密 码 学

（第九讲）

公开密钥密码（1）

张焕国

武汉大学计算机学院

目　录

目　录

一、公开密钥密码体制的基本思想

1、传统密码的缺点：

①*收发双方持有相同密钥，密钥分配困难，网络环境更突出。*

$$K_e = K_d$$

②*不能方便地实现数字签名，商业等应用不方便。*

一、公开密钥密码体制的基本思想

2、公开密钥密码的基本思想：

①*将密钥K一分为二，一个专门加密，一个专门解密：$K_e \neq K_d$*

②*且由K_e不能计算出K_d，于是可将K_e公开，使密钥分配简单。*

③*由于$K_e \neq K_d$且由K_e不能计算出K_d，所以K_d便成为用户的指纹，于是可方便地实现数字签名。*

一、公开密钥密码体制的基本思想

3、公开密钥密码的基本条件：

①*E和D互逆；* *基本条件，保密条件*

$D(E(M))=M$

②$K_e \neq K_d$*且由*K_e*不能计算出*K_d *；安全条件*

③***E和D都高效。*** *实用条件*

④$E(D(M))=M$ *保真条件*

*如果满足①②③可保密，如果满足②③④可保真，如果4个条件都满足，**可同时保密保真。***

二、公开密钥密码的基本工作方式

- 设 M为明文，C为密文，E为公开密钥密码的加密算法，D为解密算法，K_e为公开的加密钥，K_d为保密的解密钥，每个用户都分配一对密钥，而且将所有用户的公开的加密钥K_e存入共享的密钥库$PKDB$。

A	K_{eA}
B	K_{eB}

$PKDB$

二、公开密钥密码的基本工作方式

1、确保数据秘密性：A $\xrightarrow{M}$ B

发方：

①A首先查**PKDB**，查到B的公开的加密钥K_{eB}。

②A用K_{eB} 加密M得到密文C： C=E（M，K_{eB}）

③A发C给B。

收方：

①B接受C。

②B用自己的K_{dB}解密，得到明文M=D(C，K_{dB})。

二、公开密钥密码的基本工作方式

1、确保数据秘密性：

安全性分析：

①只有B才有K_{dB}，因此只有B才能解密，所以确保了秘密性。

②任何人都可查**PKDB**得到A的K_{eA}，所以任何人都可冒充A给B发送数据。不能确保真实性。

二、公开密钥密码的基本工作方式

2、确保数据真实性：A $\xrightarrow{M}$ B

发方：

①A首先用自己的K_{dA}对M解密，得到C=D(M，K_{dA})。

②A发C给B。

收方：

①B接受C。

②B查**PKDB**查到A的公开的加密钥K_{eA}。

③B用K_{eA}加密C，得到明文M=E（C，K_{eA}）。

二、公开密钥密码的基本工作方式

2、确保数据秘密性：

安全性分析：

①只有A才有K_{dA} ，因此只有A才能解密产生C，所以确保了真实性。

②任何人都可查**PKDB**得到A的K_{eA}，所以任何人都可加密得到明文。不能确保秘密性。

二、公开密钥密码的基本工作方式

3、同时确保数据秘密性和真实性：A $\xrightarrow{M}$ B

发方：

①A首先用自己的K_{dA}对M解密，得到S：

$S=D(M, K_{dA})$

②查**PKDB**，查到B的公开的加密钥K_{eB}。

③用K_{eB} 加密S得到C：

$C=E(S, K_{eB})$

④A发C给B。

二、公开密钥密码的基本工作方式

3、同时确保数据秘密性和真实性：

收方：

①B接受C。

②B用自己的K_{dB}解密C，得到S：

$S=D\ (C,\ K_{dB})$

③B查**PKDB**查到A的公开的加密钥K_{eA}。

④B用A的公开的加密钥K_{eA} 加密S，得到M：

$M=E\ (S,\ K_{eA})$

二、公开密钥密码的基本工作方式

3、同时确保数据秘密性和真实性：

安全性分析：

①只有A才有K_{dA}，因此只有A才能解密产生S，所以确保了真实性。

②只有B才有K_{dB}，因此只有B才能获得明文，所以确保了秘密性。

三、RSA公开密钥密码

- 1978年美国麻省理工学院的三名密码学者R.L.Rivest,A.Shamir和L.Adleman提出了一种基于大合数因子分解困难性的公开密钥密码，简称为RSA密码。
- RSA密码被誉为是一种风格幽雅的公开密钥密码。既可用于加密，又可用于数字签名，安全、易懂。
- RSA密码已成为目前应用最广泛的公开密钥密码。

三、RSA公开密钥密码

1、加解密算法

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随机地选取一个正整数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；

⑥加密运算：$C=M^e \bmod n$

⑦解密运算：$M=C^d \bmod n$

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

要证明：D(E(M))=M

$$M = C^d = (M^e)^d = M^{ed} \mod n$$

因为$ed = 1 \mod \phi(n)$，这说明$ed = t\phi(n)+1$,其中t为某整数。所以，

$$M^{ed} = M^{t\phi(n)+1} \mod n \text{ 。}$$

因此要证明 $M^{ed} = M \mod n$，只需证明

$$M^{t\phi(n)+1} = M \mod n \text{ 。}$$

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

在（M，n）＝1的情况下，根据数论(Euler定理)，

$$M^{t\Phi(n)} = 1 \mod n ,$$

于是有，

$$M^{t\Phi(n)+1} = M \mod n 。$$

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

在（M，n）≠1的情况下，分两种情况：

第一种情况：M∈{1,2,3,...,n-1}

因为n=pq，p和q为素数，

M∈{1,2,3,...,n-1}，且（M，n）≠1 。

这说明M必含p或q之一为其因子，而且不能同时包含两者，否则将有M≥n，与M∈{1,2,3,...,n-1}矛盾。

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

不妨设M＝ap 。

又因q为素数，且M不包含q，故有（M，q）＝1，
于是有，$M^{\Phi(q)} = 1 \mod q$ 。

进一步有，$M^{t(p-1)\Phi(q)} = 1 \mod q$。

因为q是素数，Φ(q)＝（q-1），所以t(p-1)Φ(q)
＝tΦ(n)，所以有

$$M^{t\Phi(n)} = 1 \mod q。$$

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

于是，$M^{t\Phi(n)} = bq+1$，其中b为某整数。

两边同乘M，

$$M^{t\Phi(n)+1} = bqM+M \text{ 。}$$

因为$M = ap$，故

$$M^{t\Phi(n)+1} = bqap+M = abn+M \text{ 。}$$

取模n得，

$$M^{\Phi(n)+1} = M \mod n \text{ 。}$$

三、RSA公开密钥密码

2、算法论证

① *E和D的可逆性*

在（M，n）≠1的情况下，分两种情况：

第二种情况：M＝0

当M＝0时，直接验证，可知命题成立。

三、RSA公开密钥密码

2、算法论证

②*加密和解密运算的可交换性*

$D(E(M))=(M^e)^d=M^{ed}=(M^d)^e=E(D(M)) \mod n$

所以，RSA密码可同时确保数据的秘密性和数据的真实性。

③*加解密算法的有效性*

RSA密码的加解密运算是模幂运算，有比较有效的算法。

三、RSA公开密钥密码

2、算法论证

④*在计算上由公开密钥不能求出解密钥*

小合数的因子分解是容易的，然而大合数的因子分解却是十分困难的。关于大合数的因子分解的时间复杂度下限目前尚没有一般的结果，迄今为止的各种因子分解算法提示人们这一时间下限将不低于O（EXP（lnNlnlnN）$^{1/2}$）。根据这一结论，只要合数足够大，进行因子分解是相当困难的。

三、RSA公开密钥密码

2、算法论证

④*在计算上由公开密钥不能求出解密钥*

假设截获密文C，从中求出明文M。他知道

$$M \equiv C^d \mod n ,$$

因为n是公开的，要从C中求出明文M，必须先求出d，而d是保密的。但他知道，

$$ed \equiv 1 \mod \Phi(n),$$

e是公开的，要从中求出d，必须先求出$\Phi(n)$，而$\Phi(n)$是保密的。

三、RSA公开密钥密码

2、算法论证

④*在计算上由公开密钥不能求出解密钥*

但他又知道，

$$\Phi(n)=(p-1)(q-1),$$

要从中求出$\Phi(n)$，必须先求出p和q，而p和q是保密的。但他知道，

$$n=pq,$$

要从n求出p和q，只有对n进行因子分解。而当n足够大时，这是很困难的。

三、RSA公开密钥密码

2、算法论证

④*在计算上由公开密钥不能求出解密钥*

只要能对n进行因子分解，便可攻破RSA密码。由此可以得出，*破译RSA密码的困难性≤对n因子分解的困难性。*目前尚不能证明两者是否能确切相等，因为不能确知除了对n进行因子分解的方法外，是否还有别的更简捷的破译方法。

目前只有Rabin密码具有：

破译Rabin密码的困难性=对n因子分解的困难性。

四、RSA密码的实现

1、参数选择

为了确保RSA密码的安全，必须认真选择密码参数：

① *p和q要足够大；*

一般应用：p和q应 512 b　重要应用：p和q应 1024 b

②*p和q应为强素数*

文献指出，只要(p-1)、(p+1)、(q-1)、(q+1)四个数之一只有小的素因子，n就容易分解。

③ *p和q的差要大；*

四、RSA密码的实现

1、参数选择

④ *(p-1）和（q-1）的最大公因子要小。*

如果（ p-1）和（q-1）的最大公因子太大，则易受迭代加密攻击。

⑤ *e的选择*

随机且含1多就安全，但加密速度慢。于是，有的学者建议取e＝2^{16}+1＝65537

⑥ *d的选择*

d不能太小，要足够大

⑦ *不要许多用户共用一个模 n；易受共模攻击*

四、RSA密码的实现

2、大素数的产生

①概率产生

目前最常用的概率性算法是Miller检验算法。Miller检验算法已经成为美国的国家标准。

②确定性产生

- *确定性测试*
- *确定性构造*

四、RSA密码的实现

3、大素数的运算

①快速乘方算法

- *反复平方乘算法：*

设e的二进制表示为

$$e = e_{k-1}\ 2^{k-1} + e_{k-2}\ 2^{k-2} + \ldots, + e_1\ 2^1 + e_0$$

则 $M^e = ((\ldots(M^{e_{k-1}})^2\ M^{e_{k-2}})^2 \ldots M^{e1})^2\ M^{e_0} \bmod n$

- *设e为k位二进制数，w(e)为e的二进制系数中为1的个数，则最多只需要计算w(e）-1次平方和w(e)次数的模乘。从而大大简化了计算。*

四、RSA密码的实现

3、大素数的运算

②快速模乘算法

- *反复平方乘算法解决了快速乘方取模的问题，仍未解决快速模乘的问题；*
- *Montgomery算法是一种快速模乘的好算法；*
- *将以上两种算法结合成为实现RSA密码的有效方法。*
- *硬件协处理器是提高运算效率的有效方法。*

四、RSA密码的实现

3、大素数的运算

- *Montgomery算法的思路：*
  - *要计算 $Y=AB \mod n$,因为n很大，取模运算困难，采取一个小的模R，回避大模的计算。*
  - *利用空间换时间，多用存储空间换取快速。*
  - 缺点：*不能直接计算出 $Y=AB \mod n$ ，只能计算出中间值 $ABR^{-1} \mod n$ ，因此还需要预处理和调整运算。一次性计算$Y=AB \mod n$并不划算。*
  - 适合：*RSA等密码中多次的模乘计算。*

习 题

① 证明RSA密码加解密算法的可逆性

② 证明RSA密码加解密算法的可交换性

③ 说明对于RSA密码从公开加密钥不能求出保密的解密钥

④ 令$p=3, q=11, d=7, m=5$, 手算密文C。

⑤ 设RSA密码的$e=31, n=35, C=10$, 手算明文M。

习 题

⑥设A，B为正整数，D=(A,B)。试证明：
$\phi(AB)=D\,\phi(A)\,\phi(B)/\,\phi(D)$

⑦ *RSA密码的快速运算*

- *分析反复平方乘算法的效率*
- *说明Montgomery算法为什么效率高？它适合哪些情况下应用？*

⑧*编程实现RSA密码的加解密运算。*

⑨ *在RSA中使用e=3作为加密指数有和优缺点？使用d=3作解密指数的做法好吗？为什么？*

习 题

① 证明RSA密码加解密算法的可逆性

② 证明RSA密码加解密算法的可交换性

③ 说明对于RSA密码从公开加密钥不能求出保密的解密钥

④ 令$p=3, q=11, d=7, m=5$, 手算密文C。

⑤ 设RSA密码的$e=31, n=35, C=10$, 手算明文M。

习 题

⑥设A，B为正整数，D=(A,B)。试证明： $\phi(AB)=D\,\phi(A)\,\phi(B)/\phi(D)$

⑦*RSA密码的快速运算*

- *分析反复平方乘算法的效率*
- *说明Montgomery算法为什么效率高？它适合哪些情况下应用？*

⑧*编程实现RSA密码的加解密运算。*

⑨ *在RSA中使用e=3作为加密指数有和优缺点？使用d=3作解密指数的做法好吗？为什么？*


谢 谢！