

《密码学》设计之三——

RSA 加密算法中大数运算的实现

一、 RSA 算法

(1) RSA 的密钥对生成算法:

- 1.选取两个大素数 p 和 q , 两个数长度接近且相差较大。
- 2.计算 $n=p*q, \varphi(n)=(p-1)(q-1)$
3. 随机选取整数 e , 满足 $\gcd(e, \varphi(n))=1$
4. 计算 d , 满足 $d*e \equiv 1 \pmod{\varphi(n)}$ 。

注: p 和 q 保密。 e 和 n 为公钥, d 为私钥。

(2) RSA 加密

将明文编码成整数分组 m , m 对应的十进制数小于 n , 即整数分组 m 的位数小于 $\log_2 n$ bits。

$$c=E(m) \equiv m^e \pmod{n}$$

(3) RSA 解密

$$m=D(c) \equiv c^d \pmod{n}$$

二、 功能要求:

(1) 构建 RSA 加密算法中针对 512 位大整数运算的函数库, 包括大整数乘法运算函数、大整数幂模运算函数、大整数素性判断函数、利用扩展 Euclid 算法求一个大整数在模运算下的逆元的函数。

(2) 实现 RSA 算法中参数, 包括大素数 $p, q, n, \Phi(n)$ 的生成、公钥对 (n, e) 的生成、私钥的生成;

- (3) 实现对明文编码、明文加密生成密文的过程演示；
- (4) 实现对相应密文解密的过程演示；
- (5) 给出算法实现的代码、运行测试。