第3章 一次同余方程

3.3密码学中的应用

密码学的基本概念

密码学包括密码编码学和密码分析学. **密码编码学**是研究把消息变换成秘密信息的方法. 需要变换的消息称为**明文**, 变换所得到的秘密信息称为**密文**；**密码分析学**是研究破译密文的方法.

密码学的基本概念

如图3-1所示, 一个密码算法通常由5个部分构成: ①明文空间（全体明文的集合）；②密文空间（全体密文的集合）；③密钥空间（全体密钥的集合）；④加密变换（算法）；⑤解密变换（算法）.

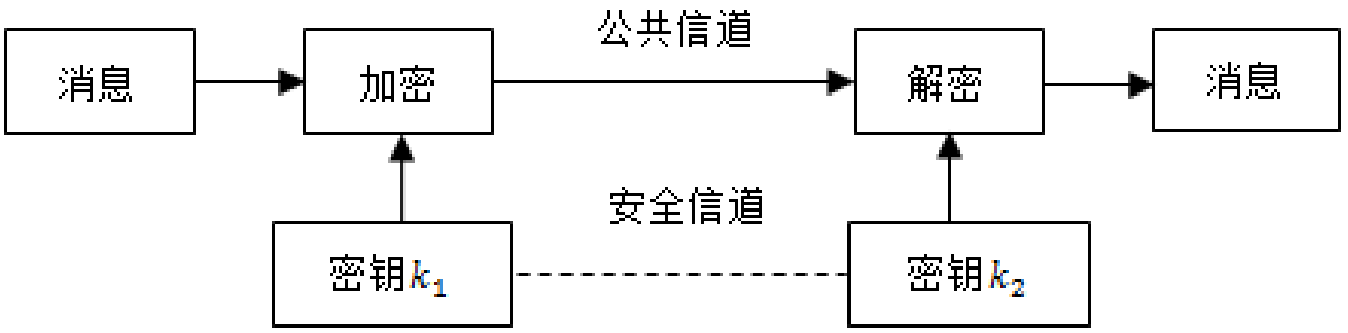

图 3-1　保密通信示意图

密码学的基本概念

如果一个密码算法的加密密钥和解密密钥相同, 或者容易从其中一个推导出另一个, 称为**对称密码算法**. 对称密码算法需要一个安全信道来传输共享的加密（解密）的密钥.

如果一个密码算法的加密密钥和解密密钥不同, 密码分析者不能从一个加密密钥计算出解密密钥, 称为**公钥密码算法**, 或者非对称密码算法. 非对称密码算法（公钥密码算法）不需要安全信道来传输共享的加密和解密的密钥. 非对称算法的加密密钥公开, 解密密钥保密.

故在图3-1中的密钥k_1和k_2可能相同, 也可能不同. 安全信道标为虚线表示不是一定必要的. 对称密码算法需要安全信道来传输密钥, 非对称密码算法则不需要.

仿射密码

仿射密码是一种对称密码算法.

记$Z_{26} = \{0, 1, 2, 3, \ldots, 25\}$分别对应26个字母, 也即模26的最小非负完全剩余系. 即字母a对应集合中的0, b对应1, ……, z对应25. 这里的字母不分大小写. 选择整数k, 要求$(k, b) = 1$, 那么$k = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$之一. 再选择$b \in Z_{26}$. 一起组成密钥$(k, b)$.

设p为要加密的明文字母，仿射密码的加密变换为:
$c \equiv kp + b \pmod{26}$. 解密变换:
$p = k^{-1}(c - b) \pmod{26}$. 其中: k^{-1}是k模26的逆元, 即
$k^{-1} \times k \equiv 1 \pmod{26}$.

【例3.3.1】 选定(k, b)为(7, 3), 那么加密变换为
$c \equiv 7p + 3 \pmod{26}$.

加密明文: *hot*.

首先转化这三个字母分别为数字7, 14和19. 然后加密:

$$7\begin{bmatrix}7\\14\\19\end{bmatrix}+\begin{bmatrix}3\\3\\3\end{bmatrix}\equiv\begin{bmatrix}0\\23\\6\end{bmatrix}(\mathrm{mod}\,26);$$

故明文*hot*对应的密文串为: *axg*.

由于$7 \times 15 (\mathrm{mod}\, 26) \equiv 1$，故$7^{-1} (\mathrm{mod}\, 26) = 15$，故解密变换为：

$$p = 15 \times (c - 3) (\mathrm{mod}\, 26)$$

故解密过程为：

$$15\left(\begin{bmatrix} 0 \\ 23 \\ 6 \end{bmatrix} - \begin{bmatrix} 3 \\ 3 \\ 3 \end{bmatrix}\right) \equiv \begin{bmatrix} -45 \\ 300 \\ 45 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 14 \\ 19 \end{bmatrix} (\mathrm{mod}\, 26)$$

故解密得到的明文为*hot.*

【例3.3.2】 若选用仿射变换加密，字母H加密后对应字母A, 字母T加密后对应字母G, 求用于加密的参数(k, b).

解: 加密变换为$c \equiv kp + b \pmod{26}$, H的字母序为7, A的字母序为0, T的字母序为19, G的字母序为6, 代入相应的数值得:

$$\begin{cases} 0 \equiv 7k + b \pmod{26} \\ 6 \equiv 19\mathrm{k} + b \pmod{26} \end{cases}.$$

两式相减得

$$6 \equiv 12k \pmod{26}.$$

由于(12,26)|6, 方程有解.

首先解方程

$6k \equiv 1 \pmod{13}$.

由欧几里德算法可得, $k \equiv 11 \pmod{13}$.

实际上, 由于数值很小, 很容易看出1=13-6×2, 两边模13得$k \equiv -2 \pmod{13}$.

写出方程$ax \equiv b \pmod{m}$的全部解.

$x \equiv \frac{b}{(a,m)} x_0 + \frac{m}{(a,m)} t \pmod{m}, t = 0,1,2, \ldots, (a,m) - 1$.

故方程

$$6 \equiv 12k \pmod{26}$$

的所有解为

$$k \equiv 11 \times \frac{6}{(12,26)} + \frac{26}{(12,26)} t \pmod{26},\ t = 0,1.$$

即$k = 7 + 13t \pmod{26}, t = 0,1.$

即$k = 7, 20.$

注意到放射密码要求k与26互素, 故$k = 7$, 代入原方程得$b = 3.$

3.3.3 RSA公钥密码算法

第二次世界大战中, 德军的对称加密设备Enigma提供了强大的消息保密功能. 但如何把加密使用的密钥分发到各个作战部队和潜艇等一直困扰着密码学家们. 其他国家的密码学家面临同样的问题. 直到1976年, RSA算法的出现很好地解决了这个问题.

RSA算法是目前最有影响力的非对称加密算法之一. 现有的对称密码算法如AES、国密算法SM4等实现了对消息的保密功能, 但如何把加密时使用的密钥安全地发送给消息接收者, 主要还是使用RSA等公钥密码算法.

RSA算法是公钥密码算法. 也即是说，该算法的加密密钥和解密密钥是不同的，其中加密密钥是公开的，任何人都可以得到；解密密钥是保密的，仅有消息接收者知道. 该算法能够抵御已知的密码攻击方法, 已被ISO推荐为公钥数据加密标准.

【人物传记】1976年, Diffie和Hellman提出了一个革命性的密码系统, 称为公钥密码系统. 他们提出了这个系统的概念和思想, 也提出了一个密钥交换算法: DH密钥交换算法. 该算法不能用于加密. 1978年, Ron Rivest, Adi Shamir和Leonard Adleman三人提出了一个实际可行的公钥密码算法: RSA算法, 该算法能实现对消息加密, 也可以用于数字签名. RSA是三位设计者的首字母, 他们获得了2002年的图灵奖.

下面描述RSA算法的密钥产生及加密解密过程.

（1）密钥产生

① 选择两个大素数p和q, 计算$n = p \times q, \varphi(n) = (p-1) \times (q-1)$, 其中$\varphi(n)$是$n$的欧拉函数值.

② 选一个整数e, 满足$1 < e < \varphi(n)$, 且$gcd(\varphi(n), e) = 1$. 通过$d \times e \equiv 1 (mod \varphi(n))$, 计算出$d$.

③ 以$\{e, n\}$为公开密钥, $\{d, n\}$为秘密密钥.

假设Bob是秘密消息的接收方, 则只有Bob知道秘密密钥$\{d, n\}$, 所有人都可以知道公开密钥$\{e, n\}$.

2．加密

如果需要保密的消息为m, 选择Bob的公钥$\{e, n\}$, 计算: $c \equiv m^e \pmod{n}$, 然后把密文c发送给Bob.

3．解密

接收方Bob收到密文c, 计算: $m \equiv c^d \pmod{n}$.

所得结果m即为发送方欲发送的消息.

由RSA的算法描述可知, 密码分析者知道加密所使用的公开密钥$\{e, n\}$. 他想要得到解密用的密钥, 可以通过分解$n = p \times q$, 从而得到n的欧拉函数$\varphi(n)$,

在RSA算法的加密和解密阶段, 其计算量主要集中在大数的模幂运算,使用前面介绍的模重复平方法或平方乘算法, 能有效的降低计算量.

把该算法放入保密通信模型中, 可以有如图3-2所示的保密通信示意图.

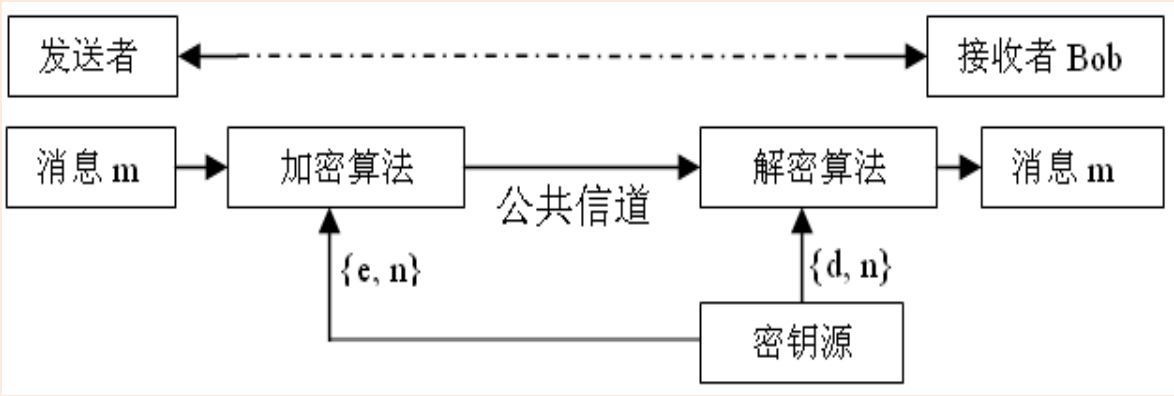

图3-2 密码算法RSA示意图

【例3.3.3】 在RSA算法密钥产生过程中，设选择的两个素数$p=13$，$q=23$，取加密时的参数$e=17$.（1）求解密时的参数d；（2）假设消息发送者欲发送的消息为$m=17$，计算对应的密文；（3）密码分析者在整个通信过程可以直接获得哪些数据？给出参数和对应的数值.

解：（1）$\varphi(n) = (p-1)\times(q-1) = 12\times 22 = 264$

由欧几里德算法得

264=17×15+9

17=9+8

9=8+1

再逐步回代得

1=9-8=9-(17-9)=9×2-17=(264-17×15)×2-17=264×2-17×31

等式两端模264得 $d \equiv -31 \equiv 233(\mathrm{mod}\,264)$

（2）$n = p \times q = 13 \times 23 = 299$

消息为$m = 17$对应的密文为

$c \equiv m^e \pmod{n} \equiv 17^{17} \pmod{299}$

用模重复平方的思想，$17^{17} \pmod{299}$

$$\equiv 17^{16} \times 17 \pmod{299}$$

逐步计算得$17^2 \pmod{299} \equiv -10, 17^4 \pmod{299} \equiv 100,$

$17^8 \pmod{299} \equiv 133, 17^{16} \pmod{299} \equiv 48.$

故 $c = 17^{17} \pmod{299} \equiv 48 \times 17 \pmod{299} \equiv 218$

容易验证 $218^{233} \pmod{299} \equiv 17.$

（3）在公钥密码算法中，密码分析者知道消息的接收方的公钥$\{e,n\}$, 以及加密消息在传输信道上的密文c. 在本例中，密码分析者可以直接获得的数据有$e=17, n=299, c=218.$

下面通过【例3.3.4】和【例3.3.5】证明密文接收者通过解密计算得到的数值等于发送方加密的消息.

【例3.3.4】 设p, q是两个不同的奇素数, $n = pq$, a是与n互素的整数. 令整数e满足$1 < e < \varphi(n)$且$(e, \varphi(n)) = 1$, 存在正整数d, 使得

$$ed \equiv 1(\mathrm{mod}\,\varphi(n)), 1 < d < \varphi(n).$$

而且, 对于整数$c \equiv a^e(\mathrm{mod}\,n)$, $(1 \leq c < n)$, 有

$$c^d \equiv a(\mathrm{mod}\,n).$$

证明: 因$(e,\varphi(n))=1$, 故满足$ed\equiv 1(\mathrm{mod}\,\varphi(n))$ 的d存在.

即存在正整数k, 使$ed=1+k\varphi(n)$.

由欧拉定理知 $a^{\varphi(p)}\equiv 1(\mathrm{mod}\,p)$, 所以

$a^{ed}\equiv a^{1+k\varphi(n)}\equiv a^{1+k\varphi(p)\varphi(q)}\equiv a(a^{\varphi(p)})^{k\varphi(q)}\equiv a(mod\,p)$.

同理可得 $a^{ed}\equiv a(mod\,q)$.

从而 $a^{ed}\equiv a(mod\,n)$.

即 $c^{d}\equiv a^{ed}\equiv a(mod\,n)$.

【例3.3.5】 设p,q是两个不同的奇素数, $n=pq$, 且设整数e,d满足

$ed \equiv 1(\mathrm{mod}\,\varphi(n)), 1<d<\varphi(n).$

那么, 对于整数$c \equiv a^e(\mathrm{mod}\,n)$, $(1 \leq c<n)$, 有$c^d \equiv a(\mathrm{mod}\,n)$. 其中$a$为任意整数. 即$a$是与$n$不一定互素的整数.

证明: 设$(a,n)=1$, 由【例3.3.4】知结论成立.

若$(a,n)=n$, 则$n \mid a$, 即$a \equiv 0(mod\ n)$, 从而

$c \equiv a^e \equiv 0(\mathrm{mod}\,n).$

所以

$c^d \equiv 0 \equiv a(\mathrm{mod}\,n).$

若$1 < (a,n) < n$, 则必有$a = kp(1 \le k < q)$或$a = kq(1 \le k < p)$.

设$a = kq$, 此时必有$(a,p) = 1$, 那么有

$$a^{ed} \equiv a^{1+k\varphi(n)} \equiv a^{1+k\varphi(p)\varphi(q)} \equiv a(a^{\varphi(p)})^{k\varphi(q)} \equiv a(mod\, p)$$

和$a^{ed} \equiv 0 \equiv a(\mathrm{mod}\, q)$.

所以 $a^{ed} \equiv a(\mathrm{mod}\, n)$.

即 $c^d \equiv a^{ed} \equiv a(mod\, n)$.

由RSA算法可知，因为$\{e,n\}$为公开密钥，破解RSA算法最直接的想法就是分解n，由$n=p\times q$可得到$\varphi(n)=(p-1)\times(q-1)$, 通过$d\times e\equiv 1 mod \varphi(n)$可以求出$d$. 也就是说，RSA算法的安全性依赖于这样的假设：分解因子问题是计算上困难的问题.

单向函数

满足下面条件的函数$f(\,)$称为**单向函数**:

（1）给定x, 计算$y=f(x)$是容易的；

（2）给定y, 计算$x=f^{-1}(y)$在计算上是不可行的.

例如, 在RSA算法中，已知$\{e,n\}$, 加密消息m所做的计算$c\equiv m^e(\mathrm{mod}\,n)$是容易的

单向陷门函数

满足下面条件的函数称之为**单向陷门函数**:

（1）已知x, 则计算$y = f(x)$容易；

（2）已知y, 但不知k, 则计算$x = f_k^{-1}(y)$是不可行的；

（3）已知k和y, 则计算$x = f_k^{-1}(y)$容易.

例如, 对于RSA算法, 由于任何人都知道接收方的公钥, 因而进行加密计算$c \equiv \mathrm{m}^e (\mathrm{mod}\, n)$容易；若已知$n = pq$中$p$和$q$的值, 则容易得到$d$, 故计算$m \equiv c^d (\mathrm{mod}\, n)$也很容易；但若不知$n = pq$中$p$和$q$的值或者$d$的值, 要实现解密在计算上是困难的. RSA算法的安全性，就依赖于分析者虽然知道n是两个素数p和q的乘积，但是从计算上却难以得到p和q的值，从而无法得到d的值, 就不能实现对密文的正常解密.

在RSA算法中, 选取大素数p, q, 记$n = pq, \varphi(n) = (p-1)(q-1)$, 再选择正整数$e$, 满足$(e, \varphi(n)) \equiv 1$, 求得$d$, 满足$ed = 1(\mathrm{mod}\,\varphi(n))$.

加密变换: 明文串P编码为数字M, 则密文
$C \equiv M^e (m \bmod n)$.

解密变换: $M \equiv C^d \pmod{n}$, 再将数字M解码得明文串P.

在解密变换中, 由于接收方可能知道$n = pq$, 于是可以令$x \equiv C^d \pmod{n}$, 则等价于解方程组

$$\begin{cases} x \equiv C^d \pmod{p} \\ x \equiv C^d \pmod{q} \end{cases}.$$

由现有的研究结论, 这会降低解密时的计算量到原来计算量的25%.

《信息安全数学基础》 第3章

《信息安全数学基础》 第3章

《信息安全数学基础》 第3章