



哈爾濱工業大學(深圳)

HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

# RSA密码算法实验





# 实验目的

---

- 掌握 RSA 算法的密钥生成方法
- 掌握 RSA 算法的加解密过程
- 了解RSA算法的具体应用



# 实验内容

## 编写代码实现RSA加密解密程序

- 1) 随机选取满足条件的 $p$ 、 $q$ 和 $d$ ，要求 $p$ 和 $q$ 的值在1000-10000之间，也就是二进制长度不小于14bit.
- 2) 以附件的明文lab2-Plaintext.txt作为待加密的明文，可以自行设定编码格式。  
方式1：每个英文字母对应一个数字，规则如下：每个字母或数字与一个两位的十进制数字对应，（如：数字为00 - 09， $a-z = 10-35$ ， $A-Z = 36-61$ ），明文的一个分组块由4个十进制数字组成，即两个字母。去掉空格和其他标点符号。  
方式2：直接将字符的ASCII码两个字符组成一个十进制数处理（六位十进制数）。
- 3) 用公钥加密，私钥解密。
- 4) 将 $p, q, n, e, d, \phi(n)$ 的值以及加密后的密文、解密后的明文输出到文件或屏幕。



## 实验原理

### ➤ RSA的密钥产生过程

- (1) 生成两个保密的大素数  $p$  和  $q$  ;
- (2) 计算这两个素数的乘积  $n$ ,  $n = p \times q$  ;
- (3) 计算小于  $n$  并且与  $n$  互质的个数, 即欧拉函数  $\varphi(n) = (p-1)(q-1)$  ;
- (4) 选择随机的素数  $e$  , 满足  $1 < e < \varphi(n)$  , 并且  $e$  和  $\varphi(n)$  互质, 即  $\gcd\{\varphi(n), e\} = 1$  ;
- (5) 根据  $d \cdot e \equiv 1 \pmod{\varphi(n)}$  , 求出  $d$  ;

保密  $d$ , 公开  $n$  和  $e$ ; 以  $\{e, n\}$  为公钥,  $\{d, n\}$  为私钥。  
 $p$  和  $q$  销毁



## 实验原理

➤ 加密算法

$$c \equiv m^e \pmod{n}$$

➤ 解密算法

$$m \equiv c^d \pmod{n}$$

**Tips: 要求 $m < n$ ，如果 $m > n$ ，需要进行分组。**

加密时首先将明文比特串分组，使得每个分组对应的十进制数小于 $n$ ，即分组长度小于 $\log_2 n$ 。



# RSA-密钥

- 两个素数:  $p=17, q=11$
- 计算  $n=pq=17*11=187$
- 计算  $\varphi(n)=(p-1)(q-1)=16*10=160$
- 选择  $e$ , 其中  $\gcd(e, 160)=1$ , 假设  $e=7$
- 求解  $d$ , 其中  $ed=1 \bmod 160, 2 < d < 160$   
 $d=23$ , 验证  $23*7=161=1*160+1$

公钥PU={7, 187}

私钥PR={23, 187}

# RSA-加密/解密

- $M=88 \quad (88 < 187)$
- 加密
$$C = 88^7 \bmod 187 = 11$$
- 解密
$$M = 11^{23} \bmod 187 = 88$$



- 大整数库官网 <https://gmplib.org/>



## 实验原理

### ➤如何找到足够的大随机素数 $p$ 和 $q$

- Miller-Rabin算法TEST( $n$ )细节:

1. 找出整数 $k, q$ , 其中 $k > 0, q$ 是奇数, 使得 $(n - 1 = 2^k q)$ ;
2. 随机选取整数 $a, 1 < a < n - 1$ ;
3. If  $a^q \bmod n = 1$ 或者 $n - 1$ , 返回“很可能为素数”;
4. For  $j = 1$  to  $k - 1$  do
5. If  $a^{2^j q} \bmod n = n - 1$ , 返回“很可能为素数”
6. 返回“合数”





## 实验原理

➤ 如何通过  $d \cdot e \equiv 1 \pmod{\varphi(n)}$  求得  $d$

### ◆ 扩展的欧几里德算法

如果  $(a,b)=1$ ，则  $b$  在  $\text{mod } a$  下有乘法逆元（不妨设  $b < a$ ），即存在一  $x (x < a)$ ，使得  $bx \equiv 1 \pmod{a}$ 。推广的Euclid算法先求出  $(a,b)$ ，当  $(a,b)=1$  时，则返回  $b$  的逆元。

EXTENDED EUCLID  $(a,b)$  (设  $b < a$ )

1.  $(X_1, X_2, X_3) \leftarrow (1, 0, a)$ ;  $(Y_1, Y_2, Y_3) \leftarrow (0, 1, b)$  ;
2. if  $Y_3 = 0$  then return  $X_3 = (a, b)$  ; no inverse;
3. if  $Y_3 = 1$  then return  $Y_3 = (a, b)$  ;  $Y_2 = b^{-1} \pmod{f}$ ;
4.  $Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor$
5.  $(T_1, T_2, T_3) \leftarrow (X_1 - QY_1, X_2 - QY_2, X_3 - QY_3)$  ;
6.  $(X_1, X_2, X_3) \leftarrow (Y_1, Y_2, Y_3)$  ;
7.  $(Y_1, Y_2, Y_3) \leftarrow (T_1, T_2, T_3)$  ;
8. goto 2



## 实验原理

- 加密和解密运算都是模指数运算,  $c \equiv m^e \bmod n$   $m \equiv c^d \bmod n$
- 可以通过 $e-1$ 次模乘来实现计算, 但是如果 $e$ 非常大, 效率会很低下
- **平方-乘**算法可以把计算所需的模乘的次数减少

### 求模指数实例

$$11^{23} \bmod 187 = [(11^1 \bmod 187) * (11^2 \bmod 187) * (11^4 \bmod 187) * (11^8 \bmod 187) * (11^8 \bmod 187)] \bmod 187$$

$$11^1 \bmod 187 = 11$$

$$11^2 \bmod 187 = 121$$

$$11^4 \bmod 187 = 14641 \bmod 187 = 55$$

$$11^8 \bmod 187 = 214358881 \bmod 187 = 33$$

$$\begin{aligned} 11^{23} \bmod 187 &= (11 * 121 * 55 * 33 * 33) \bmod 187 \\ &= 79720245 \bmod 187 = 88 \end{aligned}$$



## 实验原理

# 计算 $a^b \bmod p$

```
y=1
while(1)
{
    if (b == 0)
        return y;
    while (b > 0 && b % 2 == 0)
    {
        a = (a * a) % p;
        b = b / 2;
    }
    b--;
    y = (a * y) % p;
}
```

## 快速幂介绍视频

[https://www.bilibili.com/video/BV16Z4y1M7y1?from=search&seid=12692871177987833892&spm=id\\_from=333.337.0.0](https://www.bilibili.com/video/BV16Z4y1M7y1?from=search&seid=12692871177987833892&spm=id_from=333.337.0.0)



## 实验注意细节

- 1、RSA中加密解密用10进制来算；
- 2、加密时明文4个十进制位一组明文加密，也就是一个4位数。
- 3、如果最后一个分组不足4位，比如1个字母，明文分组可以自己设定一个2位数的值进行填充。这个2位数自己设定（大于61的数字），解密时删除。
- 4、明文加密后的密文分组需要处理长度，否则解密时不知道如何分组。为保险起见，设置密文的分组长度可为最大可能的长度  $\log_2 n$ 。
- 5、对于长度不足的情况，要前面补0
- 6、解密时如果明文长度不足4位也是前面补0



## 实验要求

## • 提交内容

- ① 源代码
- ② 实验结果截图

- 截止时间

下一次实验课前提交至HITsz Grader 作业提交平台，具体截止日期参考平台发布。

- 登录网址：： <http://grader.tery.top:8000/#/login>
- 推荐浏览器： Chrome
- 初始用户名、密码均为学号，登录后请修改

实验指导书: <https://cryptography.p.cs-lab.top/>

课件链接: <https://gitee.com/hitsz-cslab/cryptography-labs/tree/master/stupkt>

**请同学们开始实验！**

