信息安全研究所

密码学

第十讲　公钥密码基础

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室

目 录

武漢大學

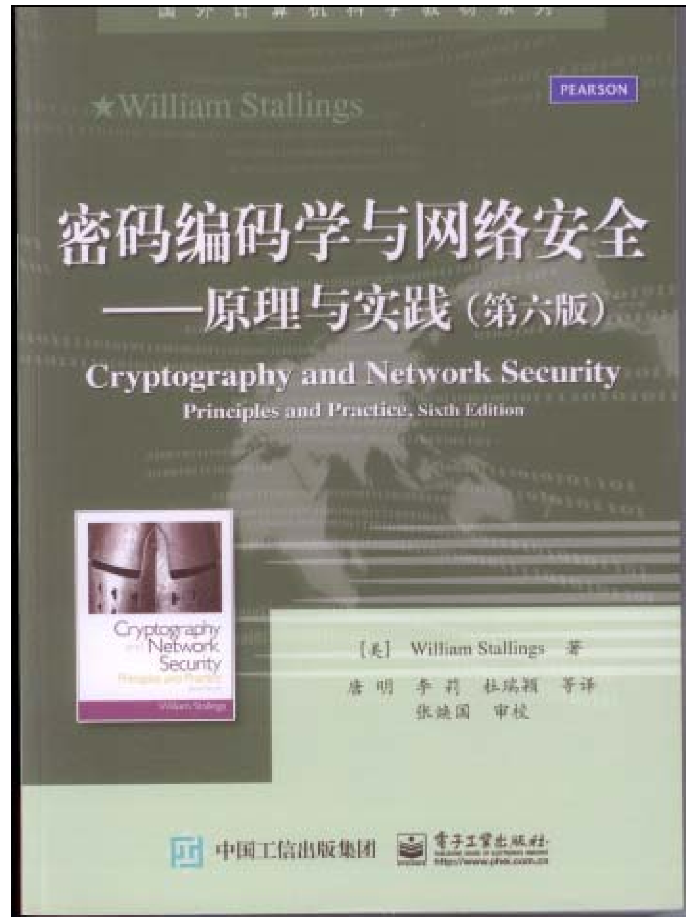
目 录

武漢大學

教材与主要参考书

教材

参考书



本讲内容

一、公钥密码的基本思想

二、公钥密码的基本工作方式

三、RSA密码

四、离散对数问题

五、EIGamal密码

一、公钥密码的基本思想

1、传统密码的优缺点：

①优点

- 理论与实践都很成熟。
- 安全容易把握。
- 加解密速度快。

②缺点

- 收发双方持有相同密钥， $K_e = K_d$ ，密钥分配困难，网络环境更突出。
- 不能方便地实现数字签名，商业等应用不方便。

一、公钥密码的基本思想

2、公开密钥密码的基本思想：

①将密钥 K 一分为二：K_e 和 K_d 。K_e 专门加密， K_d 专门解密， $K_e \neq K_d$ 。

②由 K_e 不能计算出 K_d ，于是可将 K_e 公开，使密钥 K_e 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。

- 称上述密码为公开密钥密码，简称为公钥密码。

一、公钥密码的基本思想

3、公开密钥密码的基本条件：

①*E*和 *D*互逆；——————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可用于保密，如果满足②③④可用于保真，如果4个条件都满足，可同时用于保密和保真。
- 注意：条件④是保真的一个充分条件，不是必要条件。

一、公钥密码的基本思想

4、公钥密码的理论模型

(1)单向函数

设函数 $y=f(x)$，如果满足以下两个条件，则称为单向函数：

① 如果对于给定的 x，要计算出 $y=f(x)$很容易；

② 而对于给定的 y，要计算出 $x=f^{-1}(y)$很难。

(2)利用单向函数构造密码

- 用正变换作加密，加密效率高；
- 用逆变换作解密，安全，敌手不可破译；
- 但是合法收信者也无法解密。

一、公钥密码的基本思想

(3) 单向陷门函数

设函数 $y=f(x)$，且 f 具有陷门，如果满足以下两个条件，则称为单向陷门函数：

① 如果对于给定的 x，要计算出 $y=f(x)$ 很容易；

② 而对于给定的 y，如果不掌握陷门要计算出 $x=f^{-1}(y)$ 很难，而如果掌握陷门要计算出 $x=f^{-1}(y)$ 就很容易。

(4) 利用单向陷门函数构造密码

① 用正变换作加密，加密效率高；

② 用逆变换作解密，安全；

③ 把陷门信息作为密钥，且只分配给合法用户。确保合法用户能够方便地解密，而非法用户不能破译。

一、公钥密码的基本思想

(5)单向函数的研究现状

- 理论上：尚不能证明单向函数一定存在；
- 实际上：密码学认为只要函数单向性足够应用就行了；
- 已找到一些单向性足够的函数：

①大合数的因子分解问题

大素数的乘积容易计算（$p \times q \Rightarrow n$），而大合数的因子分解困难($n \Rightarrow p \times q$)。

②有限域上的离散对数问题

有限域上大素数的幂乘容易计算（$a^b \Rightarrow c$），而对数计算困难($\log_a c \Rightarrow b$)。

③椭圆曲线离散对数问题

设d是正整数，G是解点群的基点，计算$dG=Q$是容易的，而由Q求出d是困难的。

二、公钥密码的基本工作方式

- 设M为明文，C为密文，E为加密算法，D为解密算法。
- 每个用户都配置一对密钥:K_e为公开的加密钥，K_d为保密的解密钥。
- 将所有用户的公开的加密钥K_e存入共享的密钥库**PKDB**。
- 保密的解密钥K_d由用户妥善保管。

PKDB

A	K_{eA}
B	K_{eB}

武漢大學

二、公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接收C。

②B用自己的K_{dB}解密，得到明文$M=D(C, K_{dB})=D(E(M, K_{eB}), K_{dB})$。

二、公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，所以确保了数据的秘密性。

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

二、公钥密码的基本工作方式

2、确保数据真实性： $\mathbf{A} \xrightarrow{M} \mathbf{B}$

发方：

①A首先用自己的K_{dA}对M解密，得到C=D(M，K_{dA})。

② A发C给B。

收方：

①B接收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}）

=E（D(M，K_{dA})，K_{eA}）。

二、公钥密码的基本工作方式

2、确保数据真实性：

安全性分析：

①只有A才有K_{dA}，因此只有A才能解密产生C，所以确保了数据的真实性。

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。不能确保数据的秘密性。

二、公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：

① A首先用自己的K_{dA}对M解密，得到S：

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

② A查PKDB，查到B的公开的加密钥K_{eB}。

③ A用K_{eB}加密S得到C：

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

④A发C给B。

二、公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接收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，所以确保了数据的真实性。

②只有B才有K_{dB}，因此只有B才能获得明文，所以确保了数据的秘密性。

三、RSA公钥密码

- 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之一。

三、RSA公钥密码

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 $\phi(n)=(p-1)(q-1)$，对 $\phi(n)$保密；

④随机地选取一个正整数e，$1< e <\phi(n)$且（e ，$\phi(n)$）$=1$，将 e 公开；

⑤根据 $ed=1 \mod \phi(n)$，求出d，并对d 保密；

⑥加密运算：$C=M^e \mod n$

⑦解密运算：$M=C^d \mod n$

● 公开加密钥$K_e= <e,n>$，保密解密钥$K_d = <p,q,d, \phi(n)>$

武漢大學

三、RSA公钥密码

2、算法论证

① *E*和*D*的可逆性

要证明： $D(E(M))=M$

即要证明： $M = C^d = (M^e)^d = M^{ed} \bmod n$

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

$$M^{ed} = M^{t\phi(n)+1} \bmod n 。$$

因此要证明 $M^{ed} = M \bmod n$，只需证明

$$M^{t\phi(n)+1} = M \bmod n 。$$

武漢大學

三、RSA公钥密码

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)，

$$M^{t\phi(n)} = 1 \bmod n \text{，}$$

于是有，

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

三、RSA公钥密码

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＝0

当M＝0时，直接验证，可知命题成立。

注意：因为是mod n运算，所以$M \in \{0,1,2,3,\ldots,n\text{-}1\}$

第二种情况： $M \neq 0$ ，$M \in \{1,2,3,\ldots,n\text{-}1\}$

因为n=pq，p和q为素数， $M \in \{1,2,3,\ldots,n\text{-}1\}$，且（$M$，$n$）≠1 。

这说明M必含p或q之一为其因子，且不能同时包含两者，否则将有$M \geq n$，与$M \in \{1,2,3,\ldots,n\text{-}1\}$矛盾。

三、RSA公钥密码

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，$M^{\phi(q)}=1 \bmod q$ 。

进一步有，$M^{t(p-1)\phi(q)}=1 \bmod q$。

因为q是素数，$\phi(q)=(q-1)$，所以$t(p-1)\phi(q)=t\phi(n)$，所以有

$$M^{t\phi(n)}=1 \bmod q。$$

武漢大學

三、RSA公钥密码

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，

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

武漢大學

三、RSA公钥密码

2、算法论证

②加密和解密运算的可交换性

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

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，运算是比较有效的。

三、RSA公钥密码

2、算法论证

④在计算上由公开的加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

$$O（EXP（\ln N \ln\ln N）^{1/2}）。$$

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公钥密码

2、算法论证

④在计算上由公开的加密钥不能求出解密钥

假设攻击者截获了密文*C*，想求出明文*M*。他知道

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

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，

$$ed \equiv 1 \bmod \phi(n),$$

*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公钥密码

2、算法论证

④在计算上由公开的加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。

四、离散对数问题

- 离散对数问题是目前已知的良好的单向函数
- 离散对数问题是许多密码的安全基础

①设p为素数，则模p的余数构成有限域：

$$F_p = GF(p) = \{0,1,2,\ldots,p-1\}$$

F_p的非零元素构成乘法循环群F_p^*

$$F_p^* = \{1,2,\ldots,p-1\}$$
$$= \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p-1}\},$$

则称 α 为F_p^*的生成元或模 p 的本原元。

②求 α 的摸幂运算为：

$$y = \alpha^x \bmod p，1 \leqslant x \leqslant p-1,$$

四、离散对数问题

③求对数 x 的运算为

$$x=\log_{\alpha} y，1 \leqslant x \leqslant p-1$$

由于上述运算是定义在有限域F_p 上的，所以称为离散对数运算。

- 从x计算y是容易的。可是从y计算x就困难得多，利用目前最好的算法，对于认真选择的p将至少需用$O(p^{1/2})$次以上的运算，只要p足够大，求解离散对数问题是相当困难的。

武漢大學

五、ElGamal公钥密码

- 准备：随机地选择一个大素数p，且要求p-1有大素数因子。再选择一个模p的本原元 α 。将p和 α 公开作为密码的基础参数。

(1) 密钥生成

- 用户随机地选择一个整数d作为自己保密的解密钥，$2 \leqslant d \leqslant p-2$ 。
- 用户计算$y = \alpha^d \bmod p$，并取y为自己公开的加密钥。
- 显然，由公开钥y 计算秘密钥d，必须求解离散对数，而这是极困难的。

五、ElGamal公钥密码

(2) 加密

- 将明文消息M（$0 \leqslant M \leqslant p-1$)加密成密文的过程如下：

①随机地选取一个整数k，$2 \leqslant k \leqslant p-2$。

②计算： $U = y^{k} \bmod p$;

$$C_1 = \alpha^{k} \bmod p;$$

$$C_2 = UM \bmod p;$$

③取 $C =$（C_1，C_2）作为的密文。

五、ElGamal公钥密码

(3) 解密

● 将密文（C_1，C_2）解密的过程如下：

①计算$V = C_1^{\,d} \bmod p$

②计算

$$M = C_2 V^{-1} \bmod p$$

获得明文。

五、ElGamal公钥密码

- 解密的可还原性证明如下：

$$
\begin{aligned}
C_2 V^{-1} \bmod p &= (UM)V^{-1} \bmod p \\
&= UM(C_1^{\,d})^{-1} \bmod p \\
&= UM((\alpha^k)^d)^{-1} \bmod p \\
&= UM((\alpha^d)^k)^{-1} \bmod p \\
&= UM((y)^k)^{-1} \bmod p \\
&= UM(U)^{-1} \bmod p \\
&= M \bmod p
\end{aligned}
$$

五、ElGamal公钥密码

(4) 安全性

- 由于ElGamal密码的安全性建立在GF（p）离散对数的困难性之上，而目前尚无求解GF（p）离散对数的有效算法，所以在p足够大时ElGamal密码是安全的。
- 为了安全p应为150位以上的十进制数，而且p-1应有大素因子。
- d和k都不能太小。
- 为了安全加密和签名所使用的k必须是一次性的。

五、ElGamal公钥密码

(4) 安全性

- 如果 k不是一次性的，时间长了就可能被攻击着获得。又因y是公开密钥，攻击者自然知道。于是攻击者就可以根据$U=y^k \bmod p$ 计算出U，进而利用**Euclid**算法求出U^{-1}。又因为攻击者可以获得密文C_2，于是可根据式$C_2=UM \bmod p$ 通过计算$U^{-1}C_2$得到明文M。
- 设用同一个k加密两个不同的明文M和M'，相应的密文为（C_1，C_2）和（C_1'，C_2'）。因为$C_2/C_2'=M/M'$，如果攻击者知道M'，则很容易求出M。

五、ElGamal公钥密码

(5) ElGamal密码的应用

- 由于ElGamal密码的安全性得到世界公认，所以得到广泛的应用。
  - 著名的美国数字签名标准DSS，采用了ElGamal密码的一种变形。
  - 电子邮件标准S/MIME采用了ElGamal密码。
  - 俄罗斯的数字签名标准也是ElGamal密码的一种变形，而且数据规模选得更大。
- 为了适应不同的应用，人们在应用中总结出18种不同的ElGamal密码的变形。

五、ElGamal公钥密码

(5) ElGamal密码的应用

①加解密速度快

由于实际应用时ElGamal密码运算的素数p比RSA要小，所以ElGamal密码的加解密速度比RSA快。

②随机数源

由ElGamal密码的解密钥d和随机数k都应是高质量的随机数。因此，应用ElGamal密码需要一个好的随机数源，也就是说能够快速地产生高质量的随机数。

③大素数的选择

为了ElGamal密码的安全，p应为150位（十进制数）以上的大素数，而且p-1应有大素因子。

五、ElGamal公钥密码

⑹ ElGamal密码的实现技术

1、大素数的产生

①概率性产生

- 前最常用的概率性算法是；随机产生一个整数，进行Miller检验。如果不能通过检验，则肯定不是素数。如果通过检验，则是素数的改概率足够大。
- 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：一个整数 经过测试后，可确定是否是素数。
- 确定性构造：利用已知小素数，构造大素数。

五、ElGamal公钥密码

2、大数的运算

①快速乘方算法

● 反复平方乘算法：计算M^e

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 $M^e = ((\ldots(M^{e_{k-1}})^2 M^{e_{k-2}})^2 \ldots M^{e_1})^2 M^{e_0} \bmod n$

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。

五、ElGamal公钥密码

2、大数的运算

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，仍未完全解决快速模乘的问题；
- **Montgomery**算法是一种快速模乘的好算法；
- 教材中给出了一个基本**Montgomery**算法，目前已有多种改进算法，其效率更高。
- 将以上两种算法结合成为实现**EIGamal**密码的有效方法。

五、ElGamal公钥密码

2、大数的运算

- **Montgomery算法的思路：**
  - 要计算 $Y=AB \bmod n$,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。
  - 应用空间换时间的策略，多用存储空间换取快速。
  - 缺点：不能直接计算出 $Y=AB \bmod n$ ，只能计算出中间值 $ABR^{-1} \bmod n$ ，因此还需要预处理和调整运算。一次性计算$Y=AB \bmod n$并不划算。
  - 适合：ElGamal等密码中的多次模乘计算。

谢　谢！