密码学作业003 学号 20131910023 姓名 金洋

密码学作业003（以Word文档提交）：

1. 什么是因子分解问题？

答：两个大的素数相乘，为这两个数数相乘得到一个数是容易的，但分解这个大数且恢复原来的两个大素数却是困难的。

1. 基于Fermat小定理证明欧拉公式.

欧拉公式: p,q是两个不同的素数，令g=gcd(p-1,q-1)，求证：当gcd(a,pq)=1时，

证明：由条件知不整除a，且g|q-1，



同理 

又gcd(p,q)=1,故

1. 基于群的结论证明欧拉公式.

欧拉公式: p,q是两个不同的素数，令g=gcd(p-1,q-1)，求证：当gcd(a,pq)=1时，

引理1．若a,b,c为任意3个整数,m为正整数,且(m,c)=1,则当ac≡bc(mod m)时,有a≡b(mod m)；

引理2．设m是一个[整数](http://baike.baidu.com/view/71484.htm" \t "http://baike.baidu.com/_blank),且m>1,b是一个[整数](http://baike.baidu.com/view/71484.htm" \t "http://baike.baidu.com/_blank)且(m,b)=1.如果a1,a2,a3,a4,…am是模m的一个完全剩余系,则ba[1],ba[2],ba[3],ba[4],…ba[m]也构成模m的一个完全剩余系.

证明：构造素数p的既约[剩余系](http://baike.baidu.com/view/1758580.htm" \t "http://baike.baidu.com/_blank)



因为(a,p)=1，由引理2可得



也是p的一个既约[剩余系](http://baike.baidu.com/view/1758580.htm" \t "http://baike.baidu.com/_blank)。由既约剩余系的性质，



即得,

又(q-1)/g为整数易知

同理

又gcd(p,q)=1,故

1. 证明RSA密码体制的解密正确性.

证明：最终得到，



以下证明

①当（m,pq）=1时



故

②当（m,pq）=pq，即m=0 mod (pq)

，故

③当1<（m,pq）<pq，则（m,pq）为p或q；

不妨考虑（m,pq）=q，则m=sq，且（s,p）=1

对\*式做修改





又（p,q）=1,结合以上两式，可得\*式=m

综合①②③知，即RSA密码体制的解密正确性得证；

1. 解释RSA密码体制的共模攻击.

假设有一家公司COMPANY，在员工通信系统中用RSA加密消息。COMPANY首先生成了两个大质数P,Q，取得PQ乘积N。并且以N为模数，生成多对不同的公钥及其相应的私钥。

COMPANY将所有公钥公开。而不同的员工获得自己的私钥，比如，员工A获得了私钥.员工B获得了私钥. 现在，COMPANY将一条相同的消息，同时经过所有公钥加密，发送给所有员工。此时，就可能出现共模攻击。

共模攻击利用的大前提就是，RSA体系在生成密钥的过程中使用了相同的模数N。依以上面的案例展开:

假设COMPANY用所有公钥加密了同一条信息M，也就是



此时员工A拥有密钥他可以通过，解密得到消息m；同时员工B拥有密钥他可以通过，解密得到消息m；

如果，此时有一个攻击者，同时监听了A和B接收到的密文，因为模数不变，以及所有公钥都是公开的，那么利用同模攻击，他就可以在不知道的情况下解密得到消息m。

这里就是要论证，当N不变的情况下，知道 可以在不知道的情况下，解出m。

首先假设，互质，即gcd()=1。此时则有

式中，皆为整数，但是一正一负。

通过扩展欧几里德算法，我们可以得到该式子的一组解（），假设s1为正数,s2为负数.

因为

所以

又前面提到

所以，即证明了命题：当N不变的情况下，知道 可以在不知道的情况下，解出m。

1. 查阅文档，了解因子分解问题用于密码设计时对于参数规模的要求。

RSA遭受攻击的很多情况是因为算法实现的一些细节上的漏洞所导致的，所以在使用RSA算法构造密码系统时，为保证安全，在生成大素数的基础上，还必须认真仔细选择参数，防止漏洞的形成。根据RSA加解密过程，其主要参数有三个：模数N，加密密钥e，解密密钥d。

### I 模数N的确定

### 虽然迄今人们无法证明，破解RSA系统等于对N因子分解，但一般相信RSA系统的安全性等同于因子分解，即：若能分解因子N，即能攻破RSA系统，若能攻破RSA系统，即能分解因子Ⅳ。因此，在使用RSA系统时，对于模数N的选择非常重要。在RSA算法中，通过产生的两个大素数p和q相乘得到模数N，而后分别通过对它们的数学运算得到密钥对。由此，分解模数N得到p和q是最显然的攻击方法，当然也是最困难的方法，如果模数N被分解，攻击者利用得到的P和q便可计算出，进而通过公开密钥e由解密密钥d，则RSA体制立刻被攻破。相当一部分的对RSA的攻击就是试图分解模数N，选择合适的Ｎ是实现RSA算法并防止漏洞的重要环节。一般地，模数N的确定可以遵循以下几个原则：

### ①p和q之差要大。

### 当p和q相差很小时，在已知n的情况下，可假定二者的平均值为，然后利用，若等式右边可开方，则得到及，即N被分解。

②p-1和q-1的最大公因子应很小。

③p和q必须为强素数。

一素数p如果满足：

条件一：存在两个大素数，，使得|p-1且|p+1；

条件二：存在四个大素数，，，使得。则此素数为强素数。其中，，，称为3级的素数，，称为2级的素数，p则称为1级的素数，很明显地，任何素数均为3级的素数。只有两个强素数的积所构成的N，其因子分解才是较难的数学问题。

④p和q应大到使得因子分解N为计算上不可能。

RSA的安全性依赖于大数的因子分解，若能因子分解模数N，则RSA即被攻破，因此模数N必须足够大直至因子分解N在计算上不可行。因子分解问题为密码学最基本的难题之一，如今，因子分解的算法已有长足的进步，但仍不足以说明RSA可破解。为保证安全性，实际应用中所选择的素数P和拿至少应该为300位以上的二进制数，相应的模数N将是600位以上的二进制数。

目前，SET(Secure Electronic Transaction)协议中要求CA采用2048比特长的密钥，其他实体使用1024比特的密钥。随着计算能力的提高和分布式运算的发展，安全密钥的长度将是动态增长的。

Jadith Moore给出了使用RSA时有关模数的一些限制：

①若给定模数的一个加/解密密钥指数对已知，攻击者就能分解这个模数。

②若给定模数的一个加/解密密钥指数对已知，攻击者无需分解模数Ⅳ就可以计算出别的加/解密密钥指数对。

③在通信网络中，利用RSA的协议不应该使用公共模数。

④消息应该用随机数填充以避免对加密指数的攻击。

### II e的选取原则

### 在RSA算法中，e和互质的条件容易满足，如果选择较小的e，则加、解密的速度加快，也便于存储，但会导致安全问题。

### 一般地，e的选取有如下原则：

### ①e不能够太小。在RSA系统中，每人的公开密钥P只要满足即可，也即e可以任意选择，为了减少加密运算时间，很多人采用尽可能小的e值，如3。但是已经证明低指数将会导致安全问题，故此，一般选择e为16位的素数，可以有效防止攻击，又有较快速度。

②e应选择使其在的阶为最大。即存在i，使得，

可以有效抗击攻击。

### III d的选取原则

### 一般地，私密密钥d要大于。在许多应用场合，常希望使用位数较短的密钥以降低解密或签名的时间。例如IC卡应用中，IC卡CPU的计算能力远低于计算机主机。长度较短的d可以减少IC卡的解密或签名时间，而让较复杂的加密或验证预算(e长度较长)由快速的计算机主机运行。一个直接的问题就是：解密密钥d的长度减少是否会造成安全性的降低?很明显地，若d的长度太小，则可以利用已知明文M加密后得，再直接猜测d，求出是否等于M。若是，则猜测J下确，否则继续猜测。若d的长度过小，则猜测的空间变小，猜中的可能性加大，已有证明当时，可以由连分式算法在多项式时间内求出d值。因此其长度不能过小。