信息安全技术

近世代数基础

1 群论

- 群是一个集合 G，连同一个运算 "$\cdot$"，它结合任何两个元素 a 和 b 而形成另一个元素，这个集合和运算 必须满足叫做四个要求:
  - 1.封闭性。对于所有 G 中 a, b，运算 $a \cdot b$ 的结果也在 G 中。
  - 2.结合律。对于所有 G 中的 a, b 和 c，等式 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 成立。
  - 3.单位元。存在 G 中的一个元素 e，使得对于所有 G 中的元素 a，等式$ae=ea=a$成立。
  - 4.逆元。对于每个 G 中的 a，存在 G 中的一个元素 b 使得 $a \cdot b = b \cdot a = e$，这里的 e 是单位元，数 b 叫做整数 a 的逆元$b=a^{-1}$ 。

交换群：

G是群，若对任意a，$b \in G$都有

$$ab = ba$$

则称G是交换群

有限群

无限群

有限群的阶

循环群

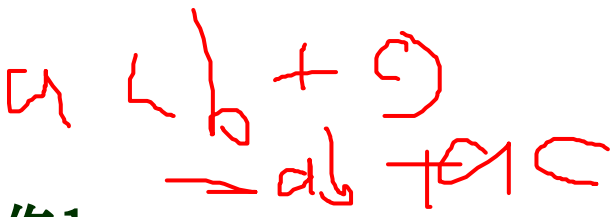
循环群的生成元

群的性质

- 群中的单位元是唯一的
- 群中每一个元素的逆元是唯一的
- (消去律) 对任意的 $a,b,c \in G$ ，如果 $a \cdot b = a \cdot c$，或 $b \cdot a = c \cdot a$ ，则 $b = c$

1.3 有限域理论

- 域的概念
  - 域是由一个非空集合F组成，在集合F中定义了两个二元运算符：“+”和“·”，并满足：
  - 在加法和乘法上封闭 。
  - 加法和乘法符合结合律
  - 加法和乘法符合交换律
  - 符合乘法对加法的分配律
  - 关于加法成群，单位元记作0
  - 非0元乘法构成群，单位元记作1
- 域记为{ F,+, · }



两个定义：

减法：$a-b=a+(-b)$

除法：$a/b=a(b^{-1})$

域的实质：

域是一个可以在其上进行加法、减法、乘法和除法运算而结果不会超出域的集合。如有理数集合、实数集合、复数集合都是域，但整数集合不是

有限域（Galois Field，伽罗瓦域）

有限域的阶

有限域的两个定理

定理1：有限域的阶只能是素数幂。

定理2：对于素数p，与任意正整数n，存在p^n阶的域，记为GF(p^n)，阶为p的域GF(p)称为素域。

密码学常用素域GF(p)或阶为2^m的域GF(2^m)

GF(5)有限域中的计算

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(a)模5的加法

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b)模5的乘法

生成元与逆元

- 生成元
  - 可证明：在GF(p)中至少存在一个元素g，使得GF(p)中任意非零元素可以表示成g的某次方幂的形式，g称为GF(p)的生成元
- 逆元
  - GF(p)中任意元素a

    $a^{-1}=a^{p-2}$

生成元的例子

- 有限域GF（23），5是GF（23）的生成元

$5^0=1$	$5^1=5$	$5^2=2$	$5^3=10$	$5^4=4$
$5^5=20$	$5^6=8$	$5^7=17$	$5^8=16$	$5^9=11$
$5^{10}=9$	$5^{11}=22$	$5^{12}=18$	$5^{13}=21$	$5^{14}=13$
$5^{15}=19$	$5^{16}=3$	$5^{17}=15$	$5^{18}=6$	$5^{19}=7$
$5^{20}=12$	$5^{21}=14$	$5^{22}=1$		

$GF(2^m)$域

0,1系数的多项式

加法：同次项系数异或

乘法：单项式相乘，系数相乘，指数相加
多项式相乘，两式的单项式相乘，然后相加

0,1系数的多项式可以方便的用二进制数表示

不可约多项式

生成元与逆元

- 生成元：

  $GF(2^m)$有生成元

- 逆元

  $a \in GF(2^m)$，$a \neq 0$

  则$a^{-1}=a^{2^m-2}$

例子：GF（2^4）

- 取：$f(x) = x^4 + x + 1$

GF（2^4）的元素：

(0000)	(0001)	(0010)	(0011)	(0100)	(0101)	(0110)	(0111)
(1000)	(1001)	(1010)	(1011)	(1100)	(1101)	(1110)	(1111)

例子（续）

所以，（1011）＋（1001）＝（0010）

$$（1101）\cdot（1001）=(x^3+x^2+1)\cdot(x^3+1)$$

$$=x^6+x^5+x^2+1$$

$$=(x^4+x+1)(x^2+x)+(x^3+x^2+x+1)$$

$$=(x^3+x^2+x+1)\bmod f(x)$$

$$=(1111)$$

生成元为：a=x

$a^0=(0001)$	$a^1=(0010)$	$a^2=(0100)$	$a^3=(1000)$	$a^4=(0011)$	$a^5=(0110)$
$a^6=(1100)$	$a^7=(1011)$	$a^8=(0101)$	$a^9=(1010)$	$a^{10}=(0111)$	$a^{11}=(1110)$
$a^{12}=(1111)$	$a^{13}=(1101)$	$a^{14}=(1001)$	$a^{15}=a^0=(0001)$		

两个困难问题

- 大数的因数分解
  - 两个差不多大的素数的乘积，只要数大，按照目前的计算技术，十年八年算是快的
- 离散对数的问题
  - 困难程度不在大数因数分解之下
- 这两大难题成了现代公钥密码技术的安全保障