信息安全数学基础

同济大学
杨礼珍

作业

- 阅读《密码学原理与实践》2-3页中1.1.1节部分。
- 阅读《抽象代数基础教程》89-90页中2.3节部分、154-155页、163页中3.2节概念部分。
- 练习1.1 计算下列数值:
  - (a) 7503 mod 81
  - (b)(-7503)mod 81
  - (c)81 mod 7503
  - (d)(-81)mod 7503
- 练习1.2 判断对错:
  - (a)3≡5(mod 2)
  - (b) 7≡13(mod 5)
- 练习1.3 设A是所有奇数构成的集合，B是所有偶数构成的集合。请问A、B关于整数的加法运算是否是群？请证明你的结论。
- 练习1.4 证明S_4不是Abel群。

<table>
<tr><th colspan="2">RSA公钥密码算法</th><th>所涉数学概念与原理</th></tr>
<tr><td>公钥(n,b)</td><td rowspan="2">■p、q为素数
■$n=pq$
■b与$(p-1)(q-1)$互素
■$a=b^{-1} \bmod (p-1)(q-1)$</td><td rowspan="4">■$a \equiv b \pmod{n}$：表示n整除b-a，读作“a与b模n同余”，n称为模数

■ a mod n：表示a除以n所得到的余数。

■$a=b^{-1} \bmod m$ 当且仅当 $ab \bmod m=1$

■$Z_n=\{0,1,\ldots,n-1\}$

■$\phi(n)$：欧拉函数，Z_n中与n互素的整数的个数。

■$x^{\varphi(n)} \equiv 1 \pmod{n}$：欧拉定理，费马小定理(n为素数)的推广</td></tr>
<tr><td>私钥(a,p,q)</td></tr>
<tr><td>加密$e_k(x)$</td><td>$y=x^b \bmod n$</td></tr>
<tr><td>解密$d_k(y)$</td><td>$x=y^a \bmod n$</td></tr>
</table>

<table>
<tr><th colspan="2">RSA公钥密码算法</th><th>所涉算法</th></tr>
<tr><td rowspan="4">公钥(n,b)
私钥(a,p,q)</td><td>p、q为素数</td><td>使用素性测试算法生成随机素数</td></tr>
<tr><td>■n=pq</td><td>大整数的算术运算</td></tr>
<tr><td>■b与(p-1)(q-1)互素</td><td>欧几里德算法</td></tr>
<tr><td>■$a=b^{-1} \bmod (p-1)(q-1)$</td><td>扩展欧几里德算法</td></tr>
<tr><td>加密$e_k(x)$</td><td>$y=x^b \bmod n$</td><td rowspan="2">平方-乘算法
中国剩余定理（用于加快解密速度）</td></tr>
<tr><td>解密$d_k(y)$</td><td>$x=y^a \bmod n$</td></tr>
</table>

<table>
<tr><th colspan="2">乘法群G上的ElGamal公钥密码体制</th><th>所涉数学原理与概念</th></tr>
<tr><td>私钥a</td><td>$a\in\{1,\ldots,n-1\}$</td><td rowspan="4">群(G, ·)：集合G及定义在其上的二元运算·，且满足某些性质。运算为乘法时，称为乘法群。

$\alpha\in G$的阶为n 定义为满足$\alpha^n=1$(1为G中的单位元)的最小正整数。α的阶为|G|时称α为群G的生成元、本原元，或者原根（常见于数论中）
以下群在密码学中最为重要：

■$(Z^*_p,\cdot)$，p为素数， $Z^*_p = Z_p /\{0\}$

■$(F^*_{2^n},\cdot)$， $F^*_{2^n}$ 表示有限域F_{2^n}的乘法群

■(E,+)，其中E是模素数p的一个椭圆曲线</td></tr>
<tr><td>公钥
(G,α,β)</td><td>乘法群G中的n阶元素$\alpha,\beta=\alpha^a$</td></tr>
<tr><td>加密运算</td><td>选取随机数k $\in\{1,\ldots,n-1\}$
$y_1=\alpha^k$
$y_2=x\,\beta^k$</td></tr>
<tr><td>解密运算</td><td>$y_2(y_1^{\,a})^{-1}$</td></tr>
</table>

乘法群G上的ElGamal公钥密码体制所基于的离散问题	备注
$\alpha,\beta \in G$且α 的阶为n，求a $\in Z_n$满足$\alpha^a=\beta$，记 a=**$\log_\alpha\beta$**，称为β的离散对数	在数论中，**$\log_\alpha\beta$**写成**$ind_\alpha\beta$**，称为β的指数

常见素性测试算法	所基于的数论内容
Solovay-Strassen算法	二次剩余
Fetmat素性测试	费马(Fetmat)小定理
Miller-Rabin算法	费马小定理

乘法群G上的ElGamal公钥密码体制		所涉数学计算
私钥a	$a\in\{1,\ldots,n-1\}$	生成伪随机数（密码学伪随机数生成器部分）
公钥 (G,α,β)	乘法群G中的n阶元素$\alpha,\beta=\alpha^a$	**生成G中的本原元，由本原元生成n阶元素**
加密运算	选取随机数k $\in\{1,\ldots,n-1\}$ $y_1=\alpha^k$ $y_2=x\beta^k$	**G上的平方-乘算法：求**α^k、β^k **群G上的乘法运算**
解密运算	$y_2(y_1^a)^{-1}$	

群、环、域的概念

群(Group)(G,·)，其中G为元素集合， ·是定义在G上的二元运算，满足以下性质：

封闭性	对$\forall a,b \in G$有$a \cdot b \in G$
结合律	对$\forall a,b,c \in G$有$(a \cdot b) \cdot c=a \cdot(b \cdot c)$
存在单位元（单位元通常用e或1表示）	$\exists e\in G$，使得对于$\forall a \in G$有$e \cdot a=a \cdot e=a$，称e为G的单位元。
可逆性	对$\forall a \in G$，$\exists b\in G$满足 $a \cdot b= b \cdot a=e$，b称为a的逆元，表示成$\mathbf{b=a^{-1}}$

Abel群（又称交换群）

- 为简约起见，在运算符·明确的情况下，群(G, ·)经常用G来代替。
- 若群G满足交换性则称为**交换群**，或者**阿贝尔群(Abel群)**。

交换律	对∀a,b ∈G有a · b=b · a

Abel群的例子

- (Z,+)是Abel群：整数集合Z={...-2,-1,0,1,2,...}，以及定义在其上的加法运算+

封闭性	对∀a,b ∈Z有a+b ∈Z
结合律	对∀a,b,c ∈Z有(a+b)+c=a+(b+c)
0是单位元	对于∀ a ∈Z有0+a=a+0=a
可逆性	对∀a ∈Z，有(-a)+a=a+(-a)=0，因此-a是a的逆元
交换律	对∀a,b ∈Z有a + b=b + a

群的例子

- 当p为素数时(Z^*_p, ·) 是Abel群：其中Z^*_p={1,2,...,p-1}，· 表示mod p乘法运算，即a · b=(ab)mod n。如果p不是素数，则不是群，因为不是所有元素都存在逆元。介绍同余性质时再证明。
- (Z_n, +) 是Abel群：其中+表示mod n加法运算，即a + b表示a+bmod n（这里是Z上的+运算）。介绍同余性质时再证明。
- Mat_n(R)表示R上的所有n×n矩阵的集合，则Mat_n(R)关于矩阵加法运算是Abel群，单位元是全0矩阵$0_{n\times n}$。
- GL(n,R)表示R上的所有n×n可逆矩阵的集合，则GL(n,R)关于矩阵乘法运算是群，但不是Abel群，单位元是单位矩阵$I_{n\times n}$。

群的例子

- 设X是大小为n的有限集合，记S_n={集合X上的所有置换}。那么S_n关于映射合成运算构成群。S_1，S_2是交换群，S_3不是Abel群。当n>3时，S_n不满足交换律。

设$X=\{x_1,x_2,x_3\}$。令$e,e' \in S_3$满足

$e(x_1)=x_1, e(x_2)=x_3, e(x_3)=x_2$，

$e'(x_1)=x_2, e'(x_2)=x_3, e'(x_3)=x_1$，

那么$ee'(x_1)=e(x_2)=x_3$，

$e'e(x_1)=e'(x_1)=x_2$。

因此 $ee' \neq e'e$。

环和域

- 环(Ring)(R,+, ·)：R是元素集合，+, ·是定义在R上的二元运算，且满足如下性质则称为**环**：

<table>
<tr><td colspan="2">(R,+)是Abel群（单位元记为0）</td></tr>
<tr><td rowspan="3">乘法·满足</td><td>封闭性</td></tr>
<tr><td>结合律</td></tr>
<tr><td>存在单位元，记为1</td></tr>
<tr><td>+, ·满足分配律</td><td>对∀a,b,c ∈R，有(a+b)c=(ac)+(bc)，c(a+b)=(ca)+(cb)</td></tr>
<tr><td colspan="2">若乘法·满足交换性，则称为交换环</td></tr>
<tr><td colspan="2">若R为交换环，且R/{0}对乘法运算可逆，则称为域。元素个数无限的称为无限域，个数有限的域称为有限域。</td></tr>
</table>

环和域的例子

- 学习过的域：
  - 实数域(R,+,.)
  - 有理数域(Q,+,.)
  - 复数域(C,+,.)
- (Z,+, ·)是交换环，但不是域
- (Z_m,+, ·)是交换环，但只当m为素数时是域。以后证明。
- (Mat_n(R),+ ,·)是交换环，其中+ ,·分别表示R上的矩阵加法和乘法，但n>1时不是域。