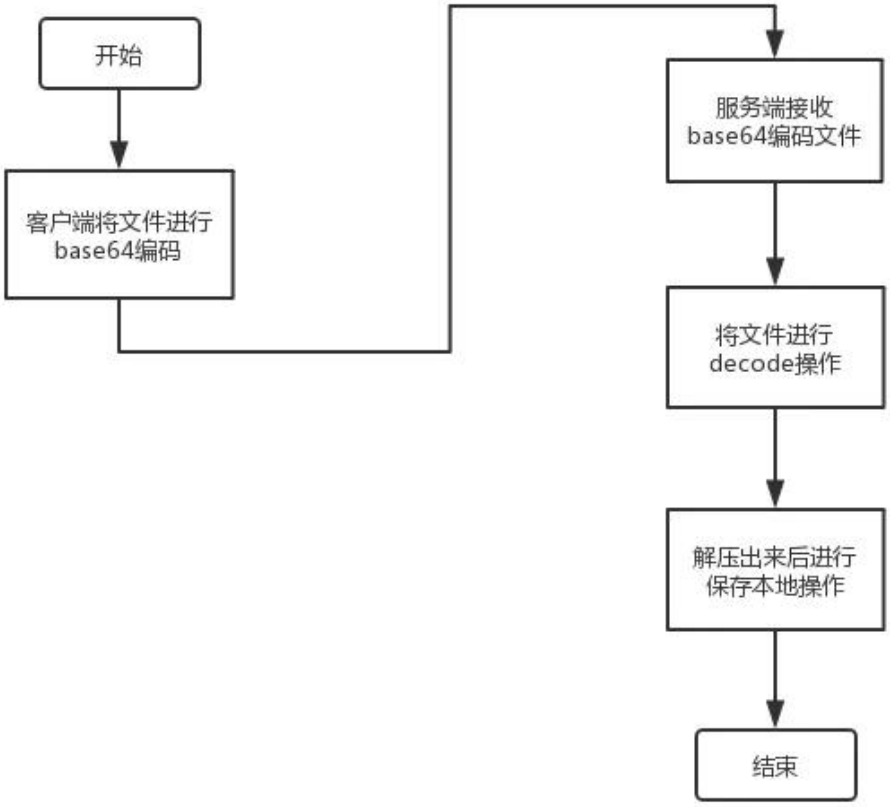


图 7-base64 加解密过程

5 工具测试与分析

5.1 测试

1、密钥生成调用 openssl 库中的命令

下面是示例代码

openssl genrsa -out C:\Users\annie\Desktop\testkey.txt 1024

生成一个 1024 位的 RSA 私钥，并将其保存到 C:\Users\annie\Desktop\testkey.txt 中

openssl rsa -in C:\Users\annie\Desktop\testkey.txt -pubout -out C:\Users\annie\Desktop\testpubkey.txt

取 RSA 私钥，并提取其对应的公钥，保存到 C:\Users\annie\Desktop\testpubkey.txt

openssl rsautl -encrypt -in hello.txt -inkey testpubkey.txt -pubin -out helloen.txt

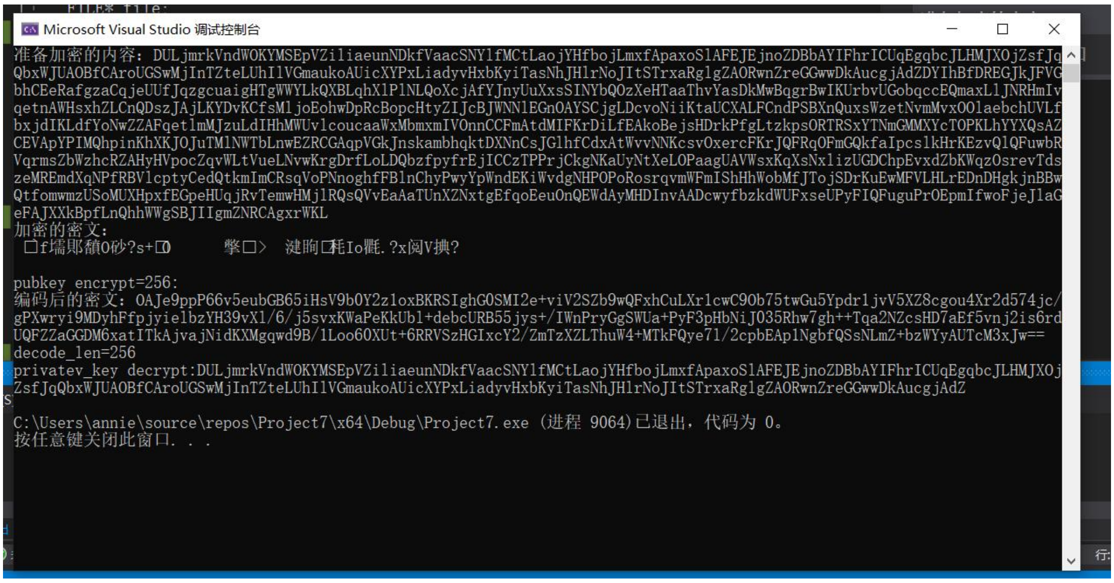
使用 testpubkey.txt 中的公钥对 hello.txt 文件进行 RSA 加密，并将加密后的结果保存到 helloen.txt。

openssl rsautl -decrypt -in helloen.txt -inkey testkey.txt -out hellode.txt

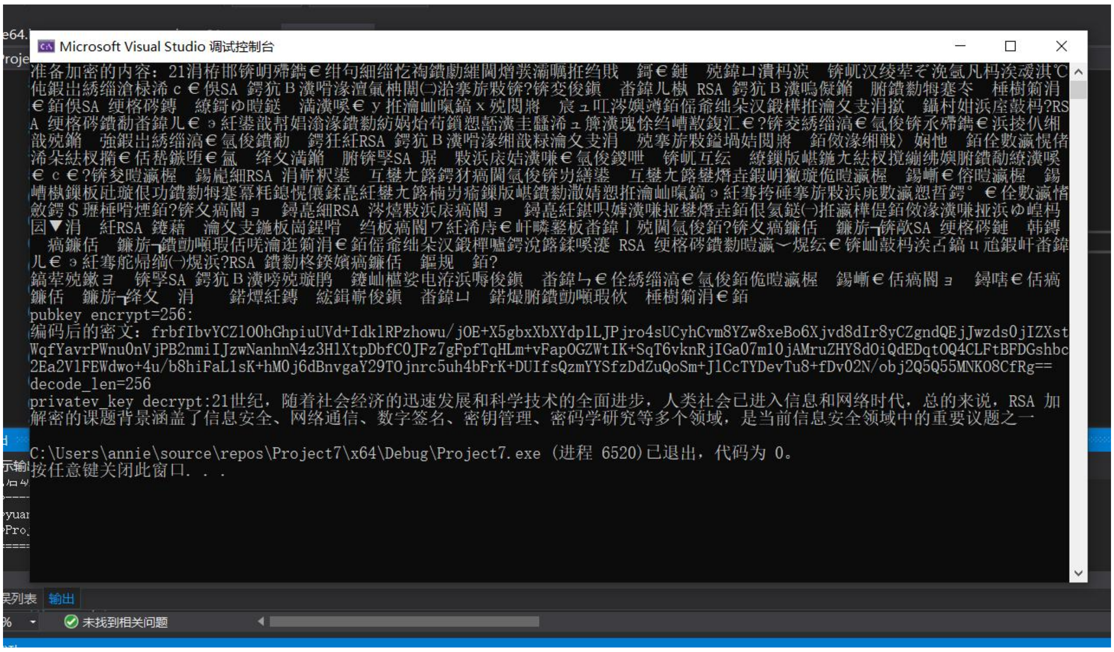
使用 testkey.txt 中的私钥对 helloen.txt 文件中的 RSA 加密数据进行解密，并将解密后的原始内容保存到 hellode.txt。

2、测试结果：

（1）英文文件加解密



2）中文



5.2 调试过程中遇到的主要问题

Openssl 库已经升级到 3.0 以上的版本，调试会出现问题，不支持 RSA 加解密的函数，此时应该用 1.0 以下的一个版本。

结　论

本设计经过近 1 个多月的努力，系统基本满足 RSA 对大文件加解密方面的需要。完成后的工具实现了对中英文文件加解密等功能。用户能够非常方便地输入文件得到需要的结果。

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，作者认真学习了数组，栈，函数等相关的编程知识，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。

限于作者知识水平和经验有限，此系统还有许多有待完善和改正的地方，恳请各位老师和读者批评指正。

参考文献

[1] 蔺冰．王力洪.C 语言程序设计[M]．陕西：西安电子科技大学出版社，2016。

[2] 严蔚敏，李冬梅，吴伟民．数据结构（C 语言版第二版）[M]．北京：人民邮电出版社，2022。

[3] 李飞，吴春旺，王敏．信息安全理论与技术[M]．2021 年 12 月第 2 版．西安电子科技大学出版社，2021.

[4]张仕斌，万武南，张金全．应用密码学[M]．2017 年 1 月第 1 版．西安电子科技大学出版社，2017.