东南大学网络空间安全学院

密码学与安全协议

第二讲 密码学的数学基础

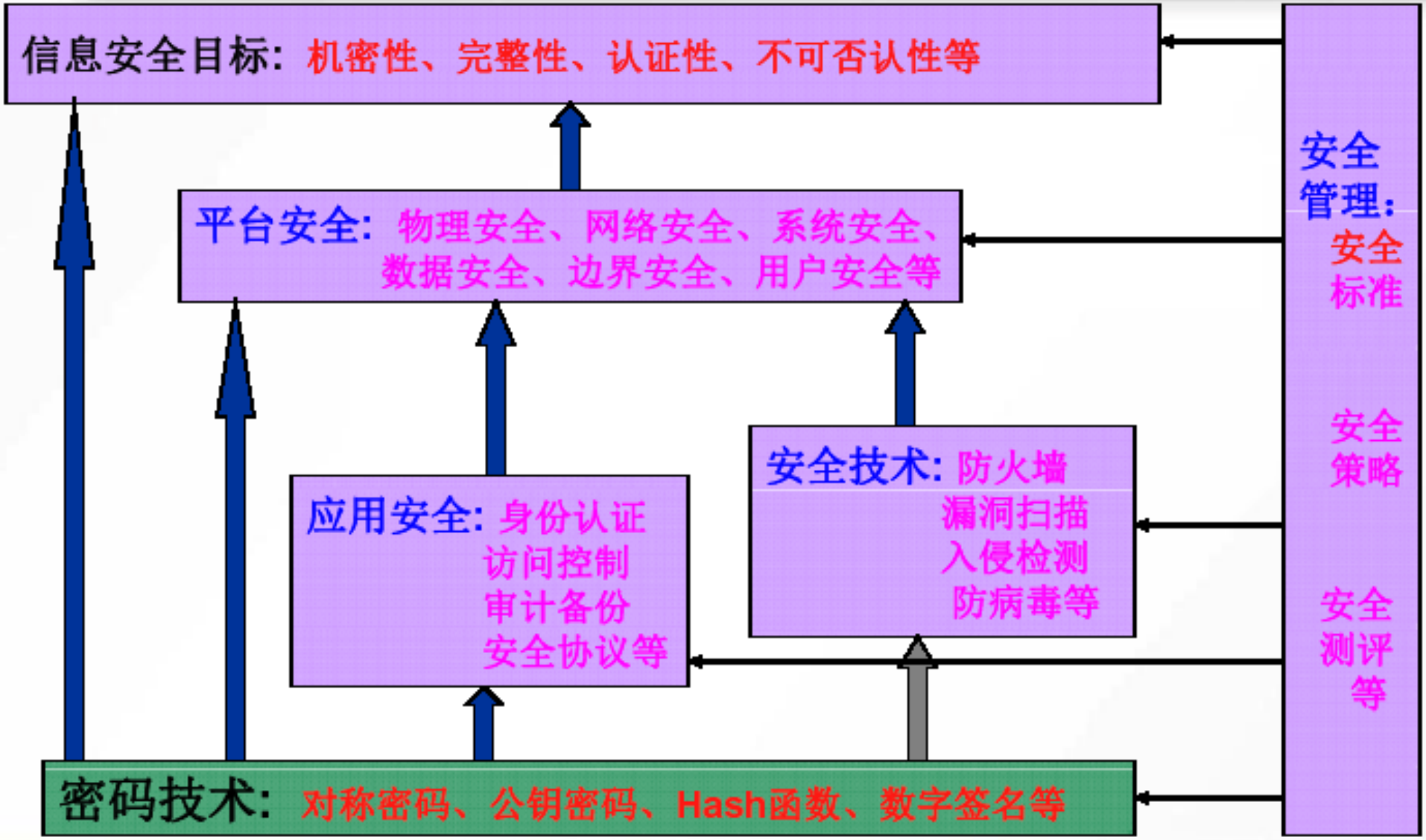
黄　杰

信息安全研究中心

内容的回顾

- 信息安全解决的本质安全问题是什么？
- 信息安全的基本需求（安全服务）
- 如何理解信息安全？
- 密码编码学分哪几个部分？

信息安全与密码学的关系



本讲内容

- 有限域
- 数论基础

知识点

1、有限域和无限域

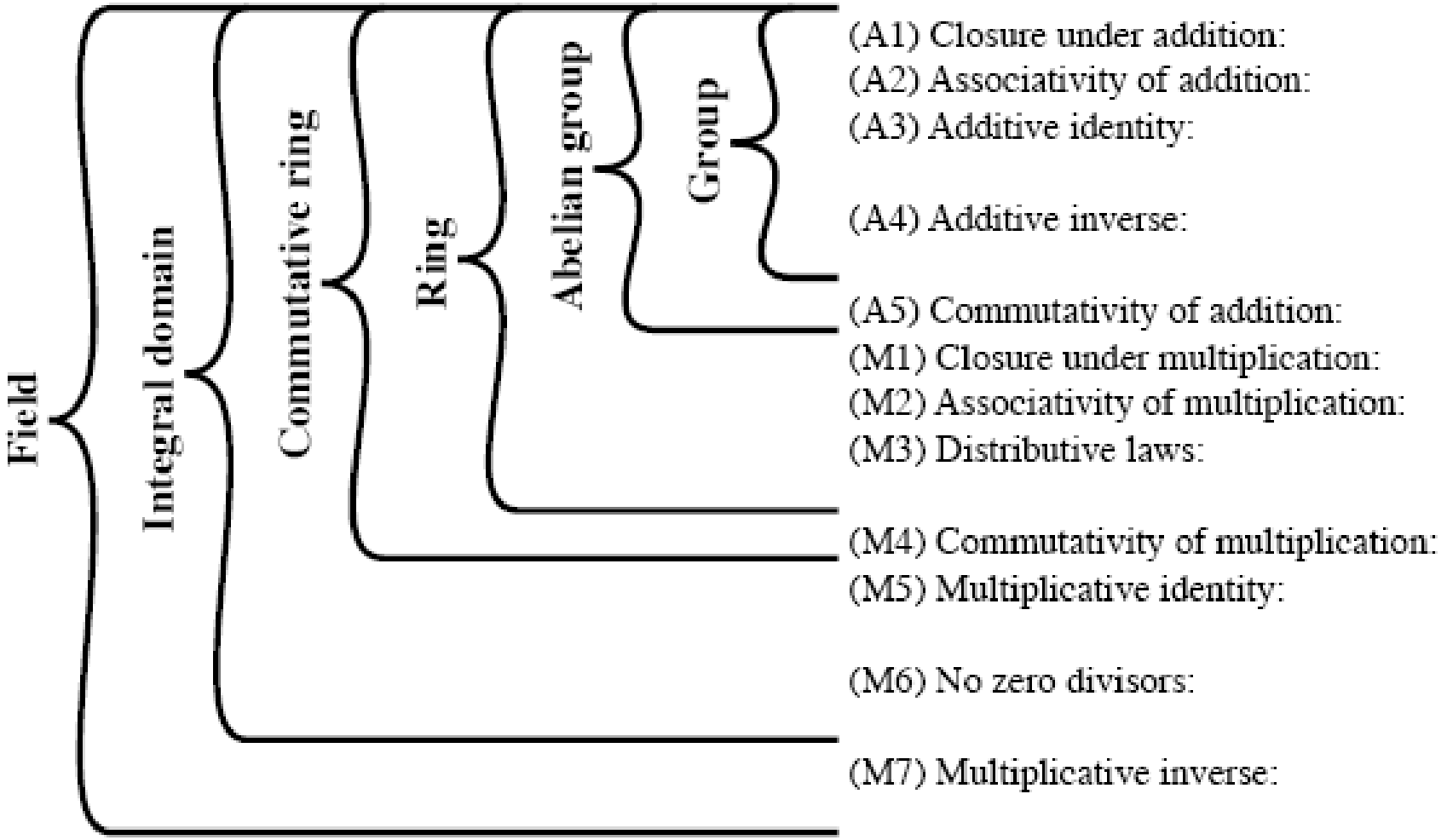
2、多项式模运算

3、Euler定理

4、离散对数

有限域

群、环和域（Field）


Field
Integral domain
Commutative ring
Ring
Abelian group
Group
(A1) Closure under addition:
(A2) Associativity of addition:
(A3) Additive identity:
(A4) Additive inverse:
(A5) Commutativity of addition:
(M1) Closure under multiplication:
(M2) Associativity of multiplication:
(M3) Distributive laws:
(M4) Commutativity of multiplication:
(M5) Multiplicative identity:
(M6) No zero divisors:
(M7) Multiplicative inverse:

群

- 群：记为{G, •}，一个二元运算集合
  - 封闭性： a，b ∈G，则 a•b ∈G
  - 结合律：a,b,c ∈G,则 a•(b•c)= (a•b)•c
  - 单位元：e,a ∈ G，则 a•e = e•a =a
  - 逆元：a,a’ ∈ G，则 a•a’ = a’ •a =e

- 交换群（Abelian Group）
  - 交换律：任意 a,b ∈G,则 a•b = b•a

环

- 环：记为{R, +, x}，两个二元运算（加、乘）集合
  - 乘法封闭性： a， b ∈R，则 ab ∈R
  - 乘法结合律：a, b, c ∈R, 则 a(bc)= (ab)c
  - 分配律： a, b, c ∈R ，则 a(b+c)= ab + ac

- 交换环(Commutative Ring)
  - 乘法交换律：任意 **a, b** ∈R, 则 ab = ba

- 整环(Integral Domain)
  - 乘法单位元：**e, a** ∈ R ，则 **a e** = **e a** = **a**
  - 无零因子： **a**，**b** ∈ R，且 ab = 0，则a=0 或 b=0

域（Galois）

- 域：记为{F, +, X}，两个二元运算集合
  - 乘法逆元： $a \in F$（0除外），则$a^{-1} \in F$, 且

$$a\ a^{-1} = (a^{-1})a = 1。$$

- 移位密码算法
  - 数学描述：设P，C，K={0,2,…,25}，对k∈ K,定义$e_k(x)=x+k \pmod{26}=y \in C$同时$d_k(y)=y-k \pmod{26}$
  - 注1：26个英文字母与模26剩余类集合{0,….,25}建立一一对应：
  - 2*.当k=3时，为Caesar密码，即

    a b c d e f g h i j k l m n o p q r s t u v w x y z

    D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
  - 例子: cipher => FLSKHU
  - 实际算法为：$\forall x \in P \quad 有 \quad e_3(x) = x + 3 (\mathrm{mod}\ 26) = y$
  - 同时有，$d_3(y)=y-3 \pmod{26}$

乘数密码算法

- 加密函数取形式为 $e_k(x)=kx \pmod{26}$, $k \in \{1,2,\ldots 25\}$，且gcd(k,26)=1
- 该算法的数学描述为：设P=C= {1,2,…25}， K={k ∈Z%26 |gcd(k,26)=1},对k∈K，定义$e_k(x)=kx \pmod{26}$和$d_k(y)=k^{-1}(y) \pmod{26}$，x,y ∈Z%26
- 例子: k=9,

  ABCDEFGHIJKLMNOPQRSTUVWXYZ

  AJSBKTCLUDMVENWFOXGPYHQZIR
- 加密操作:

  cipher => SUFLKX

问题：

1、有理数、实数集合和整数集合是域吗？

2、在密码学中，为什么要以域为研究对象呢？

模 运 算

- 定义1：整除
  - $a=qn$
  - n整除a，n称为a的一个因子，n|a
- 定义2：整数的唯一分解定理
  - $a = qn + r, \quad 0 \le r < n$
- 剩余：r
- 模运算：a mod n
  - a除以n所得的余数

同余和剩余类

- 同余的概念：若整数a和b有(a mod n)=(b mod n)，则称a与b在mod n下同余,记为a≡b mod n 。
- 对于满足{r}={a|a=qn+r, q∈Z}的整数集称为同余类。

- 剩余类
  - 定义：比n小的非负整数集合为Zn， Zn＝{0,1,2,…,n-1}，这个集合称为剩余类集合，或模n的剩余类。
  - Zn中的每一个整数都代表一个剩余类
  - 模n的k约化。

模算术（Modular Arithmatic)

- 在mod n的n个剩余类集{0，1，2，…，n-1}上可以定义模算术如下:
- 加法: [(a mod n) + (b mod n)] mod n= (a+b) mod n
- 减法: [(a mod n) - (b mod n)] mod n= (a-b) mod n
- 乘法:[(a mod n) × (b mod n)] mod n= (a × b) mod n

模算术的性质

- 模运算有下述性质：
  - 若n|(a-b)，则a≡b mod n
  - a≡b mod n等价于b≡a mod n
  - 若a≡b mod n且b≡c mod n ，则a≡c mod n

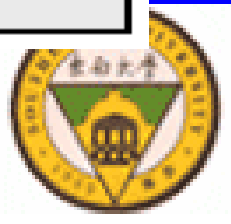
例：模8加法和乘法

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

模算术的性质

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive laws	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$



Euclid算法计算最大公因子

- 最大公因子gcd(a,b)=max[k,其中k|a且k|b]。
- 整数a和b互素，如果gcd(a,b)=1。
- 定理：对于任意正整数a和b，有：

  gcd(a,b)=gcd(b, a mod b).
- Euclid算法：
  - 1.A←a； B←b
  - 2.若B=0，则返回A=gcd(A,B)
  - 3.R=A mod B
  - 4.A ←B
  - 5.B←R
  - 6.转到2

有限域GF(p^n)

- 无限域：例如有理数集合、实数集合、复数集合。在其上可以定义加法、减法、乘法、除法，这些运算满足封闭性。加法和乘法满足交换律、结合律，分配律。
- 元素个数为p^n的有限域一般记为GF(p^n)。有限域在密码编码学中具有重要的地位。
- GF代表Galois Field，以第一位研究有限域的数学家的名字命名。
- GF(p^n)的两种特殊情形：GF(p)和GF(2^n)。

最简单的有限域GF(2)

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

w	-w	w^{-1}
0	0	—
1	1	1

加法等价于”异或”运算，乘法等价于逻辑”与”运算。

GF(7)和GF(8)的代数运算

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

多项式运算

●设集合S由域Z_n上次数不大于n-1的所有多项式组成，每一个多项式具有如下形式：

$$f(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0=\sum_{i=0}^{n-1}a_ix^i$$

●其中a_i在集合{0，1，…，p-1}上取值。S中共有p^n个不同的多项式。

●例如p=2, n=3时，集合中共有$2^3=8$个多项式。

●GF(2^n)中的元素可以表示为一个n位的二进制整数，即域Z_2上一个次数小于n-1的多项式，
其中的系数取值为0或1。

多项式模运算

- 定义运算：
  - 该运算遵循基本代数规则中的普通多项式运算规则
  - 系数运算以**p**为模
  - 如果乘法的结果是次数大于**n-1**的多项式，那么必须将其除以某个次数为**n**的既约多项式**m(x)**并取余式。
- 在以上运算基础上的集合**S**为有限域。

乘法逆元的求法

EXTENDED EUCLID(m, b)

1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^{-1} mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 – Q B1, A2 – Q B2, A3 – Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2

有限域GF(2^n)

- 动机
  - 构造的整数集合必须是一个域。
  - 加密运算要求将整数集平均地映射到自身。
  - Z_8无法做到：

    非零元素 1 2 3 4 5 6 7

    出现次数 4 8 4 12 4 8 4
  - 原因：以8为模

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

有限域GF(2^n)

- 以下运算可以做到：
- 非零元素 1 2 3 4 5 6 7
- 出现次数 7 7 7 7 7 7 7
- 原因：既约多项式为$m(x)= x^3+x+1$

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

(b) Multiplication

GF(2^3)上的加法和乘法表

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

问题

1、密码算法为什么采用有限域而不是无限域？

2、密码学为什么采用模运算？

3、为什么密码学采用$GF(2^n)$形式的有限域，而不采用$GF(p)$形式的有限域？

数 论 入 门

素数

- 任意正整数可由素数的乘积来表示。

$$a = \prod_{p \in P} p^{a_p}, a_p \geq 0$$

  - 整数12可用{a_2=2, a_3=1}来表示
  - 整数18可用{a_2=1, a_3=2}来表示
- 两数相乘。→对应指数相加。
- 整除的表示。→对应指数比较大小。
- 最大公因子的计算。→对应指数取最小值。
  - K=gcd(a,b)-->对所有的p，k_p=min(a_p,b_p)

Fermat定理

- Fermat定理：若p是素数，a是正整数且不能被p整除，则

$$a^{p-1} \equiv 1 \bmod p$$

- Fermat定理的另一种有用表示：若p是素数，a是任意正整数，则

$$a^{p} \equiv a \bmod p$$

Euler函数

- Euler函数Φ(n)，指小于n且与n互素的正整数的个数。
- 对于素数p有：

$$\Phi(p)=p-1$$

- 例如，P=7,小于7且与7互素的正整数有：1，2，3，4，5，6，所以Φ(7)=6
- 如果p=15，Φ(15)=??
- Φ(15)= 8
- 对于两个素数p和q，p≠q，那么对n=pq，有：

$$\Phi(n)=\Phi(pq)=\Phi(p)\times\Phi(q)=(p-1)\times(q-1)$$

Euler定理

- **Euler定理：对于任意互素的a和n，有：**

$$a^{\phi(n)} \equiv 1 \mod n$$

- **Euler定理的另一种有用表示：**

$$a^{\phi(n)+1} \equiv a \mod n$$

- **推论：给定两个素数p和q，整数n=pq，对于小于n的任意正整数a(0<m<n)，有以下关系式成立：**

$$a^{\phi(n)+1} \equiv a^{(p-1)(q-1)+1} \equiv a \mod n$$

- **推论的另一种表达形式：**

$$a^{k\phi(n)+1} \equiv a \mod n$$

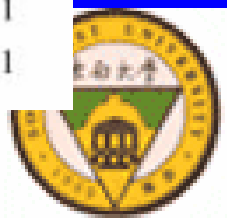
离散对数

- 作用？
- 使得$a^m \equiv 1 \pmod n$成立的最小正幂为m。此时，称m为：
  - a模n的阶
  - a所产生的周期长
  - a所属的模n的指数
- 本原根
  - 若a是n的本原根，则a的1到Φ(n)次幂的模n各不相同的，且均与n互素。
- 当p为素数时，若a是n的本原根，则a的1到(p-1)次幂的模p各不相同的。

模19的整数幂

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

a : primitive root



离散对数

- 离散对数的定义
  - 对于某素数**p**，**p**的本原根为**a**；
  - 对于任何整数**b**， **b ≡ r mod p** ；
  - 存在唯一的整数**i**, $0 \le i \le (p-1)$，使得
    $$b \equiv a^i \bmod p$$
  - **i**称为以**a**为底**b**的指标 $ind_{a,p}(b)$ 也记为离散对数，记为 $\mathbf{dlog_{a,p}(b)}$
- 离散对数的性质
- 离散对数的计算

  $y \equiv g^x \bmod p$

  已知**g,x,p**,计算**y**是容易的

  已知**y,g,p**,计算**x**是困难的

问题

1、Euler定理NP问题是什么？

2、离散对数中，为什么要采用本原根？