

南京邮电大学

实验报告

(2025 / 2026 学年 第 二 学期)

课程名称	计算机问题求解：使用算法
实验名称	密码算法
实验时间	2026 年 6 月 18 日
指导单位	计算机学院软件工程系
指导教师	

学生姓名	班级学号		
学院(系)	计算机学院	专 业	软件工程

实验报告

实验名称	密码算法			指导教师	
实验类型	设计	实验学时	2	实验时间	2026 6 18

一、 实验目的和要求

了解密码学中加/解密的基本原理，掌握数论的基本知识；理解非对称密码体制 RSA 加密算法的工作原理和流程；设计并实现一个简单的 RSA 公开密钥系统，能用公开密钥对明文进行加密，并用私人密钥对密文进行解密。。

二、 实验环境(实验设备)

操作系统：（Windows 10等）

调试软件名称：

调试软件版本号：

上机地点：学6-

三、实验原理及内容

算法原理

RSA 算法基于大数分解难题，核心步骤如下：

1. 密钥生成：选取两个大质数 p 、 q ，计算 $n = p \times q$ ，欧拉函数 $\phi(n) = (p-1)(q-1)$ ；
2. 选公钥 e ：满足 $1 < e < \phi(n)$ 且 $\gcd(e, \phi(n)) = 1$ ；
3. 求私钥 d ： d 是 e 关于 $\phi(n)$ 的模逆元，即 $e \times d \equiv 1 \pmod{\phi(n)}$ ，用扩展欧几里得算法求解；
4. 加密：密文 $C = M^e \bmod n$ ；
5. 解密：明文 $M = C^d \bmod n$ 。

正确性保证来自欧拉定理： $M^{\phi(n)} \equiv 1 \pmod{n}$ ，因此 $M^{(e \times d)} = M^{(k\phi(n)+1)} \equiv M \pmod{n}$ 。

快速幂取模（反复平方法）将指数运算从 $O(\exp)$ 降至 $O(\log \exp)$ ，是实现中的关键优化。

代码实现

```
#include <iostream>
#include <vector>
#include <cmath>
#include <cstring>
using namespace std;

// =====
// RSA 公开密钥系统
// =====

// 快速幂取模：计算 base^exp mod mod
long long modPow(long long base, long long exp, long long mod)
{
    long long result = 1;
    base %= mod;
    while (exp > 0) {
        if (exp & 1) result = result * base % mod;
        base = base * base % mod;
        exp >>= 1;
    }
    return result;
}

// 扩展欧几里得算法：求 a 关于 m 的模逆元
// 即找 x 使得 a*x ≡ 1 (mod m)
long long extGcd(long long a, long long b, long long& x, long long& y) {
    if (b == 0) { x = 1; y = 0; return a; }
    long long x1, y1;
    long long g = extGcd(b, a % b, x1, y1);
    x = y1;
    y = x1 - (a / b) * y1;
    return g;
}
```

实验报告

四、实验小结（包括问题和解决方法、心得体会、意见与建议等）

【遇到的问题及解决方法】

1. 模逆元计算出负数：扩展欧几里得算法求出的 x 可能为负，直接使用会导致私钥 d 为负数。解决方法是在返回前执行 $(x \% m + m) \% m$ ，确保结果落在正整数范围内。
2. 公钥 e 的选取不够通用：最初写死 $e=3$ ，但在某些 p 、 q 组合下 $\gcd(3, \phi(n)) \neq 1$ 导致密钥无效。改为从常用候选值 $\{7, 11, 13, 17, 19, 23\}$ 中自动选第一个满足互质条件的值。

【心得体会】

RSA 的巧妙之处在于它把[分解大数很难]这个数学事实转化成了安全性保证。整个算法涉及的数论知识——欧拉定理、模逆元、扩展欧几里得——单独看都不复杂，但组合起来能形成如此实用的密码系统，让人印象深刻。实验中体会最深的是快速幂取模的重要性：没有它，哪怕是几百以内的数做指数运算都会溢出。这也让我理解了为什么算法优化在密码学里格外关键。

五.支撑毕业要求指标点

- (1) 3-2-M能够根据用户需求, 选取适当的研究方法和技术手段, 确定复杂工程问题的解决方案。
- (2) 3-3-H能综合利用专业知识对解决方案进行优化, 体现创新意识, 并考虑健康、安全以及环境等因素。
- (3) 7-2-M正确理解和评价计算机及应用领域复杂工程问题实施对环境保护及社会可持续发展等的影响, 评价产品周期中可能对人类和环境造成的损害和隐患。

六、指导教师评语

评 分	细 则	评分项	优秀	良好	中等	合格
	遵守实验室规章制度					
	学习态度					
	算法思想准备情况					
	程序设计能力					
	解决问题能力					
	课题功能实现情况					
	算法设计合理性					
	算法效能评价					
	回答问题准确度					
	报告书写认真程度					
	内容详实程度					
	文字表达熟练程度					
	其它评价意见					
	本次实验能力达成评价 (总成绩)					
成 绩		批阅人		日 期		