实验原理

一．非对称密钥加密概述

前面讲述了对称密钥加密体制。使用对称密钥加密体制进行保密通信时，任意不同的两个用户之间都应该使用互不相同的密钥。这样，如果一个网络中有n个用户，他们之间彼此都可能进行秘密通信，这时网络中将需要n(n-1)/2个密钥（其中，每个用户都需要保存n-1个密钥），这样巨大的密钥量给密钥分配和管理带来了极大的困难。另外，随着计算机网络，特别是因特网的发展，网络上互不相识的用户可能需要进行保密的会话（例如，如果用户在进行电子商务活动时，需要保密的连接，这时的客户对象可能根本不是固定的对象）。最后，对称密钥加密机制难以解决签名验证问题。

非对称密钥加密也称为公开密钥加密，或者叫做公钥加密算法。使用公开密钥密码的每一个用户都分别拥有两个密钥：加密密钥和解密密钥，它们两者并不相同，并且由加密密钥得到解密密钥在计算机上是不可行的。每一个用户的加密密钥都是公开的。因此，加密密钥也称为公开密钥。所有用户的公开密钥都将记录在作用类似于电话号码薄的密钥本上，而它可以被所有用户访问，这样每一个用户都可以得到其他所有用户的公开密钥。同时，每一个用户的解密密钥将由用户保存并严格保密。因此，解密密钥也称为私有密钥。

非对称密码算法解决了对称密码体制中密钥管理的难题，并提供了对信息发送人的身份进行验证的手段，是现代密码学最重要的发明。公钥加密算法一般是将对密钥的求解转化为对数学上的困难问题的求解，例如RSA算法的安全性是建立在“大数分解和素性检测”这个数论难题的基础上，已知两个大素数a、b，求出a*b是容易计算的，而已知a*b，想知道其是哪两个大素数的乘积目前还没有好的计算方法，另外也有一些非对称加密算法（如ELGamal算法）的安全性是基于求“离散对数”这个数学难题上的。

在公钥密码系统中每个实体都有自己的公钥和相应的私钥。公钥密码系统的加密变换和解密变换分别用E和D表示。任何实体B要向实体A发送信息m的步骤如下：实体B首先获得实体A的真实公钥的拷贝（eA），实体B使用eA计算密文c=E（m）并发送给实体A，实体A使用自己的私钥dA，计算m=D（c）解密密文，恢复出明文m。这里公钥不需要保密，但要保证它的真实性，即eA确实是实体A掌握的私钥dA所对应的公钥。提供真实的公钥比安全地分配密钥实现起来要容易得多。这也是公钥密码系统的主要优点之一。

公钥密码系统的主要目的是提供保密性，它不能提供数据源认证(data origin authentication)和数据完整性(data integrity)。数据源认证是指：指定的数据是在以前的某个时间确实是由真正的源创建的。数据完整性是指：真正的源创建该数据后经过传输后存储没有发生改变。数据源认证和数据完整性要由其他技术来提供（如消息认证码技术、数字签名技术等）。

从本质上来看，公钥密码比对称密钥密码加密的速度要慢，粗略的说，公钥加密算法RSA硬件实现比分组加密算法DES硬件实现的速度慢1500倍，而软件实现的速度要慢100倍。

公钥解密也可以提供认证保证（如：在实体认证协议、带认证的密钥建立协议等）。公钥加密中必须有颁发让发送消息的人得到想要发送到的那个人的公钥的真实拷贝，否则就会受到伪装攻击。在实践中有很多方法分发真实的公钥，如：使用可信的公共文件，使用在线可信服务器，使用离线服务器和认证。

公钥加密的优点：

- 大型网络中的每个用户需要的密钥数量少。
- 对管理公钥的可信第三方的信任程度要求不高而且是离线的。
- 只有私钥是保密的，而公钥只要保证它的真实性。

缺点：

- 多数公钥加密比对称密钥加密的速度要慢几个数量级。
- 公钥加密方案的密钥长度比对称加密的密钥要长。
- 公钥加密方案没有被证明是安全的。

公钥密码的概念本身就被公认为是密码学上的一块里程碑。二十多年来的研究表明，公钥密码成功地解

决了计算机网络安全中的密钥管理，身份认证和数字签名等问题，已经成为信息安全技术中的重大核心技术。

二．RSA算法概述

RSA加密算法于1977年由美国麻省理工学院的Ronal Rivest，Adi Shamir和Len Adleman三位年轻教授提出，并以三人的姓氏Rivest，Shamir和Adleman命名为RSA算法。这三位科学家荣获2002年度图灵奖，以表彰他们在算法方面的突出贡献。该算法利用了数论领域的一个事实，那就是虽然把两个大质数相乘生成一个合数是件十分容易的事情，但要把一个合数分解为两个质数的乘积却十分困难。合数分解问题目前仍然是数学领域尚未解决的一大难题，至今没有任何高效的分解方法。它无须收发双方同时参与加密过程，既可以用于保密也可以用于签名，因而非常适合于电子邮件系统的加密，互连网和信用卡安全系统。

三．RSA算法的加密和解密过程

在RSA算法中，每个实体有自己的公钥(e，n)及私钥(d，n)，其中n = pq（p、q是两个大素数），φ(n) = (p-1)(q-1)，ed = 1 mod φ(n)，显然e应该满足gcd(e，φ(n))= 1。实体B加密消息m，将密文在公开信道上传送给实体A。实体A接到密文后对其解密。具体算法如下。

1．公私钥的生成算法

RSA的公私钥生成算法十分简单，可以分为五步：

（1）随机地选择两个大素数p和q，而且保密；

（2）计算n=pq，将n公开；

（3）计算φ(n)=(p-1)(q-1)，对φ(n)保密；

（4）随机地选择一个正整数e，1<e<φ(n)且(e，φ(n))=1，将e公开；

（5）根据ed=1 mod φ(n)，求出d，并对d保密。

公开密钥是由(e，n)构成，私有密钥由(d，n)构成。

2．加密算法

实体B的操作如下：

（1）得到实体A的真实公钥（e，n）；

（2）把消息表示成整数m，0＜m≤n－1；

（3）使用平方－乘积算法，计算$C = E_k(m) = m^e \bmod n$；

（4）将密文C发送给实体A。

3．解密算法

实体A接收到密文C，使用自己的私钥d计算$m = D_k(C) = C^d \bmod n$。

我们选择p=3，q=11，得到n=33，φ(n)=(p-1)(q-1)=2×10=20。由于7和20互质，故设e=7。对于所选的e=7，解方程7×d=1 mod 20，可以得到d=3。因此公钥为(7，33)，私钥为(3，33)。

在我们的例子中，由于所选的p和q太小，破译当然很容易，我们的例子只是用来说明此算法的原理。对于明文SUZANNE，RSA的加密和解密过程如表3-1-1所示。

表3-1-1　RSA加解密过程示例

加密				解密			
明文（m）		m^e	密文（C）	密文（C）	C^d	明文（m）	
符号	值	m^7	m^7(mod33)	m^7(mod33)	C^3	C^3(mod33)值	符号
S	19	893871739	13	13	2197	19	S
U	21	1801088541	21	21	9261	21	U
Z	26	8031810176	5	5	125	26	Z
A	1	1	1	1	1	1	A

N	14	105413504	20	20	78125	14	N
N	14	105413504	20	20	78125	14	N
E	5	78125	14	14	2744	5	E