哈尔滨工业大学（深圳）
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

RSA密码算法实验

主讲教师：蒋琳

实验教师：苏婷

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

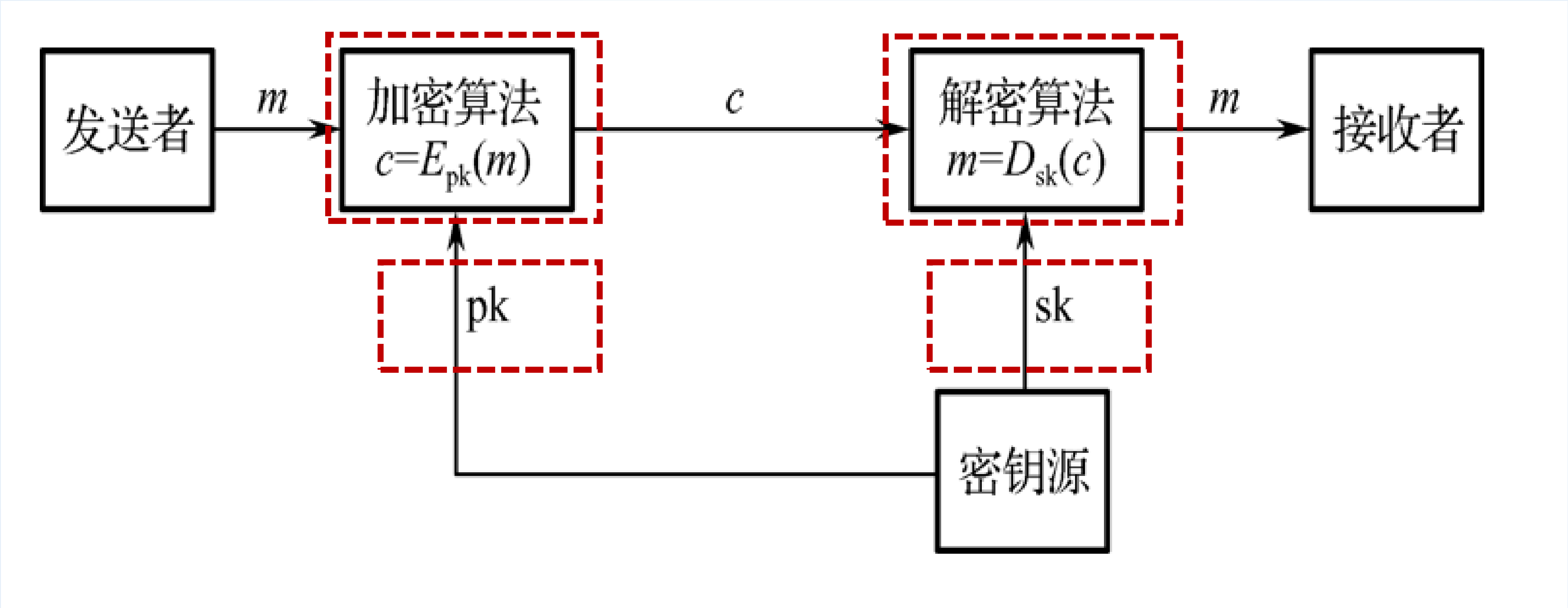
实验内容

1、完成对字符串或文件的RSA加解密算法；

2、密钥至少取32位长度。

实验原理

公钥密码体制加密过程



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) 选择一个随机数e，满足$1 < e < \varphi(n)$，并且e和$\varphi(n)$互质，即$\gcd\{\varphi(n), e\} = 1$;

(5) 根据 $d \cdot e \equiv 1 \bmod \varphi(n)$，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

$$c \equiv m^e \bmod n$$

➢ 解密算法

$$m \equiv c^d \bmod n$$

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 $\log_2 n$ 。

实验原理

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 mod 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 $(88<187)$
- 加密

  $C=88^{7} \bmod 187 = 11$
- 解密

  $M=11^{23} \bmod 187 = 88$

实验原理

- 如何找到足够的大随机素数p和q?
- 如何通过 $d \cdot e \equiv 1 \bmod \varphi(n)$ 求得d？
- 如何快速进行模幂运算?
- 如何进行大数运算?

实验原理

➢如何找到足够的大随机素数p和q

◆**Miller-Rabin概率检测法**

原理：若n为素数，则a^{n-1} =1mod n且 1mod n只有1和-1两个平方根（x^2 =1mod n ）

算法描述：把n-1写成n-1 = $2^k t$,其中t是一个奇数

随机选择一个整数a，满足1<=a<=n-1

```
b = a^t mod n
if b=1(mod n)
   then return( “n is prime” );
for i = 0 to k-1
{
    if b= -1(mod n)
    then return( “n is prime” );
    else b = b^2 (mod n)
}
return( “n is composite” );
```

可参考：
https://blog.csdn.net/ltyqljhwcm/article/details/53045840

实验原理

➢如何通过 $d \cdot e \equiv 1 \bmod \varphi(n)$ 求得d

◆ 扩展的欧几里德算法

如果$(a,b)=1$，则 b 在 mod$a$ 下有乘法逆元（不妨设$b<a$），即存在一 $x\,(x<a)$，使得 $bx \equiv 1 \bmod a$ 。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 $Y_3=(a,b)$; $Y_2=b^{-1} \bmod f$;
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，$c \equiv m^e \bmod n \quad m \equiv c^d \bmod n$
- 可以通过e-1次模乘来实现计算，但是如果e非常大，效率下降会很低下
- 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

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

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

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

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

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

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

实验原理

计算a^b mod 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;
    }
```

实验内容

1、完成对字符串或文件的RSA加解密算法；

2、密钥至少取32位长度。

实验要求

用户名/密码：学号/学号

初次登录，请修改密码！

- **截止时间**

① 两周时间内提交（**2020-12-15 00:00**）

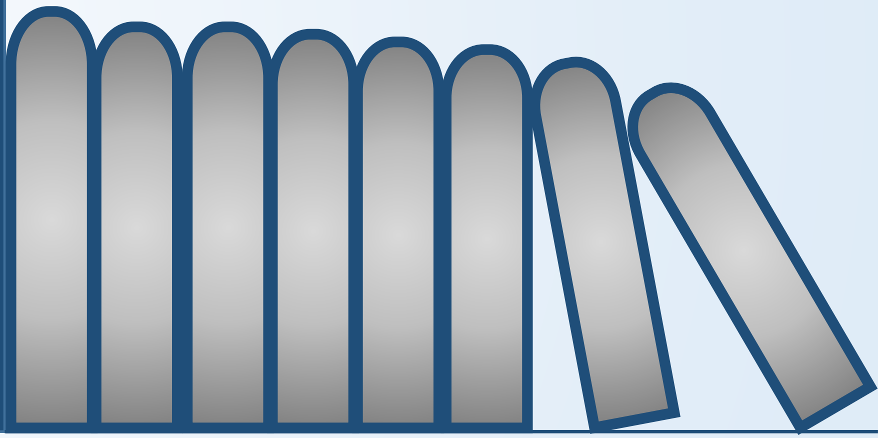
② 平台链接 http://10.249.182.83:8000/#/login

- **提交内容**

① 将源码和实验报告打成zip包上传

② 以学号_姓名命名

谢谢



实验原理

- 如何找到足够的**大随机素数p和q**
  - Solovay-Strassen概率性素性检测法
  - **Miller-Rabin概率检测法**

引理 如果 P为大于2的素数，则方程 $x^2 \equiv 1 \pmod{p}$ 的解只有 $x \equiv 1$和$x \equiv -1$。

证明 由 $x^2 \equiv 1 \pmod{p}$ ，有 $x^2 - 1 \equiv 0 \bmod p$， $(x+1)(x-1) \equiv 0 \bmod p$ ，
因此 $p|(x+1)$ 或 $p|(x-1)$或 $p|(x+1)$ 且 $p|(x-1)$。