***2023***



**网络空间安全概论 结题报告**

|  |  |
| --- | --- |
| 题 目： | Rsa和维吉尼亚加密算法实现 |
| 专 业： | 计算机科学与技术 |
| 班 级： | BSB2101 |
| 学 号： | U202115666 |
| 姓 名： | 刘文博 |
| 指导教师： | 郝义学 |
| 邮 件： | [3097365481@qq.com](mailto:3097365481@qq.com) |

目 录

[1 引言 2](#_Toc169466663)

[1.1 研究背景 2](#_Toc169466664)

[1.2 研究问题与应用前景 2](#_Toc169466665)

[2 RSA加密算法&维吉尼亚加密算法 3](#_Toc169466666)

[2.1 RSA加密算法原理 3](#_Toc169466667)

[2.2 维吉尼亚加密算法原理 4](#_Toc169466668)

[3 RSA和维吉尼亚加密算法设计与实现 6](#_Toc169466669)

[3.1 RSA加密算法设计 6](#_Toc169466670)

[3.2 维吉尼亚加密算法设计 7](#_Toc169466671)

[4 对抗样本攻击算法总结与心得 9](#_Toc169466672)

[4.1 对抗样本攻击算法总结 9](#_Toc169466673)

[4.2 对抗样本攻击算法心得 9](#_Toc169466674)

[参考文献 10](#_Toc169466675)

# 引言

## 研究背景

在现代社会，信息的安全性至关重要。无论是个人隐私、金融交易还是国家机密，都需要得到保护。RSA（Rivest-Shamir-Adleman）加密算法是现代公钥密码学的基石之一，由Ron Rivest、Adi Shamir和Leonard Adleman在1977年提出。RSA加密算法等密码学技术能够确保信息在传输和存储过程中不被未经授权的人窃取或篡改，同时具有数字签名、非对称等特点。

## 研究问题与应用前景

密码学的研究目前面临许多挑战，以下是一些主要问题:

* 量子计算机可以高效地破解许多当前使用的加密算法，如RSA和ECC（椭圆曲线加密）。为此未来应研究后量子密码学，开发对量子计算机攻击具有抗性的加密算法。
* 强加密算法通常计算复杂度高，可能导致性能瓶颈，尤其是在资源受限的环境中（如物联网设备）。为此应不断开发高效的加密算法和优化现有算法，确保在保证安全性的前提下提高性能。
* 安全地生成、分发、存储和撤销密钥是一个复杂的问题，尤其是在大规模分布式系统中。为此需要研究和实现健壮的密钥管理系统，采用硬件安全模块（HSM）和密钥托管服务等技术。

# RSA加密算法&维吉尼亚加密算法

## RSA加密算法原理

RSA算法的数学基础是：

* 大整数分解问题：RSA的安全性基于大整数分解的计算复杂性。具体来说，给定两个大质数的乘积，要找到这两个质数是非常困难的。
* 模幂运算：RSA加密和解密过程依赖于模幂运算（模n的幂次运算），这是一个单向函数，易于计算但难以反向操作。

其算法流程一般是：

**1.** 密钥生成：

1. 选择两个大质数 p 和 q。
2. 计算 n ( n = p \* q)
3. 计算 ϕ(n)（即 n 的欧拉函数 ϕ(n) = (p – 1) \* (q – 1)）
4. 选择公钥指数 e（满足 1<e<ϕ(n) 且 e 与 ϕ(n) 互质）
5. 计算私钥指数d（d \* e 模 ϕ(n) 同余1）
6. 生成密钥对（公钥：（e, n） 私钥：（d, n））

2. 加密: 将明文M转化为整数m，应用公式c ≡ m ^ e (mod n) 得到密文c

3. 解密：接受密文c，应用公式m ≡ c ^ d (mod n) 得到整数m，再转化为明文M

算法的总体原理图如图 2‑1所示。

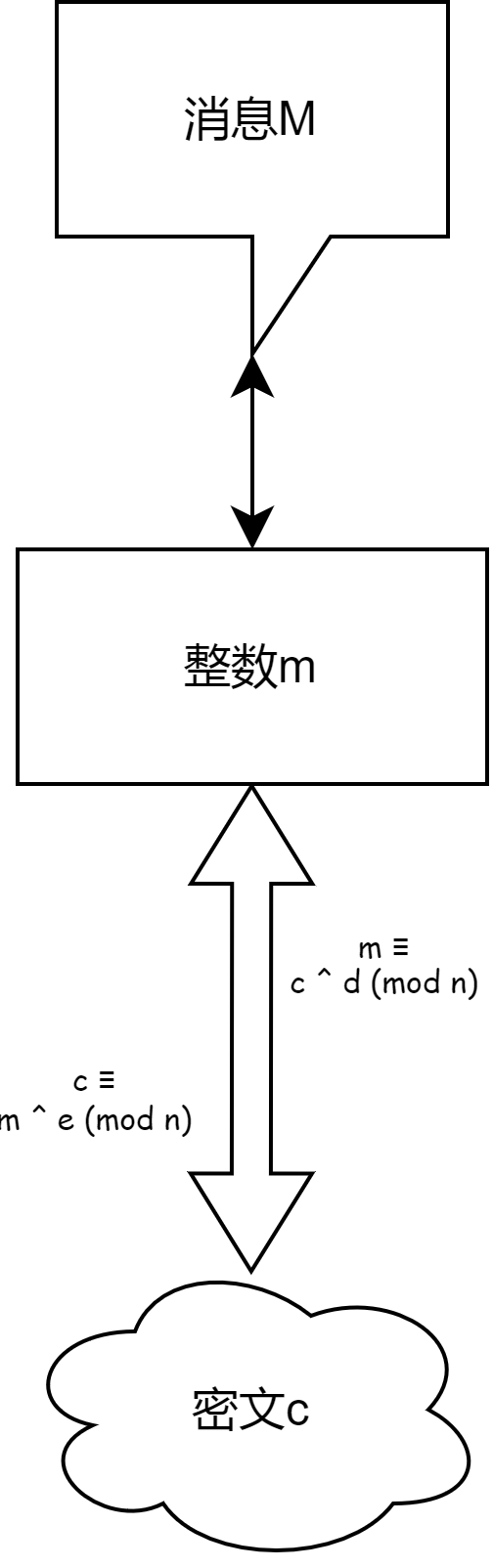


图 2‑1 rsa加密总体原理图

Rsa算法的安全性依赖与大整数分解的困难性和模幂运算的数学性质。如果攻击者不能快速进行大整数分解或者模幂运算，则将很难破解Rsa加密。

## 维吉尼亚加密算法原理

维吉尼亚密码是一种古典的多字母替换密码，利用了字母表中字母之间的周期性特征，使用一个重复的关键字或短语来对明文进行加密。

相较于凯撒密码，维吉尼亚密码将密钥按照明文的长度进行重复，直到覆盖整个明文。如果密钥长度不够，可以循环使用。

维吉尼亚密码的算法原理图如图 2‑2所示：

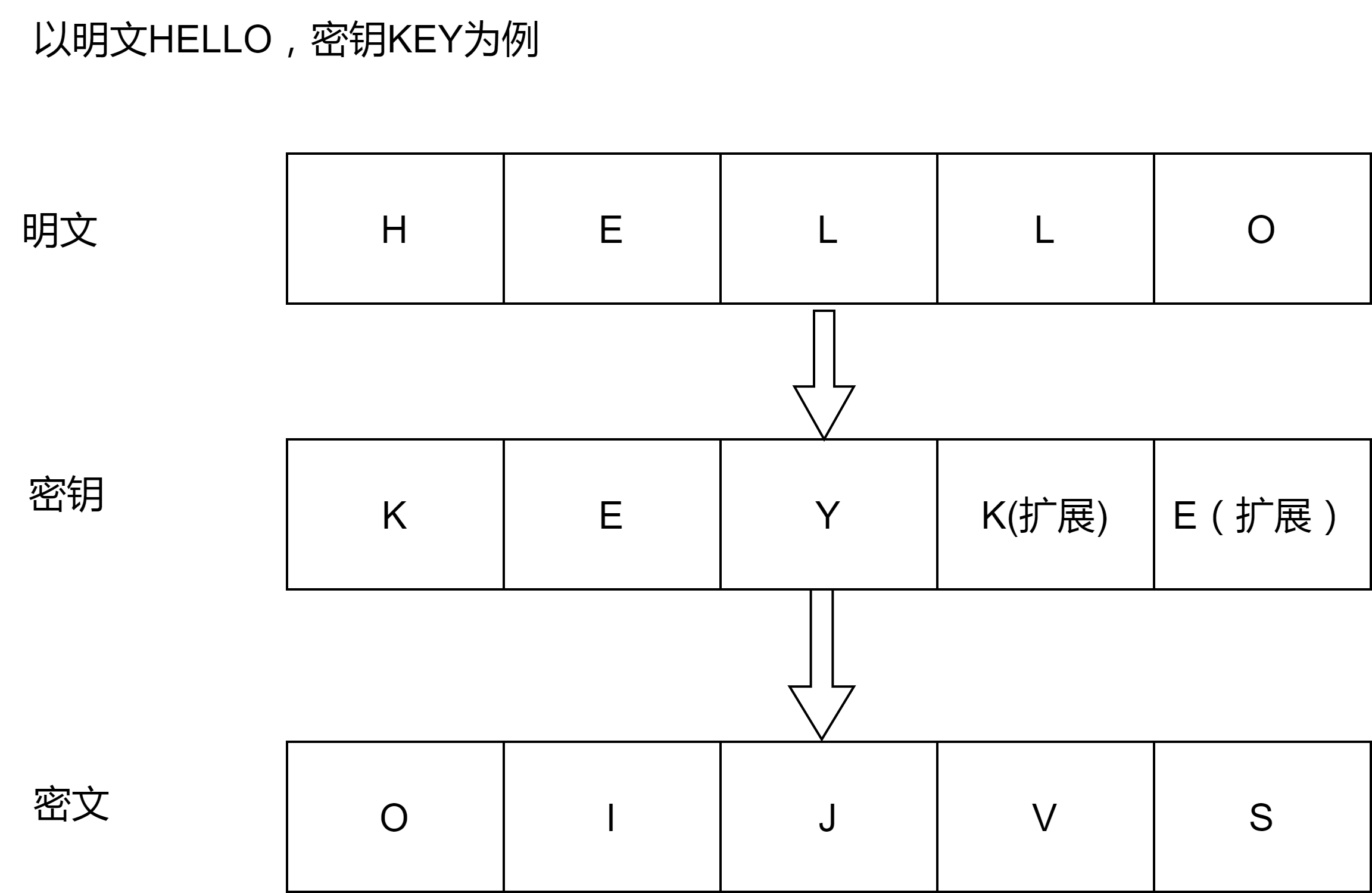


图 2‑2维吉尼亚密码原理图

维吉尼亚密码相对于简单的替换密码更为安全，因为它会对同一字母进行不同的替换。且加密过程简单，只要构建一个维吉尼亚加密表即可快速对明文进行加密。作为最著名的多表代替密码，维吉尼亚密码有多个密文表，平滑了频率分布，从而使得密码分析更加困难。

但如果密钥长度过短，或者密钥的重复性太强，仍然容易受到频率分析等攻击。总体来说安全性不如现代加密算法，但在一些简单的应用场景下仍然具有一定的实用性。

# RSA和维吉尼亚加密算法设计与实现

## RSA加密算法设计

RSA加密算法的基础在于大整数的模幂运算，故要想实现RSA加密首先需要实现大整数以及大整数的相关运算。

为此实现了一个BigInt类，其运算与算法中的高精度计算类似。在C++中通过对运算符进行重载的方式，实现对BigInt类型数据的基本运算。

程序将从两个文件public.key和private.key中读取(公钥，模数)、(私钥，模数)对进行加密和解密。

为了进一步理解算法，还实现了生成公钥、私钥对的功能，即选取质数p，q以及公钥质数e，计算得到私钥d。这里用到了扩展欧几里得算法来计算d的值。在使用扩展欧几里得算法时通过增加判断，保证计算过程中不会出现BigInt类型数据的值小于0的情况。

为了对大于模数的大整数m进行加密(算法为了简化，模数设置的比较小)，需要在加密前对大整数m按模数的长度进行划分，然后对每一个划分块分别进行加密。令每个划分块的位数小于模数的位数即可实现这一点。在解密时同样分块地对密文进行解密然后合并即可。

考虑到划分后，块中可能会出现前导0，算法的做法是直接将前导0加到结果的开头(无论是明文加密还是密文解密中均是如此)，对前导0之后的内容进行模幂运算得到结果。

考虑到模幂运算的时间复杂度，公钥指数e和模数n的值设置的比较小。如果e的值设置的比较大，则模幂运算的开销呈指数增加。如果模数n设置的比较大，则对消息进行分割后，每块消息所对应的大整数m也会比较大，即指数比较大，模幂运算的开销同样呈指数上升。

最终实现的效果如下图 3‑1所示。

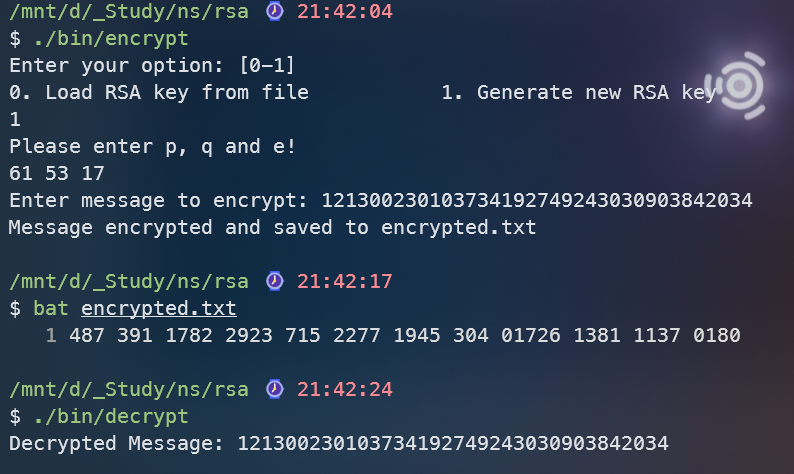


图 3‑1 rsa算法运行效果图

该算法没有调用openssh库，是从大整数类开始一步一步实现，故而性能相较成熟的库函数较为低下。但是从中可以清晰地看出rsa加密和解密是怎样一步一步时实现的。

尽管示例中没有用很大的p，q和e，但在不清楚密钥的前提下，rsa算法的安全性是可以保证的。

基于vector数据结构的大整数类，其基本运算(+, -, \*, /)是O(n)时间复杂度的，n为大整数的位数。而模幂运算，尽管使用了快速幂算法，但由于每次乘法与大整数的长度有关，最终模幂运算的复杂度依旧是O(n^e)数量级的，其中n是模数，e是公钥指数。时间开销相当大。

所以最终实现的rsa加密算法尽管安全性较高，但时间开销非常高。

## 维吉尼亚加密算法设计

维吉尼亚加密算法的思路比较简单，所以不太需要考虑性能的问题，故没有构造维吉尼亚密码加密所需的多个密文表，而是直接通过字符之间ASCII码的差值进行运算进行明文和密文之间的转换。

在加密前需要将密钥扩展到和明文字符串相同的长度，解密时也是如此。

同时还应注意，明文和密钥之间大小写的区别，大写字母和小写字母的ASCII码位于不同的区间，不能简单的叠加进行计算。

最终实现效果如下图 3‑2所示：

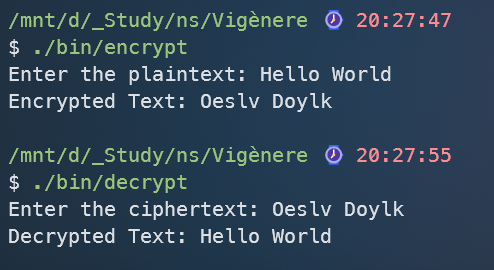


图 3‑3 Vigenere算法运行效果图

总的来说，该算法虽然实现简单，但是加密效果还是不错的，无法通过简单的词频分析就实现破译。在不知道密钥长度的情况下，也难以通过穷举攻击来破解。

该算法的加解密时间复杂度很低，是O(n)数量级的，n为明文的长度，所以在保证一定的安全性的基础上开销很小。

# Rsa和维吉尼亚加密算法实现总结与心得

## RSA和维吉尼亚算法总结

在自己动手实现了rsa和维吉尼亚算法之后，我对密码学和加解密算法有了更深一步的认识。

在实践过程中，我设计了rsa所需的数据类大整数型BigInt，设计了加密与解密独立的两个程序，同时解决了rsa加密时的分块和前导0的问题。对于维吉尼亚加解密，我设计了密钥扩展和大小写校正等算法细节，同样设计了加解密的两个程序。

最终实现了rsa和维吉尼亚的可交互的加解密程序。

完成了安全性高但时间开销大的手搓rsa和开销很小但安全性较弱的维吉尼亚加密过程。

## RSA和维吉尼亚算法心得

遇到的问题：

对于RSA算法，在实现过程中没能给出很好的平衡时间开销和数据结构复杂性的解决方案。

同时为了简化设计，没有给出将非数字符号转化为大整数的模块。

心得与建议：

希望课程能够越来越好。

# 参考文献

1. DAVID A.PATTERSON(美).计算机组成与设计硬件/软件接口(原书第4版).北京：机械工业出版社.
2. David Money Harris(美).数字设计和计算机体系结构（第二版）. 机械工业出版社

|  |
| --- |
| 一、原创性声明 |
| 本人郑重声明本报告内容，是由作者本人独立完成的。有关观点、方法、数据和文献等的引用已在文中指出。除文中已注明引用的内容外，本报告不包含任何其他个人或集体已经公开发表的作品成果，不存在剽窃、抄袭行为。  特此声明！  **作者签字: 刘文博** |