§4.2 RSA公钥密码体制

RSA是一种基于公钥密码体制的优秀加密算法，1978年由美国麻省理工学院(MIT)的研究小组成员：李维斯特(Rivest)、沙米尔(Shamir)、艾德曼(Adleman)提出的。

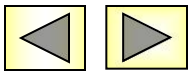
RSA算法是一种分组密码体制算法，它的保密强度是建立在具有大素数因子的合数，其因子分解是困难的（基于大数分解的难度）。

公钥和私钥是一对大素数的函数，从一个公钥和密文中恢复出明文的难度等价于分解两个大素数之积。

RSA得到了世界上的最广泛的应用，ISO在1992年颁布的国际标准X.509中，将RSA算法正式纳入国际标准。

§4.2 RSA公钥密码体制

整数n的十进制位数	因子分解的运算次数	所需计算时间（每微秒一次）
50	1.4×10^{10}	3.9小时
75	9.0×10^{12}	104天
100	2.3×10^{15}	74年
200	1.2×10^{23}	3.8×10^{9}年
300	1.5×10^{29}	4.0×10^{15}年
500	1.3×10^{39}	4.2×10^{25}年



§4.2 RSA公钥密码体制

RSA密钥体制的特点：

（1）密钥配发十分方便，用户的公开密钥可以像电话本那样公开，使用方便，每个用户只需持有一对密钥即可实现与网络中任何一个用户的保密通信。

（2）RSA加密原理基于单向函数，非法接收者利用公开密钥不可能在有限时间内推算出秘密密钥。

RSA在用户确认和实现数字签名方面优于现有的其他加密机制。

§4.2 RSA公钥密码体制

单向函数：

给定一个函数f，若对任意给定的x，计算y，使得$y=f(x)$是容易的；但对任意给定的y，计算x，使得$f(x)=y$是难解的，即计算$f^{-1}(y)$是困难的。则称f为单向函数。

例：$f(x)=a^x$（x、$a\in GF(q)$）为单向函数。

陷门单向函数：

给定一个函数f，t为f相关的参数，任意给定的x，计算y，使得$y=f(x)$是容易的；当t未知时，计算逆函数$f^{-1}(y)$难解，而当t已知时，计算$f^{-1}(y)$容易。则称为f陷门单向函数。

§4.2 RSA公钥密码体制

用于构造双钥密码的单向函数：

（1）多项式求根

（2）离散对数

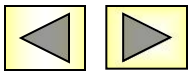
（3）大整数分解

（4）背包问题

（5）Diffie-Hellman问题

（6）二次剩余问题

（7）模n的平方根问题



§4.2 RSA公钥密码体制

欧拉函数：

设n>1若φ(n)表示比n小而与n互素的正整数的个数。则φ(n)为欧拉函数。

以n＝24为例，比24小而与24 互素的正整数为：1，5，7，11，13，17，19，23，因此，我们有φ(24)＝8。

性质：1）若p为素数，则φ(p)＝p－1。

2）若p为素数，则$\varphi(p^k)= p^{k-1}(p-1)$

3）若m与n互素，则φ(m×n)＝φ(m) ×φ(n)

4）若$n = P_1^{\alpha 1}P_2^{\alpha 2}\ldots P_t^{\alpha t}$，

则$\varphi(n)= n(1-\frac{1}{P_1})(1-\frac{1}{P_2})\ldots(1-\frac{1}{P_t})$

§4.2 RSA公钥密码体制

带余除法：

$\forall a \in Z > 0$，可找出两个唯一确定的整数q和r，使 $a = qm + r, 0 \le r < m$，q和r这两个数分别称为以m去除a所得到的商数和余数。(若$r = 0$则$m \mid a$）

§4.2 RSA公钥密码体制

欧几里德算法(Euclid)：

计算最大公约数gcd (a, b)，不需要对a, b分解因式。

方法：假设a>b

$a = b \times q_1 + r_1$

$b = r_1 \times q_2 + r_2$

$r_1 = r_2 \times q_3 + r_3$

。。。。。。

$r_{n-2} = r_{n-1} \times q_n + r_n$

$r_{n-1} = r_n \times q_{n+1} + r_{n+1}\ (r_{n+1} = 0)$

于是gcd (a, b)= r_n

§4.2 RSA公钥密码体制

例：求gcd (1547, 560)

解：$1547 = 2 \times 560 + 427$

$560 = 1 \times 427 + 133$

$427 = 3 \times 133 + 28$

$133 = 4 \times 28 + 21$

$28 = 1 \times 21 + 7$

$21 = 3 \times 7 + 0$

于是 gcd (1547, 560) = 7

§4.2 RSA公钥密码体制

RSA公钥密码算法描述

（1）设计密钥：

(a) 在离线方式下，先产生两个足够大的强质数p、q；

(b) 令n=p×q。计算欧拉函数ϕ(n)=(p-1) ×(q-1)；

(c) 选取一个与ϕ(n)互素的奇数e，称e为公开指数；

(d) 根据e×d=1 mod(ϕ(n))，找出d；

(e) 舍弃p和q（但绝不能泄露），公开(n，e)，公钥；

(f) 保密(n，d)，私钥。

§4.2 RSA公钥密码体制

（2）加密：

对于明文M，用公钥 (n，e) 加密可得到密文C。

$$C = M^e \mod (n)$$

（3）解密：

对于密文C，用私钥(n，d)解密可得到明文M。

$$M = C^d \mod (n)$$

当定义用私钥(n，d)先进行解密后，然后用公钥(n，e)进行加密，就是数字签名。

§4.2 RSA公钥密码体制

举例1：选取p=5, q=11，则n=pq =55，$\phi(n)=(p-1)(q-1)=40$

假设选取e=7；

由$d\times 7 = 1 \bmod 40$，计算出d = 23，

得到公开密钥：（n，e）=（55，7）

私有密钥：（n，d）=（55，23）

假定明文M转换为数字8。

则密文 $C = M^e \bmod n = 8^7 \bmod 55 = (8^2)^3\times 8 \bmod 55$

$= 9^3\times 8 \bmod 55 = 5832 \bmod 55 = 2$

恢复明文 $M = C^d \bmod n = 2^{23} \bmod 55 = (2^6)^3\times 2^5 \bmod 55$

$= 9^3\times 32 \bmod 55 = 26\times 9\times 32 \bmod 55$

$= 7488 \bmod 55 = 8$

§4.2 RSA公钥密码体制

举例2：设p=43，q=59，n=pq=43 × 59=2537，

ϕ(n)=(p-1)(q-1) =42 × 58 =2436， 取e=13，求d。

解方程 d × 13 ≡ 1 mod 2436（欧几里德算法）

2436=13 × 187+5　　5 =2436-13×187

13=2 × 5+3　　⟹　　3=13-2×5

5=3+2　　2=5-3

3=2+1　　1=3-2

1 = 3-2 = 3-(5-3) = 2×3-5 = 2 ×(13-2 × 5)-5 = 2 × 13-5 × 5

= 2 × 13-5 ×(2436-13 × 187) = 937 × 13-5 × 2436

即937 × 13≡1 mod 2436

于是取e=13时，d= 937

§4.2 RSA公钥密码体制

二、加密举例：若有明文public key encryptions

1、先将明文分块为两个一组(此处为简化计算考虑)：

pu bl ic ke ye nc ry pt io ns

2、将明文数字化令a,b…,z 分别为00,01,…,25 得

1520 0111 0802 1004 2404

1302 1724 1519 0814 1318

3、利用加密可得密文

0095 1648 1410 1299 1365

1379 2333 2132 1751 1324

4、解密后又得到明文

§4.2 RSA公钥密码体制

（2）加密

$C = M^e \bmod n = 1520^{13} \bmod 2537$

$= (1520^2)^6 * 1520 \bmod 2537$

$= (1730)^6 * 1520 \bmod 2537$

$= (1730^2)^3 * 1520 \bmod 2537$

$= (1777)^3 * 1520 \bmod 2537$

$= (1777)^2 * 1777 * 1520 \bmod 2537$

$= 1701 * (1777 * 1520) \bmod 2537$

$= 1701 * 1672 \bmod 2537$

= 95（密文）

§4.2 RSA公钥密码体制

（3）解密

$M = C^d \bmod n = 95^{937} \bmod 2537$

$= (95^2)^{468} * 95 \bmod 2537$

$= (1414)^{468} * 95 \bmod 2537$

$= (1414^2)^{234} * 95 \bmod 2537$

$= (240)^{234} * 95 \bmod 2537$

……

$= (625*25)*(341*788)*95 \bmod 2537$

$= 230*2323 \bmod 2537$

$= 1520 \bmod 2537 = 1520$（明文）

§4.2 RSA公钥密码体制

三、优点：

RSA算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA是被研究得最广泛的公钥算法，从提出到现在已近二十年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。该算法的加密密钥和加密算法分开，使得密钥分配更为方便。

它特别符合计算机网络环境。对于网上的大量用户，可以将加密密钥用电话簿的方式印出。如果某用户想与另一用户进行保密通信，只需从公钥簿上查出对方的加密密钥，用它对所传送的信息加密发出即可。对方收到信息后，用仅为自己所知的解密密钥将信息解密，了解报文的内容。

§4.2 RSA公钥密码体制

四、缺点：

（1）产生密钥很麻烦，受到素数产生技术的限制，而难以做到一次一密。

（2）RSA的安全性依赖于大数的因子分解，但并没有从理论上证明破译RSA的难度与大数分解难度等价。目前人们已能分解140多个十进制位的大素数，这就要求使用更长的密钥，速度更慢。而且目前人们正在积极寻找攻击RSA的方法。

（3）速度太慢，RSA的分组长度太大。为了速度问题，目前人们广泛使用单、公钥密码结合使用的方法，优缺点互补：单钥密码加密速度快，用它来加密较长的文件，然后用RSA来给文件密钥加密，极好的解决了单钥密码的密钥分发问题。