

本讲主要内容

- 公钥密码体制的简介
- 背包问题
- **RSA**算法
- **ElGamal**算法
- **ECC**算法
- **IBE**算法

回顾

- 保密通信进入**计算机网络时代**，传统密码体制逐渐暴露其固有的弱点，当时主要体现密钥管理。
- 1976年W. Diffie和Hellman 在《密码学的新方向》中首次提出了**公钥密码算法**的思想。
- 1978年后Rivest, Shamir和Adleman提出的RSA算法体现了公钥算法的思想，并具有**实用性**。
- 公钥密码体制是**现代密码学的一个标志**，到目前为止，是密码学史上最大也是唯一真正的革命。
- **公钥密码**引起密码界高度关注，并得到迅速的发展，尤其在**信息安全的应用**中涉及公钥密码技术。

引言

在公钥密码体制以前的整个密码学发展史中，所有的密码算法，包括原始手工计算的、由机械设备实现的以及由计算机实现的，都是基于**代换**和**换位**这两个基本方法，建立在**在位(字符)方式**的操作上。

而公钥密码体制则为密码学的发展提供了新的理论和技术思想，一方面公钥密码算法是建立在**数学函数**基础上的，而不是建立在**在位(字符)方式**的操作上的；另一方面公钥密码算法是以非对称的形式使用两个密钥，两个密钥的使用对**密钥分配**、**认证**等都有着深刻的意义。可以说，公钥密码体制的出现在密码学发展史上是**一次质的飞跃**。

对称密码体制的缺陷(公钥密码体制产生的必要性)

- 密钥分配问题

通信双方要进行加密通信，需要通过秘密的**安全信道**协商加密密钥，而这种安全信道在实际中很难实现。

- 密钥管理问题

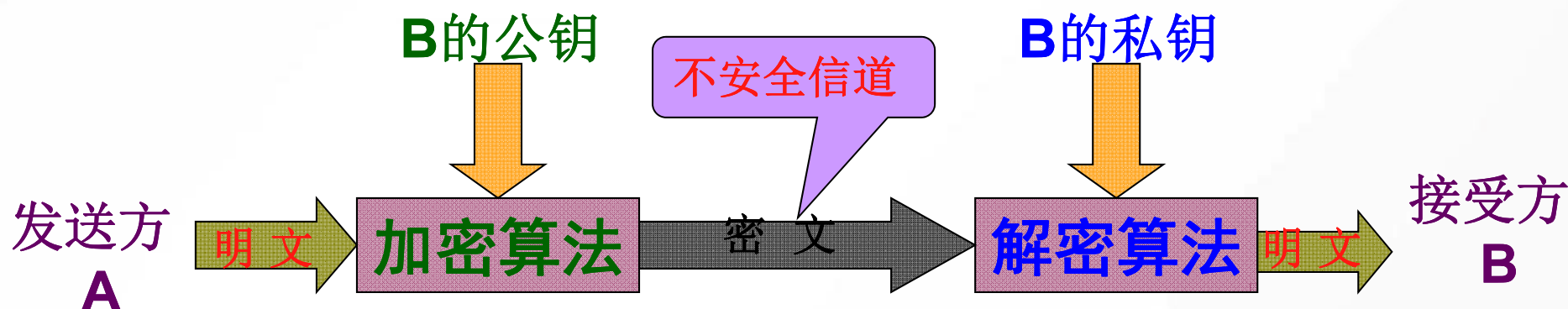
在有 n 个用户的通信网络中，每个用户要想和其它 $n-1$ 个用户进行通信，必须使用 $n-1$ 个密钥，而系统中的总密钥量将达到 $n(n-1)/2$ 。当 n 较大时，这样大的密钥量，在产生、保存、传递、使用和销毁等各个环节中都会变得很复杂，存在着**安全隐患**。

- 数字签名问题

对称密码体制中通信双方拥有同样的密钥，所以接收方可以伪造签名，发送方也可以否认发送过某消息，难于解决陌生人之间的**身份认证**和交易**信息认证**的问题。

加解密模型

- 发送方A查找接受方B的公钥。
- A采用公钥加密算法以B的公钥作为加密密钥对明文加密。
- A通过**不安全信道**将密文发送给B。
- B收到密文后使用自己的私钥对密文解密还原出明文。



基本原理(陷门单向函数)

One-way Trapdoor Function

例如在RSA算法中，首先找一个整数 n ，它是两个大素数的乘积，则 $\phi(n)$ 可求，选一个整数 e ，满足 $\gcd(e, \phi(n))=1$ ，则 e 关于 $\phi(n)$ 的乘法逆元存在，设为 $d \cdot e \equiv 1 \pmod{\phi(n)}$ 。那么 public key= (e, n) , private key= (d, n) 。
陷门为将 n 分解为素因子的乘积，则根据Euler函数， $\phi(n)$ 可求，则 e 的逆元 d 易求。

➤ 正向计算容易。即如果知道密钥 P_k 和消息 M ，容易计算 $C = f_{P_k}(M)$ 。例如在RSA中， $c = m^d \pmod{n}$

➤ 在不知道密钥 S_k 的情况下，反向计算不可行。即如果只知道加密后的消息 C 而不知道密钥 S_k ，则计算不可行 $M = f^{-1}(C)$ 。RSA中，如果知道 (n, e) ，则不易求出 d ，除非 $n = pq$ ， $\phi(n)$ 易求， e 的逆元 d 易求， $ed \equiv 1 \pmod{\phi(n)}$

➤ 在知道密钥 S_k 的情况下，反向计算容易。即如果同时知道加密消息 C 和密钥 S_k ，则计算 $M = f^{-1}_{S_k}(C)$ 是容易的。这里的密钥 S_k 相当于陷门，它和 P_k 配对使用。

解密容易， $m = c^d \pmod{n}$

公钥密码算法应满足的要求

- 接收方B产生密钥对（公钥 PK_B 和私钥 SK_B ）在计算上是容易的。
- 发送方A用接收方的公钥对消息 m 加密以产生密文 c ，即 $c = E_{pk_B}(m)$ 在计算上是容易的。
- 接收方B用自己的私钥对 c 解密，即 $m = D_{sk_B}(c)$ 在计算上是容易的。
- 攻击方由B的公钥 PK_B 求私钥 SK_B 在计算上是不可行的。
- 攻击方由密文 c 和B的公钥 PK_B 恢复明文 m 或求私钥 SK_B (选择明文攻击) 在计算上是不可行的。

公钥密码算法思考的主要问题

- 私钥和公钥是如何生成的，它们之间有着怎样的关系；
- 安全的密钥长度是多少；
- 公钥密码体制的安全性依赖的数学难题是什么；
- 如何实现加密算法(公钥加密)，以及解密算法(私钥解密)，反之亦然（数字签名）；
- 现在这种公钥密码体制的安全分析。

常用算法

- 背包问题（NP问题）。

背包算法

- 基于大整数素因子分解问题。

RSA, Rabin等

- 基于有限域乘法群上的离散对数问题。

Elgamal (DS)。

- 椭圆曲线上的离散对数问题。

ECC。

- 基于身份的密码体制

IBE。

背包算法简介 (略, 自学)

- 由默克尔 (Merkle) 和赫尔曼 (Hellman) 提出的;
- 最早提出的公开密钥算法;
- 安全性源于背包问题, 是一个NP问题;
- 大部分是不安全的, 很少使用;

背包问题

已知一长度 b 的背包及长度分别为 a_1, a_2, \dots, a_n 的 n 个物品。假定这些物品的半径和背包相同，若从这 n 个物品中选出若干物品使得恰好装满这个背包。

公式化的描述为：给定一个正整数集 $A=\{a_1, a_2, \dots, a_n\}$ ，已知 b 是 A 的某子集中元素的和。问题是，找到一个 n 元的 0 、 1 向量 $X=(x_1, x_2, \dots, x_n)$ 使得：

$$\sum_{i=1}^n a_i x_i = b$$

这是一个NP问题。

NP(Non-Deterministic Polynomial, 非确定多项式)问题,是指可以在多项式时间内验证一个解的问题,或者说可以在多项式时间内猜出一个解的问题

其中 a_1, a_2, \dots, a_n 和 b 都是正整数。

超递增序列

如果序列 a_1, a_2, \dots, a_n 满足条件:

$$a_i > \sum_{j=1}^{i-1} a_j \quad (i = 2, 3, \dots, n)$$

则称该序列为超递增序列。

P(Polynomial, 多项式)问题是可以在多项式时间内被确定机(通常意义的计算机)解决的问题

例如: $\{1, 2, 4, 8, \dots, 2^n\}$

$\{1, 3, 6, 13, 27, 52, \dots\}$

而 $\{1, 3, 4, 9, 15, 25\}$ 不是。

如果序列为超递增序列, 则背包问题则是P类问题。

MH背包密码的基本思想

利用实际上存在两类不同的背包问题，一类在线性时间内可解(超递增背包问题)，而另一类不能(普通背包问题)。

易解的背包问题可以转化成难解的背包问题。公钥使用难解的背包问题，它可很容易地被用来加密明文但不能用来解密密文。私钥使用易解的背包问题，它给出一个解密的简单方法。不知道私钥的人要破解密文就不得不解一个难解的背包问题。

将消息编码为背包问题的解。明文分组长度等于堆中物品个数，且明文位与 b 的值相对应，密文是计算得到的和值。

公私钥对的生成

公开的背包序列 a_1, a_2, \dots, a_n 是由超递增序列

b_1, b_2, \dots, b_n 进行以下变换得到的。

选取素数 p 和 u , 且 $p > \sum_{i=1}^n b_i$, $1 \leq u \leq p-1$ 。

私有的、秘密的！

利用已知 u 并根据 $uv=1 \pmod{p}$, 可求得 v 。

u 与 v 关于 $\text{mod } p$ 运算, 互为逆元!

下面作变换称为墨科-赫尔曼 (Merkle-Hellman) 变换:

$$a_k \equiv ub_k \pmod{p}, \quad k=1, 2, \dots, n$$

非超递增序列 $\{a_i\}$ 和 p 作为公钥;

超递增序列 $\{b_i\}$ 和 v 作为私钥;

加解密的实现过程

消息 $m=m_1m_2\dots m_n$ 是 n 位0, 1 二进制串

加密过程:

$$c=a_1m_1 + a_2m_2 + \dots + a_nm_n$$

c 是消息 m 的密文

解密过程:

解密过程就是解背包问题, 即已知超递增序列(私钥)和背包容量(vc), 求解 $m(m_1m_2\dots m_n)$

利用超递增序列 $\{b_i\}$ 求 vc 的解, 可得消息 m 。

$$\begin{aligned} \text{(这是因为 } vc &= va_1m_1 + va_2m_2 + \dots + va_nm_n \\ &= b_1m_1 + b_2m_2 + \dots + b_nm_n \text{)} \end{aligned}$$

$$uv \equiv 1 \pmod{p} \quad a_k \equiv u b_k \pmod{p} \quad b_k \equiv va_k \pmod{p} \quad (k=1,\dots,n)$$

举例说明（公私钥对生成）

$\{1, 3, 7, 13, 26, 65, 119, 267\}$ 是超递增序列，是私有密钥。

$$1+3+7+13+26+65+119+267=501$$

取 $p=523$ 和 $u=467$ ，可得 $v=28$ 。

通过 $uv=13076 \equiv 1 \pmod{523}$ 可验证。然后，计算：

$$a_1=467*1 \equiv 467 \pmod{523} \quad a_2=467*3 \equiv 355 \pmod{523}$$

$$a_3=467*7 \equiv 131 \pmod{523} \quad a_4=467*13 \equiv 318 \pmod{523}$$

$$a_5=467*26 \equiv 113 \pmod{523} \quad a_6=467*65 \equiv 21 \pmod{523}$$

$$a_7=467*119 \equiv 135 \pmod{523} \quad a_8=467*267 \equiv 215 \pmod{523}$$

$\{467, 355, 131, 318, 113, 21, 135, 215\}$ 是背包序列，是公开密钥。

举例说明(加解密)

设明文 $m=10101100$

加密过程:

$$a_1+a_3+a_5+a_6=467+131+113+21=732 \text{ (密文)}$$

解密解密:

接受方收到密文732后, 乘以 $v=28$, 再取模523, 即得:

$$732*28=20496=99 \text{ mod } 523$$

解超递增序列背包问题:

$$m_1+3m_2+7m_3+13m_4+26m_5+65m_6+119m_7+267m_8=99$$

使用贪心法求解超递增序列
背包问题

$$m_1=m_3=m_5=m_6=1, \quad m_2=m_4=m_7=m_8=0$$

即得明文10101100

安全性分析

- 背包问题是**NP问题**，至今还没有有效的求解方法。若对 2^n 种所有可能进行穷举搜索，当 n 很大时在**实际上**是不可能的。

以 $n=100$ 为例： $2^{100}=1.27*10^{30}$

以每秒搜索 10^7 种方案的超高速电子计算机进行穷举，一年只能完成 $3.2*10^{14}$ 次，所以共要：

$$1.27*10^{30} / 3.2*10^{14} = 4*10^{15}\text{年}$$

- 事实上，墨科-赫尔曼变换将超递增序列的特性隐蔽性不够，已被证明大多数基于背包问题的公钥密码是**不安全的**，现很少在使用，但**它的思想是值得借鉴的**。关于对背包问题的攻击，感兴趣的同学请参见相关文献。

背包密码小结

- 背包密码算法是第一个公开密钥算法，但大多数不适合数字签名。
- 背包算法的安全性源于背包问题，它是一个NP问题(随着背包中物品数目的增多而计算量呈指数增长)。尽管这个算法是不安全的，但由于它证明了如何将NP问题用于公钥密码体制，是值得研究的。
- 自从MH方案被破译后，又有许多其他的背包变型被提出，但这些背包中的大多数都被用同样的密码分析方法攻破，少数则采用更高级的分析方法，虽然有极个别的背包变型还没有破解，但人们已不再信赖它们了。

RSA公钥密码的简介

在Diffie和Hellman提出公钥密码体制的设想后两年，先后有Merkle和Hellman提出了MH背包公钥密码，Rivest、Shamir、Adleman联合提出的简称为RSA公钥密码系统。RSA虽稍后于MH背包公钥系统，但它到目前为止应用最广的一种公钥密码。RSA的理论基础是数论的欧拉定理，它的安全性（陷门是将大整数分成素因子乘机）依赖于大整数的素因子分解的困难性。

欧拉函数

给定一个正整数 n ，用 $\varphi(n)$ 表示比 n 小但与 n 互
为素数的正整数的个数，也称 $\varphi(n)$ 为欧拉函数。

$$\varphi(n) = r_1^{a_1-1} (r_1-1) r_2^{a_2-1} (r_2-1) \cdots r_n^{a_n-1} (r_n-1)$$

$$\text{其中 } n = r_1^{a_1} r_2^{a_2} \cdots r_n^{a_n}。$$

$$\text{例如: } 24 = 2^3 * 3, \quad \varphi(24) = 2^{3-1} (2-1) * 3^{1-1} (3-1) = 8$$

$$\{1, 5, 7, 11, 13, 17, 19, 23\}$$

$$35 = 5 * 7, \quad \varphi(35) = (5-1) (7-1) = 24$$

$$\{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, \\ 24, 26, 27, 29, 31, 32, 33, 34\}$$

欧拉定理

用于证明RSA解密算法的正确性

若整数 a 和 n 互素, 则 $a^{\phi(n)} \equiv 1 \pmod{n}$

证明: 设 $\phi(n)=k$ 。又设 r_1, r_2, \dots, r_k 是小于 n 并与 n 互素的数, 且由于 a 是与 n 互素的数, 则 ar_1, ar_2, \dots, ar_k 也和 n 互素且两两不同。

若: $ar_i \equiv ar_j \pmod{n}$

则根据数论定理, 因 a 与 n 互素, 所以存在 \tilde{a} 满足:

$$\tilde{a}a \equiv 1 \pmod{n}$$

$$\tilde{a}ar_i \equiv \tilde{a}ar_j \pmod{n}$$

即: $r_i \equiv r_j \pmod{n}$ (与假定矛盾)

所以, $\{r_1, r_2, \dots, r_k\} = \{ar_1, ar_2, \dots, ar_k\}$

所以, 等式 $a^k r_1 r_2 \dots r_k \pmod{n} \equiv r_1 r_2 \dots r_k \pmod{n}$ 成立。

但 r_1, r_2, \dots, r_k 和 n 互素, 故 $a^k \equiv 1 \pmod{n}$

举例说明

$$5^{\varphi(24)} \equiv 1 \pmod{24}$$

$\varphi(24)=8$ 。又**1,5,7,11,13,17,19,23**是小于24并与24互素的数.

$$\begin{aligned} 1*5 &= 5 \pmod{24} \equiv 5 & 5*5 &= 25 \pmod{24} \equiv 1 & 7*5 &= 35 \pmod{24} \equiv 11 \\ 11*5 &= 55 \pmod{24} \equiv 7 & 13*5 &= 65 \pmod{24} \equiv 17 & 17*5 &= 85 \pmod{24} \equiv 13 \\ 19*5 &= 95 \pmod{24} \equiv 23 & 23*5 &= 115 \pmod{24} \equiv 19 \end{aligned}$$

$$\begin{aligned} \{1,5,7,11,13,17,19,23\} &= \{5*1, 5*5, 5*7, 5*11, 5*13, 5*17, 5*19, 5*23\} \\ 5*1*5*5*5*7*5*11*5*13*5*17*5*19*5*23 &\pmod{24} \\ &= 1*5*7*11*13*17*19*23 \pmod{24} \end{aligned}$$

$$5^8 \equiv 1 \pmod{24} \quad \text{即: } 5^{\varphi(24)} \equiv 1 \pmod{24}$$

应用举例

计算 $2^{1000000} \bmod 77 \equiv ?$

显然, $\gcd(2, 77)=1$, $\phi(77)=\phi(7*11)$

根据欧拉定理, $2^{\phi(77)} \bmod 77 = 1$ 。

由于, $1000000=16666*60+40$

所以, $2^{1000000} \bmod 77 = 2^{16666*60+40} \bmod 77$

$$\equiv 2^{40} \bmod 77 \equiv 1024^4 \bmod 77 \equiv 23^4 \bmod 77$$

$$\equiv 67^2 \bmod 77 \equiv 10^2 \bmod 77 \equiv 23。$$

AKS算法中一个引理:

设 $n \geq 2$ 是一个自然数, $a \in I$, $\gcd(a, n)=1$,

则 n 是素数的充要条件是

$$(X+a)^n \equiv X^n + a \pmod{n}$$

$$1024^4 \bmod 77 = (23+1001)^4 \bmod 77 \quad (1001 \text{ 与 } 4 \text{ 互质})$$

$$\equiv 23^4 + 1001 \pmod{77}$$

$$\equiv (23^4 \bmod 77 + 1001 \bmod 77) \bmod 77$$

$$\equiv 23^4 \bmod 77$$

$$\equiv (462+67)^2 \bmod 77$$

$$\equiv 67^2 \bmod 77 = (4389+100) \bmod 77 = 100 \bmod 77$$

RSA的密钥对生成算法

1. 选取两个大素数 p 和 q ，两个数长度接近且相差较大。
2. 计算 $n=p*q$, $\phi(n)=(p-1)(q-1)$
3. 随机选取整数 e ，满足 $\gcd(e, \phi(n))=1$
4. 计算 d ，满足 $d*e \equiv 1 \pmod{\phi(n)}$ 。

注： p 和 q 保密。

e 和 n 为公钥， d 为私钥。

RSA的加解密过程

● 加密算法: $c=E(m) \equiv m^e \pmod{n}$

● 解密算法: $m=D(c) \equiv c^d \pmod{n}$

证明:

$$c^d = (m^e)^d = m^{ed} = m^{k\phi(n)+1}$$

$$= m * m^{k\phi(n)} = m * (m^{\phi(n)})^k \equiv m * 1 \equiv m \pmod{n}$$

若 m 与 n 互素, 根据欧拉定理, **RSA**加解密成立。

要求:

明文分组 m 对应的十进制数小于 n , 即分组 m 的长度小于 $\log_2 n$ bits。

长度为 $\log_2 n$ 的明文 m 的最大值为 $2^{\log_2 n} - 1 = n - 1$,

所以 $m < n$

RSA的加解密证明过程（续）

若 $\gcd(m, n) > 1$, 由于 $n = p * q$, 所以 $\gcd(m, n)$ 必含 p, q 之一,
设 $\gcd(p, q) = p$, 或 $m = s * p$, $1 \leq s \leq q$, 由欧拉定理得:
 $m^{\phi(q)} = 1 \pmod{q}$.

因此, 对于任何 k , 总有: $m^{k(q-1)} = 1 \pmod{q}$

$$m^{k(p-1)(q-1)} = (1)^{k(p-1)} = 1 \pmod{q}$$

即: $m^{k\phi(n)} = 1 \pmod{q}$ 或 $1 = m^{k\phi(n)} + h * q$

其中 h 是某个整数, 由假定 $m = s * p$, 得:

$$s * p = m^{k\phi(n)} * s * p + s * p * h * q, \quad m = m^{k\phi(n)+1} + s * h * p * q$$

$$m = m^{k\phi(n)+1} + s * h * n, \quad \text{即得: } m^{k\phi(n)+1} \equiv m \pmod{n}$$

RSA的加解密举例说明

$p=43$, $q=59$, $n=p*q=43*59=2539$ $\phi(2539)=42*58=2436$

取 $e=13$, 解方程 $de \equiv 1 \pmod{2436}$ 得: $d=937$

若有明文: cyber greatwall

$\log_2(2539)=11.3$, m 可小于等于11位整数

先将明文分块为: cy be rg re at wa ll

编码: 如利用英文字母表的顺序, 即a为00, b为01, ..., z为25, 将明文数字化得:

0224 0104 1706 1704 0019 2200 1111

利用加密得到密文:

1692 0803 1359 1943 2299 1254 0724

RSA的计算技巧

- 避免中间结果是天文数字，利用模运算的性质：

$$[(a \bmod n) * (b \bmod n)] \bmod n \equiv (ab) \bmod n$$

- 求 $m^e \pmod n$ 可通过指数 e 的快速取模指数算法：

参见课本Page 94

```
t ← 0; c ← 1
for i ← k downto 0
do t ← 2 × t
    c ← (c × c) mod n
if bi = 1 then t ← t + 1
    c ← (c × m) mod n
return c
```

注： $e = (b_k b_{k-1} \dots b_2 b_1)$

RSA算法的安全性

- RSA同态性质
- 选择密文攻击
- 针对 n 分解的攻击
- 侧信道攻击
- 短明文
- 针对RSA算法参数的攻击

同态性

由RSA体制的加密可知，对于一切 $m_1, m_2 \in \mathbb{Z}_n$ ，有 $E_k(m_1 m_2) \equiv E_k(m_1) E_k(m_2) \pmod{n}$ ，称这个性质为RSA的同态性质。根据这个性质，如果敌手知道密文 c_1 和 c_2 的明文 m_1 和 m_2 ，就知道 $c_1 c_2 \pmod{n}$ 所对应的明文是 $m_1 m_2 \pmod{n}$ 。

选择密文攻击

敌手对用户A和B的通信过程进行窃听，得到用户B的公开密钥 e 加密的消息 c 。为了解密 c ，敌手随机选择数 $r < n$ ，然后用B的公钥 e 计算：

$$x \equiv r^e \pmod{n}; \quad y \equiv xc \pmod{n}; \quad t \equiv r^{-1} \pmod{n}$$

敌手让B用他的私钥 d 对 y 签名，即计算 $u \equiv y^d \pmod{n}$ ，敌手收到 u 后计算：

对 x 进行解密得到明文 r

$$tu \pmod{n} \equiv r^{-1}y^d \equiv r^{-1}x^d c^d \equiv r^{-1}rc^d \equiv m \pmod{n}$$

得到密文 C 所对应的明文 M

这表明，使用RSA公钥体制时，绝对不能用自己的私钥 d 对一个陌生人提供给你的随机消息进行签名。

针对n分解的攻击

- 试除法

完全尝试小于 $n^{1/2}$ 的所有素数，直到因子找到。根据素数理论，尝试的次数上限为 $2\sqrt{n} / \log \sqrt{n}$ 。

- 因子分解分析法

$p-1$ 因子分解法、 $p+1$ 因子分解法、二次筛因子分解法、椭圆曲线因子分解法、数域筛因子分解法等。

二次筛因子分解法

基于著名的费马因子分解：找出正整数 x 、 y ，使得 $x^2 \equiv y^2 \pmod{n}$ ，即存在整数 C 满足 $cn = x^2 - y^2 = (x-y)(x+y)$ ，并且满足 $x \not\equiv \pm y \pmod{n}$ ，因此 n 是数 $x^2 - y^2 = (x-y)(x+y)$ 的因子，故 $\gcd(x+y, n)$ 或 $\gcd(x-y, n)$ 均为 n 的因子，由此便可将 n 分解。费马因子分解就是利用了二次筛法的原理，它基于等式 $cn = x^2 - y^2$ ，令 $c = 1$ ，则 $n + y^2 = x^2$ ，为找出 x 、 y 的值直接计算 $n + 1^2$ 、 $n + 2^2$ 、 \dots 、 $n + k^2$ 直至 $n + k^2$ 为完全平方数为止。如令 $n = 295927$ ， $295927 + 3^2 = 295936 = 544^2$ ，因此可得因数分解 $295927 = 544^2 - 3^2 = (544+3)(544-3) = 547 \times 541$ 。

用 $|p-q|/2$ 步找到分解。

侧信道攻击

指攻击者利用从公钥密码设备中容易获得的信息（如电源消耗、运行时间和在特意操控下的输入/输出行为等）攻击秘密信息（如私钥和随机数等）。侧信道攻击的核心思想就是首先通过对加密软件或硬件运行时产生的各种泄露信息进行监测，这些泄露信息包括程序的运行时间、能量消耗、机器发出声音和硬件发出各种电磁辐射等，然后对监测得到的各种数据进行分析和推断，从而得出算法内部运行的情况，进而破解出这些秘密信息。

短明文

用RSA加密消息 m 为 $c \equiv m^e \pmod n$ (假设 m 少于30位)。虽然 m 很小，密文 c 可能和 n 差不多大小，但攻击者可以进行如下攻击，他建立两张表：

(1) $cx^{-e} \pmod n$ 对所有的 $1 \leq x \leq 10^9$;

(2) $y^e \pmod n$ 对所有的 $1 \leq y \leq 10^9$;

然后寻找第一张表和第二张表的匹配。如果找到了一个，那么就对某个 x 和 y 有 $cx^{-e} \equiv y^e \pmod n$ ，得到 $c \equiv (\overbrace{xy}^{\text{明文}})^e \pmod n$ ，所以 $m \equiv xy \pmod n$ 。

针对RSA算法参数的攻击

- 对素数 p 和 q 的选取的一些限制:

难抵御试除法的攻击。

- p 和 q 的长度相差不能太大，大小相差比较大；
- $p-1$ 和 $q-1$ 都应有大的素数因子；

- 共模攻击

- 低指数攻击

- 不动点

若不然, $p - q = k, q = p + k$ 。则

$$(p + q)^2 - (p - q)^2 = 4pq = 4n$$
$$(p + q)^2 = 4n + k^2$$
$$p + q = \sqrt{4n + k^2}$$

又 $p - q = k$

可联立解出 p 和 q 。

循环攻击

设攻击者截获密文 c ,可如下进行重复加密:

$$c^e \equiv (m^e)^e \equiv m^{e^2} \pmod{n}$$

$$c^{e^2} \equiv (m^e)^{e^2} \equiv m^{e^3} \pmod{n}$$

...

$$c^{e^{t-1}} \equiv (m^e)^{e^{t-1}} \equiv m^{e^t} \pmod{n}$$

$$c^{e^t} \equiv (m^e)^{e^t} \equiv m^{e^{t+1}} \pmod{n}$$

若 $m^{e^{t+1}} \equiv c \pmod{n}$,即 $(m^{e^t})^e \equiv c \pmod{n}$,则有 $m^{e^t} \equiv m \pmod{n}$,

即 $c^{e^{t-1}} \equiv m \pmod{n}$,所以在上述重复加密的倒数第2步就已恢复出明文 m ,这种攻击只有在 t 较小时才是可行的.为抵抗这种攻击, p, q 的选择应保证使 t 很大.

循环攻击(续)

设 m 在模 n 下阶为 k ,由 $m^{e^t} \equiv m \pmod{n}$ 得 $m^{e^t-1} \equiv 1 \pmod{n}$,
所以 $k \mid (e^t - 1)$,即 $e^t \equiv 1 \pmod{k}$, t 取为满足上式的最小值
(为 e 在模 k 下的阶).又当 e 与 k 互素时 $t \mid \phi(k)$.为使 t 大, k 就应
大且 $\phi(k)$ 应有大的素因子.又由 $k \mid \phi(n)$,所以,为使 k 大, $p-1$
和 $q-1$ 都应有大的素因子.

共模攻击

- 不同用户不可共享模n。

假如用户A和B共享模数为n，他们的公钥分别为 e_1, e_2 ，攻击者对同一消息m加密可得： $c_1 \equiv m^{e_1} \bmod n$ 和 $c_2 \equiv m^{e_2} \bmod n$ 。攻击者截获密文 c_1 和 c_2 后，利用欧几里德(Euclid)算法计算得到r和s，满足 $r \cdot e_1 + s \cdot e_2 = 1 \bmod n$ 。然后，攻击者将计算：

$$c_1^r * c_2^s = (m^{e_1})^r (m^{e_2})^s \bmod n = m^{re_1 + se_2} \bmod n = m$$

- 不同用户选用的素因子(p或q)不能相同。

著名的素数定理：不超过x的素数的个数大约为 $x/\ln x$ 。在长度为512位的自然数中，有超过 10^{151} 个素数，且素数的概率大约为 $1/\ln x \approx 1/177$ 。

低指数攻击

- 为了增强加密的有效性，希望选择较小的加密指数 e （公钥）。如果相同的消息要送给多个实体，就不应该使用小的加密指数。例如：

$$\begin{array}{ll} c_1 \equiv m^3 \pmod{n_1} & m^3 \equiv c_1 \pmod{n_1} \\ c_2 \equiv m^3 \pmod{n_2} & \Rightarrow m^3 \equiv c_2 \pmod{n_2} \\ c_3 \equiv m^3 \pmod{n_3} & m^3 \equiv c_3 \pmod{n_3} \end{array}$$

- 由中国剩余定理可求出 $m^3 \pmod{n_1 n_2 n_3}$ 。由于 $m^3 < n_1 n_2 n_3$ ，可直接由开立方根得到 m 。

注：M.Wiener提出一种攻击，可以成功地计算出小于 $(1/3)n^{1/4}$ 的私钥 d 。

不动点

满足条件 $m^e \equiv m \pmod{n}$ 的 m 为不动点。显然，不动点对于RSA的安全有一定的威胁，因此，应当减少这样的 m 。容易证明，RSA体制下的不动点的个数为：

$$\gcd(e-1, p-1) \times \gcd(e-1, q-1)$$

因此，为了减少不动点个数，必须使 $p-1$ 和 $q-1$ 的因子尽可能少。

如果 a 是素数，那么素数 $p=2a+1$ 称为安全素数，当 p 和 q 都为安全素数时，不动点的个数最多为四个。

RSA公钥密码的小结

- 第一个**实用**的公开密钥算法。
- 目前**使用最多**的一种公钥密码算法。
- RSA的理论基础是数论的**欧拉定理**。
- RSA的安全性依赖于**大数的素因子分解**的困难性。
- 密码分析者既不能证明也不能否定RSA的安全性。
- 既能用于加密也能用于数字签名。
- 目前密钥长度1024位是安全的。

离散对数问题

构成一个有限域，非0元素， g 是本原

- 设 p 是素数， g 是 p 的本原元，即 $g^0, g^1, g^2, \dots, g^{p-2}$ 在 $\text{mod } p$ 下产生1到 $p-1$ 的所有值，所以对任意 $y \in [1, \dots, p-1]$ 有唯一的 $x \in [0, \dots, p-2]$ 使得 $y \equiv g^x \text{ mod } p$ ，称 x 为模 p 下以 g 为底 y 的离散对数，即为 $x \equiv \log_g y \pmod{p-1}$ 。
- 当 g, p, x 已知时，求 y 比较容易，但如果已知 g, p, y ，求 x 则非常困难。

公私钥对生成

- 选择一素数 p , 1024位。
- g 是 $GF(p)$ 的一个本原元.
- 选择随机数 $x \in [0, p-2]$, 计算 $y \equiv g^x \pmod{p}$
- 私有密钥为 x , 公开密钥为 y 。 g 和 p 可由一组用户共享。

注： 已知 g, x, p , 计算 y 是容易的

已知 y, g, p , 计算 x 是困难的

加解密过程

设通信双方为A和B，A和B各选一个秘密整数 x_A 和 x_B ， $x_A, x_B < p-1$ 。

A计算： $y_A \equiv g^{x_A} \pmod{p}$ x_A 为A的私钥， y_A 为A的公钥

B计算： $y_B \equiv g^{x_B} \pmod{p}$ x_B 为B的私钥， y_B 为B的公钥

y_A 和 y_B 公开。

A要对 m 加密给B， $0 \leq m \leq p-1$ ，A可在 $[0, p-2]$ 上任选随机数 k ，计算： $K \equiv y_B^k \pmod{p}$ 一次模指数运算

加解密过程(续)

加密算法:

$$c_1 \equiv g^k \pmod{p} \quad \text{一次模指数运算}$$

$$c_2 \equiv Km \pmod{p} \quad \text{一次模乘积运算}$$

$$C = (c_1, c_2)$$

解密算法:

$$\text{先计算: } K \equiv (y_B)^k \pmod{p} \equiv (g^k)^{x_B} \pmod{p}$$

$$\equiv (c_1)^{x_B} \pmod{p} \quad \text{Xb为私钥, 一次模指数运算得到K}$$

$$m \equiv c_2 / K \pmod{p} \quad \text{先求K的逆元, 然后与C2做一次模乘积运算, 求得明文m}$$

举例说明

假设 $p=2579$ ，本原元 $g=2$ ，私钥 $x=765$ ，则公钥

$$y=2^{765} \bmod 2579=949, \text{ 消息 } m=1299。$$

A**加密过程**：选择随机数 $k=853$ ，并计算 $c_1=2^{853} \bmod$

$$2579=435 \text{ 和 } c_2=1299*949^{853} \bmod 2579=2396。$$

发送密文 $(435, 2396)$ 。

B**解密过程**：消息 $m=2396*(435^{765})^{-1} \bmod 2579$
 $=1299。$

常用分析方法

- 穷举法和列表法
- 小步大步（**Baby-step Giant-step**）算法
- 指数积分法（**Index Calculus**）

穷举法和列表法

➤ 穷举法

计算 g , g^2 , $g^3 \dots$, 直到发现 $y=g^x$ 。

➤ 列表法

预先计算所有可能的值 g^i , 并对有序对 (i, g^i) 以第二项排序列表, 然后给定 y , 我们对存储的列表实施一个二分查找, 直到找到 i 使得 $y=g^i$ 。

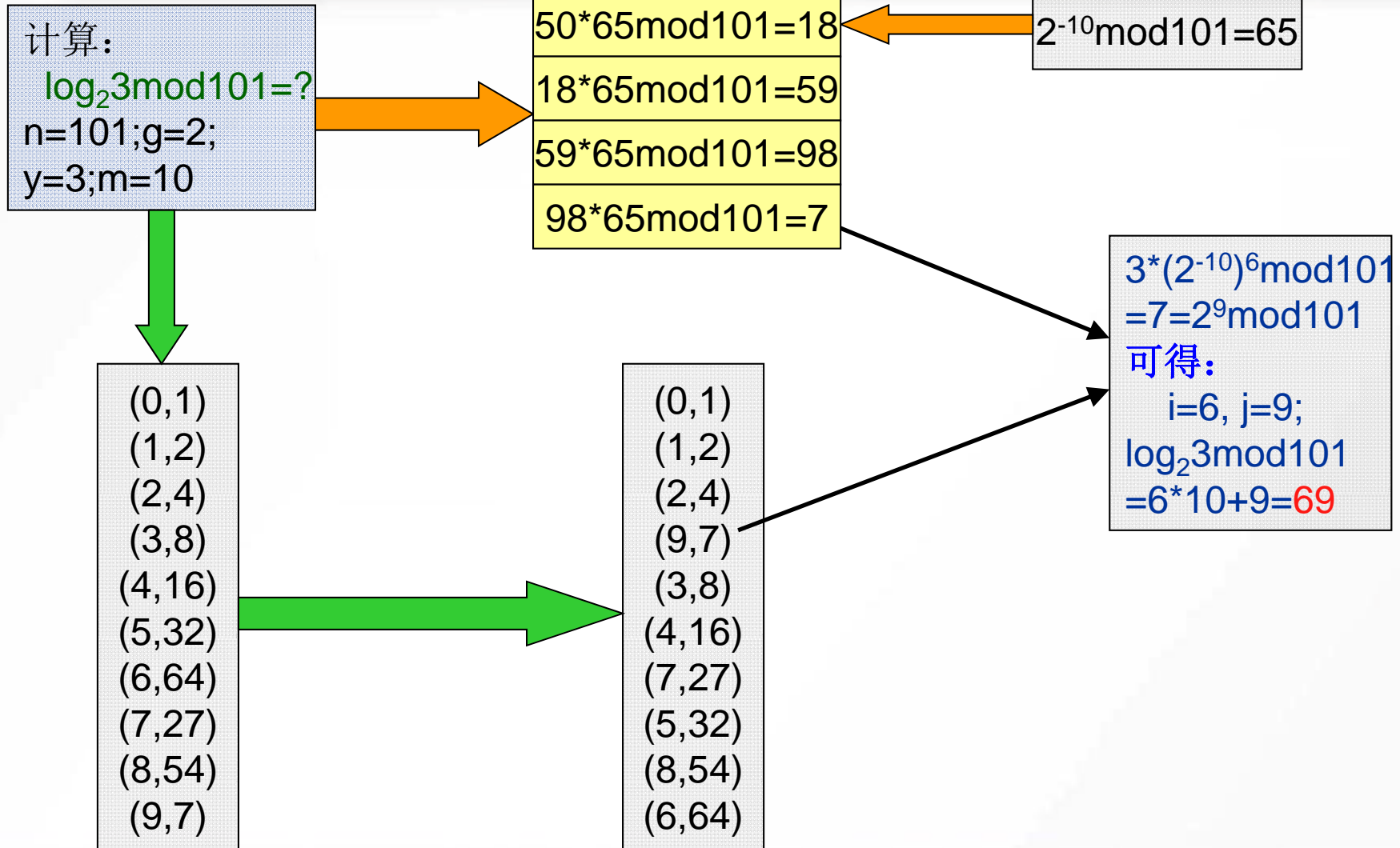
小步大步算法

设 G 是以 g 为生成元的循环群，若求解离散对数问题 $y \equiv g^x \pmod{p}$ ，相当于已知 g 和 y 求 x 。令 n 为群 G 的阶，即 $n = \#G$ ，并令 $m = \lfloor \sqrt{n} \rfloor$ ，即 m 为恰好不超过的整数。当 $x = \log_g y$ 时，可以记 $x = m \cdot i + j$ ，其中 $0 \leq i < m$ ， $0 \leq j < m$ 。这样首先对 $0 \leq j < m$ ，计算 m 个 g^j ，并把它们放在某个有序的查询表中。然后连续计算如下 m 个值： y ， $y \cdot g^{-m}$ ， $y \cdot g^{-2m}$ ， \dots ， $y \cdot g^{-mi}$ ， \dots

在第 i 步，比较 $y \cdot g^{-mi}$ 和 g^j ，如果相等，则 $\log_g y = mi + j$ 。

注：关于可查询表 g^j 的构造，最初需要 \sqrt{n} 步。 $y \cdot g^{-mi}$ 和 g^j 的比较共有 $O(\sqrt{n})$ 次，每一次应该必须在不超 $O(\sqrt{n})$ 的时间内完成。否则总共就需要 $O(n)$ 步，这就与穷举法没有区别了。因此查询表 g^j 的编排必须保证能非常快速地判断一个元素 $y \cdot g^{-mi}$ 是否在表中。比如，在简单的情况，这个判断应只需要 $\log_2 m$ 次比较即可以完成。

举例



指数积分法

- 选取因数基底S: 如同筛法选取小素数集基底一样,

$$S = \{p_1, p_2, \dots, p_m\}$$

- 建构同余方程组: 对若干随机整数 $k (0 \leq k \leq p)$, 计算 g^k .

尝试将 g^k 写成S中的元素幂次的乘积, 即 $g^k = \prod_i p_i^{e_i} \bmod p$,

式子两边取离散对数, 得 $k = \sum_i e_i \log_g(p_i) \bmod (p-1)$,

解 $\log_g(p_i) (p_i \in S)$ 。

- 计算: 随机取整数r, 计算值 $yg^r \bmod p$, 使得其值可表示为

S中元素幂次的乘积, 即取离散对数 $yg^r = \prod_i p_i^{d_i} \bmod p$

可得 $x = \log_g(y) = -r + \sum_i d_i \log_g(p_i) \bmod (p-1)$

举例

计算:

$$\log_{11} 7 \bmod 28 = ?$$

$p=29; g=11; y=7;$

因子基 $S=\{2,3,5\}$

$$11^2 \bmod 29 = 5$$

$$11^3 \bmod 29 = 26$$

$$11^5 \bmod 29 = 14$$

$$11^6 \bmod 29 = 3^2$$

$$11^7 \bmod 29 = 2^2 * 3$$

$$11^9 \bmod 29 = 2$$

$$\log_{11} 2 \bmod 28 = 9$$

$$\log_{11} 3 \bmod 28 = 17$$

$$\log_{11} 5 \bmod 28 = 2$$

$$7 * 11 \bmod 29 = 19$$

$$7 * 11^2 \bmod 29 = 2 * 3$$

$$\log_{11} 7 \bmod 28 = \log_{11} 2 + \log_{11} 3 - 2 = 24$$

离散对数算法的小结

- 基于有限域的离散对数公钥密码又称ElGamal（厄格玛尔）算法。
- ElGamal算法的安全性依赖于计算有限域上的离散对数。
- ElGamal算法的离散对数等同RSA的大数分解问题。
- ElGamal算法既可用于数字签名又可用于加密，但更多地应用在数字签名中。
- ElGamal算法未申请专利。

椭圆曲线密码体制

- 椭圆曲线在代数学和几何学上已广泛研究了150多年之久，有丰富而深厚的理论积累。
- 1985年，Koblitz和Miller提出椭圆曲线密码体制（Elliptic Curve Cryptosystem，简称ECC）
- 椭圆曲线并不是椭圆，之所以称为椭圆曲线是因为它们是用三次方程来表示的，它的一般形式：

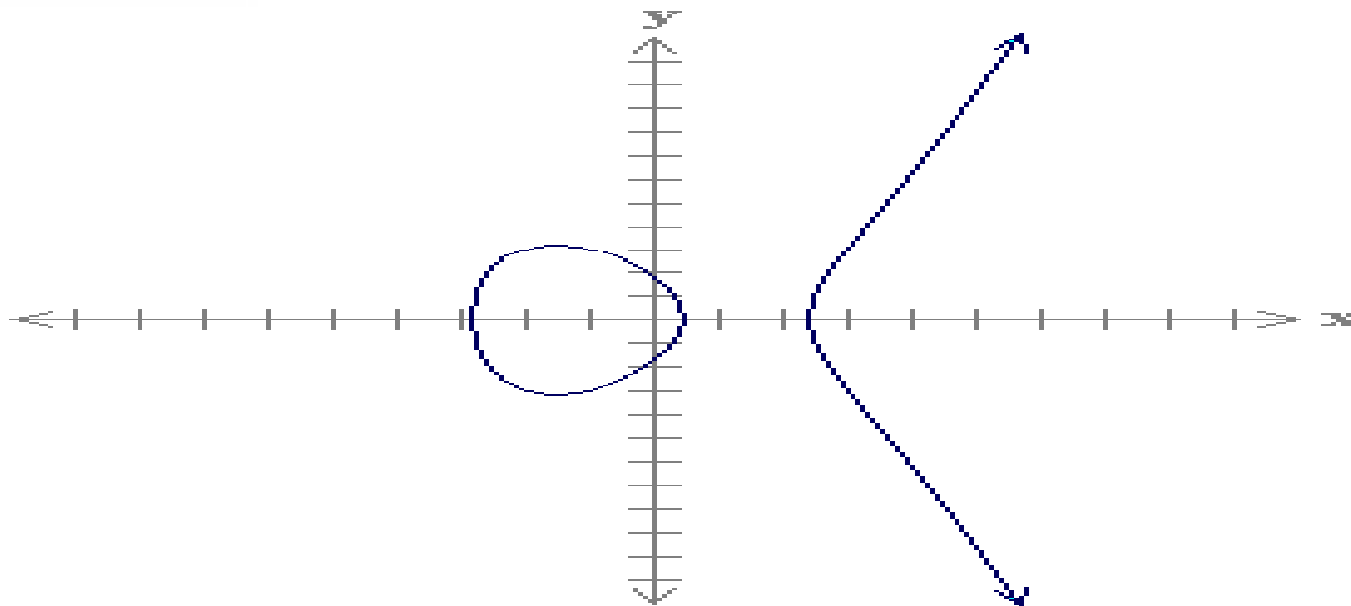
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

其中a, b, c, d和e是满足某些条件的实数。

- 大多数的椭圆曲线密码系统是在模p或 F_2 下运算。
- 椭圆曲线已经逐渐被采用，很可能是一个重要的发展方向。

椭圆曲线的定义

在实数系中，椭圆曲线可定义成所有满足方程式
 $E: y^2 = x^3 + ax + b$ 的点 (x, y) 所构成的集合。若方程式没有重复的因式
或 $4a^3 + 27b^2 \neq 0$ ，则 $E: y^2 = x^3 + ax + b$ 能成为群(group)。例如，椭圆
曲线 $E: y^2 = x^3 - 7x + 3$ 的图形如下所示。



有限群上的椭圆曲线

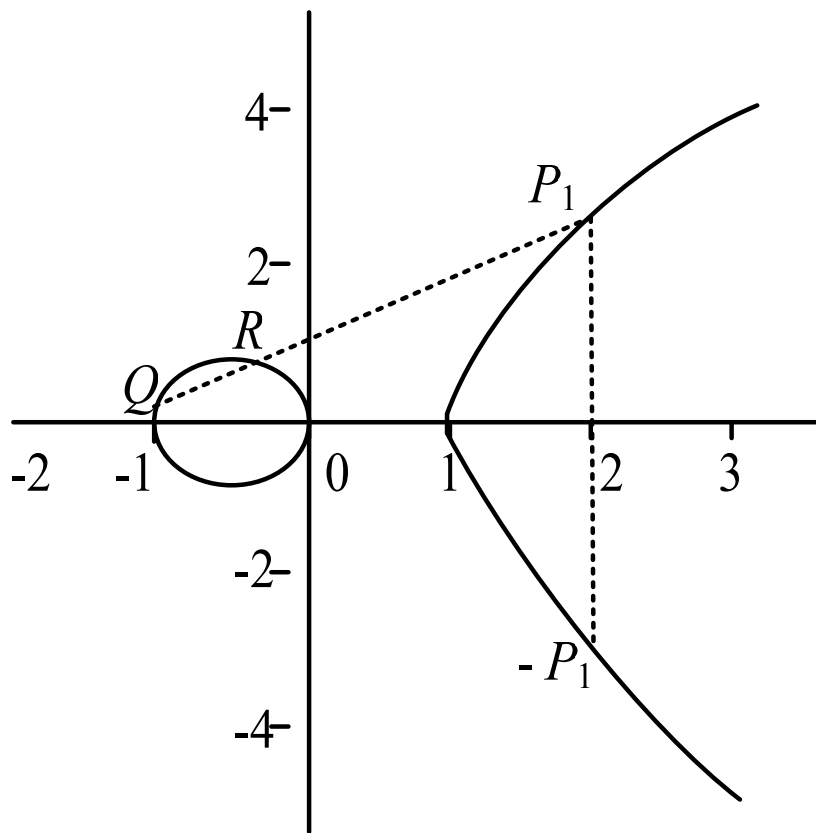
形式: $y^2 = x^3 + ax + b \pmod{p}$

其中: p 是一个素数

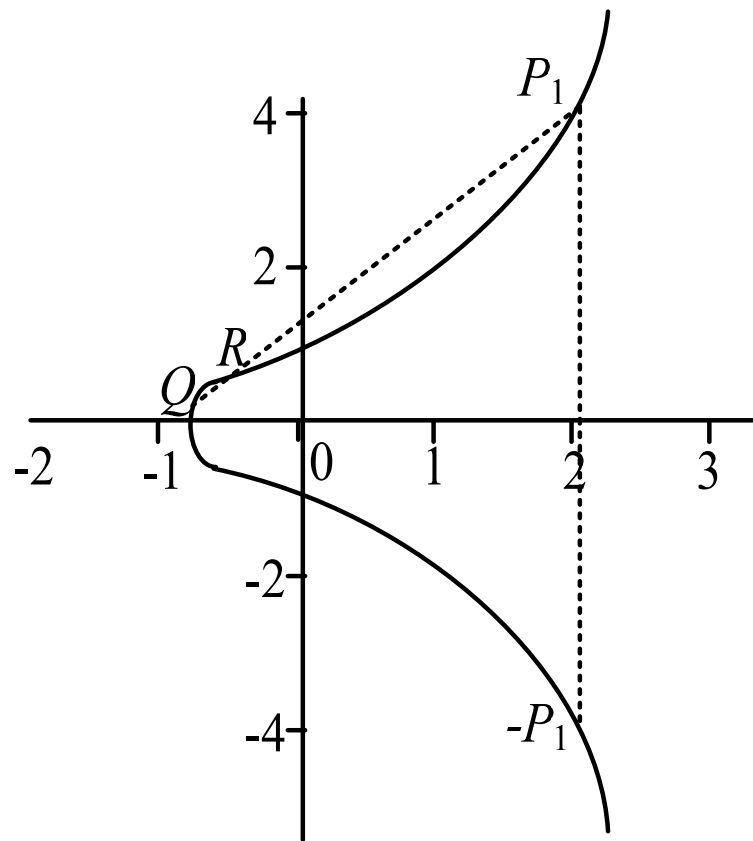
a 和 b 都是小于 p 的非负整数, 且满足:

$$4a^3 + 27b^2 \pmod{p} \neq 0$$

椭圆曲线有一个特殊的点, 记为 O , 它并不在椭圆曲线 E 上, 此点称为无限远的点(the point at infinity)。 $E_p(a, b)$ 为在模 p 之下椭圆曲线 E 上所有的点所构成的集合 (包括 O)。点 $P = (x, y)$ 对 x 坐标轴的对称点为 $-P = (x, -y)$, 而称 $-P$ 为点 P 的负点。若 $nP = O$ 且 n 为最小的正整数, 则 n 为椭圆曲线 E 上点 P 的秩。除了无限远的点 O 之外, 椭圆曲线 E 上任何可以生成所有点都可视为是 E 的生成数(generator), 但并不是所有在 E 上的点都可视为生成数。



(a) $y^2 = x^3 - x$



(b) $y^2 = x^3 + x + 1$

图4.4 椭圆曲线的两个例子

从图可见，椭圆曲线关于x轴对称。

椭圆曲线上的**加法运算定义**如下： 如果其上的3个点位于同一直线上，那么它们的和为O,单位元。

进一步可如下定义椭圆曲线上的加法律（加法法则）：

① O为加法单位元，即对椭圆曲线上任一点P，有 $P+O=P$ 。

② 设 $P_1=(x,y)$ 是椭圆曲线上的一点, 它的加法逆元定义为 $P_2=-P_1=(x, -y)$ 。

这是因为 P_1 、 P_2 的连线延长到无穷远时，得到椭圆曲线上的另一点O，即椭圆曲线上的3点 P_1 、 P_2 ，O共线，所以 $P_1+P_2+O=O$ ， $P_1+P_2=O$ ，即 $P_2=-P_1$ 。

由 $O+O=O$ ，还可得 $O=-O$

③ 设 Q 和 R 是椭圆曲线上 x 坐标不同的两点， $Q+R$ 的定义如下：画一条通过 Q 、 R 的直线与椭圆曲线交于 P_1 （这一交点是惟一的，除非所做的直线是 Q 点或 R 点的切线，此时分别取 $P_1=Q$ 和 $P_1=R$ ）。由 $Q+R+P_1=O$ 得 $Q+R=-P_1$ 。

④ 点 Q 的倍数定义如下：在 Q 点做椭圆曲线的一条切线，设切线与椭圆曲线交于点 S ，定义 $2Q=Q+Q=-S$ 。类似地可定义 $3Q=Q+Q+Q$ ，...，等。

以上定义的加法具有加法运算的一般性质，如交换律、结合律等。

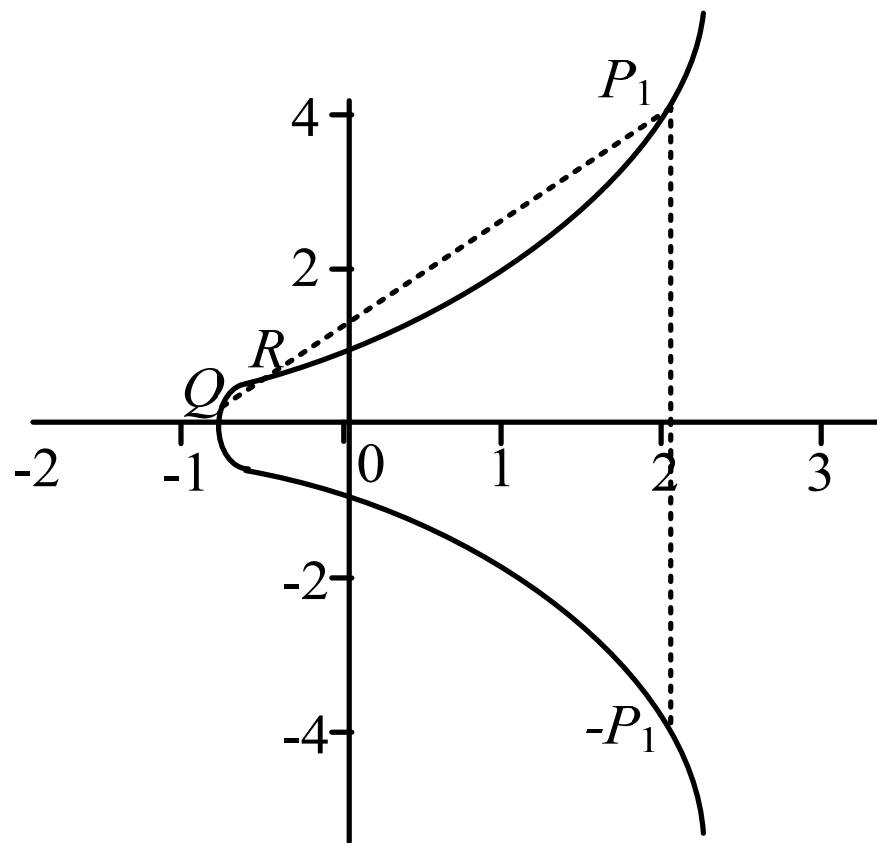
有限域上的椭圆曲线

密码中普遍采用的是有限域上的椭圆曲线，有限域上的椭圆曲线是指曲线方程定义式。所有系数都是某一有限域 $\text{GF}(p)$ 中的元素（其中 p 为一大素数）。其中最为常用的是由方程

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

$(a, b \in \text{GF}(p), \text{判别式 } 4a^3 + 27b^2 \pmod{p} \neq 0)$
定义的曲线。该椭圆曲线记为 $E_p(a, b)$

例：椭圆曲线 $E_{23}(1,1)$, $p=23$, $a=b=1$,
 $4a^3+27b^2(\bmod 23)\equiv 8\neq 0$, 椭圆曲线为:
 $y^2\equiv x^3+x+1$, 其图形是连续曲线, 由图所示。



然而我们感兴趣的是曲线在第一象限中的整数点。设 $E_p(a,b)$ 表示方程(4.2)所定义的椭圆曲线上的点集 $\{(x,y)|0 \leq x < p, 0 \leq y < p, \text{ 且 } x,y \text{ 均为整数}\}$ 并上无穷远点 O 。本例中 $E_{23}(1,1)$ 由表4.6给出，表中未给出 O

表4-8 椭圆曲线上的点集 $E_{23}(1,1)$

(0, 1)	(0, 22)	(1, 7)	(1, 16)	(3, 10)	(3, 13)	(4, 0)	(5, 4)	(5, 19)
(6, 4)	(6, 19)	(7, 11)	(7, 12)	(9, 7)	(9, 16)	(11, 3)	(11, 20)	(12, 4)
(12, 19)	(13, 7)	(13, 16)	(17, 3)	(17, 20)	(18, 3)	(18, 20)	(19, 5)	(19, 18)

一般来说, $E_p(a,b)$ 由以下方式产生:

① 对每一 $x(0 \leq x < p$ 且 x 为整数), 计算 $x^3+ax+b(\bmod p)$ 。

② 决定①中求得的值在模 p 下是否有平方根, 如果没有, 则曲线上没有与这一 x 相对应的点; 如果有, 则求出两个平方根 ($y=0$ 时只有一个平方根)。

$E_p(a,b)$ 上的加法定义如下:

设 $P, Q \in E_p(a,b)$, 则

① $P+O=P$ 。

② 如果 $P=(x,y)$, 那么 $(x,y)+(x,-y)=O$, 即 $(x,-y)$ 是 P 的加法逆元, 表示为 $-P$ 。

由 $E_p(a,b)$ 的产生方式知, $-P$ 也是 $E_p(a,b)$ 中的点, 如上例, $P=(13,7) \in E_{23}(1,1)$, $-P=(13,-7)$, 而 $-7 \bmod 23 \equiv 16$, 所以 $-P=(13,16)$, 也在 $E_{23}(1,1)$ 中。

③ 设 $P=(x_1, y_1)$, $Q=(x_2, y_2)$, $P \neq -Q$, 则
 $P+Q=(x_3, y_3)$ 由以下规则确定:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$$

$$y_3 \equiv \lambda (x_1 - x_3) - y_1 \pmod{p}$$

其中

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

椭圆曲线在模 p 下的运算规则(续)

(iii) 如果 s 和 t 为整数, 则对所有的点 $P \in E_p$ 而言,

$$(s+t)P = sP + tP$$

- 乘法规则:

(i) 如果 k 为整数, 则对所有的点 $P \in E_p$ 而言,

$$kP = P + P + \dots + P$$

(ii) 如果 s 和 t 为整数, 则对所有的点 $P \in E_p$ 而言,

$$s(tP) = (st)P$$

例：仍以 $E_{23}(1,1)$ 为例，设 $P=(3,10)$ ， $Q=(9,7)$ ，
则

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \equiv (-1) \cdot 2^{-1} \equiv 22 \cdot 12 \equiv 11 \pmod{23}$$

$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \pmod{23}$$

$$y_3 = 11(3-17) - 10 = -164 \equiv 20 \pmod{23}$$

$$-164 = -164 + 8 \cdot 23 \pmod{23} = 20 \pmod{23}$$

所以 $P+Q = (17,20)$ ，仍为 $E_{23}(1,1)$ 中的点。

若求2P则

$$\lambda = \frac{3 \cdot 3^2 + 1}{2 \times 10} = \frac{5}{20} = \frac{1}{4} \equiv 6 \pmod{23}$$

$$x_3 = 6^2 - 3 - 3 = 30 \equiv 7 \pmod{23}$$

$$y_3 = 6(3 - 7) - 10 = -34 \equiv 12 \pmod{23}$$

所以2P=(7,12)。

倍点运算仍定义为重复加法，如

$$4P = P + P + P + P。$$

从例子看出，加法运算在 $E_{2,3}(1,1)$ 中是封闭的，且能验证还满足交换律。对一般的 $E_p(a,b)$ ，可证其上的加法运算是封闭的、满足交换律，同样还能证明其上的加法逆元运算也是封闭的，所以 $E_p(a,b)$ 是一个Abel群。

【例 4-30】已知 $y^2 \equiv x^3 - 2x - 3$ 是系数在 $GF(7)$ 上的椭圆曲线, $P=(3,2)$ 是其上一点, 求 $10P$ 。

$E_7(-2,-3)$

解: $2P = P + P = (3,2) + (3,2) = (2,6),$

$$3P = P + 2P = (3,2) + (2,6) = (4,2),$$

$$4P = P + 3P = (3,2) + (4,2) = (0,5),$$

$$5P = P + 4P = (3,2) + (0,5) = (5,0),$$

$$6P = P + 5P = (3,2) + (5,0) = (0,2),$$

$$7P = P + 6P = (3,2) + (0,2) = (4,5),$$

$$8P = P + 7P = (3,2) + (4,5) = (2,1),$$

$$9P = P + 8P = (3,2) + (2,1) = (3,5),$$

$$10P = P + 9P = (3,2) + (3,5) = O.$$

可见 $P(3,2)$ 是生成元,
 P 的阶为 10

4.7.3 椭圆曲线上的点数

在 4.7.2 的例中, $GF(23)$ 上的椭圆曲线 $y^2 \equiv x^3 + x + 1$ 在第一象限中的整数点加无穷远点 O 共有 28 个。一般有以下定理:

定理 4-13 $GF(p)$ 上的椭圆曲线 $y^2 = x^3 + ax + b$ ($a, b \in GF(p)$, $4a^3 + 27b^2 \neq 0$)

在第一象限中的整数点加无穷远点 O 共有

$$1 + p + \sum_{x \in GF(p)} \left(\frac{x^3 + ax + b}{p} \right) = 1 + p + \varepsilon$$

个, 其中 $\left(\frac{x^3 + ax + b}{p} \right)$ 是 Legendre 符号。

定理中的 ε 由以下定理给出:

定理4-14 (Hasse定理) $|\varepsilon| \leq 2\sqrt{p}$.

【例 4-31】 若 $p=5$, 则 $|\varepsilon| \leq 4$. 因此 $GF(5)$ 上的椭圆曲线 $y^2 = x^3 + ax + b$ 上的点数在 2 和 10 之间。

4.7.4 明文消息到椭圆曲线上的嵌入

在使用椭圆曲线构造密码体制前，需要将明文消息镶嵌到椭圆曲线上，作为椭圆曲线上的点。设明文消息是 $m(0 \leq m \leq M)$ ，椭圆曲线由 (4.2) 给出， k 是一个足够大的整数，使得将明文消息镶嵌到椭圆曲线上时，错误概率是 2^{-k} 。实际中， k 可在 30~50 之间取值。下面取 $k = 30$ ，对明文消息 m ，如下计算一系列 x ：

$$x = \{mk + j, j = 0, 1, 2, \dots\} = \{30m, 30m + 1, 30m + 2, \dots\}$$

直到 $x^3 + ax + b \pmod{p}$ 是平方根，即得到椭圆曲线上的点 $(x, \sqrt{x^3 + ax + b})$ 。因为在 0 到 p 的整数中，有一半是模 p 的平方剩余，一半是模 p 的非平方剩余。所以 k 次找到 x ，使得 $x^3 + ax + b \pmod{p}$ 是平方根的概率不小于 $1 - 2^{-k}$ 。

反过来, 为了从椭圆曲线上的点 (x, y) 得到明文消息 m , 只需求 $m = \left\lfloor \frac{x}{30} \right\rfloor$ 。

【例 4-32】 设椭圆曲线为 $y^2 = x^3 + 3x$, $p = 4177, m = 2174$ 。则

$x = \{30 \cdot 2174 + j, j = 0, 1, 2, \dots\}$ 。当 $j = 15$ 时, $x = 30 \cdot 2174 + 15 = 65235$,

$x^3 + 3x = 65235^3 + 3 \cdot 65235 = 1444 \bmod 4177 = 38^2$ 。所以得到椭圆曲线上的点为

$(65235, 38)$ 。若已知椭圆曲线上的点 $(65235, 38)$, 则明文消息

$$m = \left\lfloor \frac{65235}{30} \right\rfloor = \lfloor 2174.5 \rfloor = 2174。$$

4.7.5 椭圆曲线上的密码

为使用椭圆曲线构造密码体制，需要找出椭圆曲线上的数学困难问题。

在椭圆曲线构成的Abel群 $E_p(a,b)$ 上考虑方程 $Q=kP$ ，其中 $P, Q \in E_p(a,b)$ ， $k < p$ ，则由 k 和 P 易求 Q ，但由 P 、 Q 求 k 则是困难的，这就是椭圆曲线上的离散对数问题，可应用于公钥密码体制。Diffie-Hellman密钥交换和ElGamal密码体制是基于有限域上离散对数问题的公钥体制，下面考虑如何用椭圆曲线来实现这两种密码体制。

1. Diffie拟Hellman密钥交换

首先取一素数 $p \approx 2^{180}$ 和两个参数 a 、 b ，则得方程(4.2)表达的椭圆曲线及其上面的点构成的Abel群 $E_p(a,b)$ 。第2步，取 $E_p(a,b)$ 的一个生成元 $G(x_1, y_1)$ ，要求 G 的阶是一个非常大的素数， G 的阶是满足 $nG=O$ 的最小正整数 n 。 $E_p(a,b)$ 和 G 作为公开参数。

两用户A和B之间的密钥交换如下进行：

- ① A选一小于 n 的整数 n_A ，作为秘密钥，并由 $P_A = n_A G$ 产生 $E_p(a, b)$ 上的一点作为公开钥。
- ② B类似地选取自己的秘密钥 n_B 和公开钥 P_B 。
- ③ A、B分别由 $K = n_A P_B$ 和 $K = n_B P_A$ 产生出双方共享的秘密钥。

这是因为 $K = n_A P_B = n_A (n_B G) = n_B (n_A G) = n_B P_A$ 。

攻击者若想获取 K ，则必须由 P_A 和 G 求出 n_A ，或由 P_B 和 G 求出 n_B ，即需要求椭圆曲线上的离散对数，因此是不可行的。

例： $p=211$ ， $E_p(0,-4)$ ，即椭圆曲线为
 $y^2 \equiv x^3 - 4$ ， $G=(2,2)$ 是 $E_{211}(0,-4)$ 的阶为241的一个
生成元，即 $241G=O$ 。A的秘密钥取为
 $n_A=121$ ，公开钥为 $P_A=121(2,2)=(115,48)$ 。B
的秘密钥取为 $n_B=203$ ，公开钥为
 $P_B=203(2,2)=(130,203)$ 。由此得到的共享密钥
为 $121(130,203)=203(115,48)=(161,169)$ ，即共
享密钥是一对数。如果将这一密钥用作单钥
加密的会话密钥，则可简单地取其中的一个
，如取x坐标，或取x坐标的某一简单函数。

2. ElGamal密码体制

(1) ElGamal密码体制的原理

密钥产生过程： 首先选择一素数 p 以及两个小于 p 的随机数 g 和 x ，计算 $y \equiv g^x \pmod p$ 。以 (y, g, p) 作为公开密钥， x 作为秘密密钥。

加密过程： 设欲加密明文消息 M ，随机选一与 $p-1$ 互素的整数 k ，计算 $C_1 \equiv g^k \pmod p$ ， $C_2 \equiv y^k M \pmod p$ ，密文为 $C=(C_1, C_2)$ 。

解密过程：
$$M = \frac{C_2}{C_1^x} \pmod p$$

这是因为

$$\frac{C_2}{C_1^x} \pmod p = \frac{y^k M}{g^{kx}} \pmod p = \frac{y^k M}{y^k} \pmod p = M \pmod p$$

针对椭圆曲线, $E_p(a,b)$:

$$P_m=(x',y')$$

$$x'=k*m+j,$$

$$y'=\sqrt{x'^3+ax'+b}$$

(2) 利用椭圆曲线实现ElGamal密码体制

首先选取一条椭圆曲线, 并得 $E_p(a,b)$, 将明文消息 m 通过编码嵌入到曲线上得点 P_m , 再对点 P_m 做加密变换。

取 $E_p(a,b)$ 的一个生成元 G , $E_p(a,b)$ 和 G 作为公开参数。

p 是个大素数, $nG=O$, n 也是一个大素数

另：p,a,b,G都是公开的参数

用户A选 n_A 作为秘密钥，并以 $P_A = n_A G$ 作为公开钥。任一用户B若想向A发送消息 P_m ，可选取一随机正整数 k ，产生以下点对作为密文：

$$C_m = \{kG, P_m + kP_A\}$$

B: $m \rightarrow P_m(x', y') \rightarrow A$

A解密时，以密文点对中的第二个点减去用自己的秘密钥与第一个点的倍乘，即

实际是加法逆元

$$P_m + kP_A - n_A kG = P_m + k(n_A G) - n_A kG = P_m$$

攻击者若想由 C_m 得到 P_m ，就必须知道 k 。而要得到 k ，只有通过椭圆曲线上的两个已知点 G 和 kG ，这意味着必须求椭圆曲线上的离散对数，因此不可行。

证明解密算法的正确性！明文 m 由点 P_m 获得， $P_m(x', y') \rightarrow m = \text{floor function}(x'/k)$

k是秘密的！
接收方A无需知道k

$PA=nA*G$, nA 是A的私钥

例： 取 $p=751$, $E_p(-1,188)$, 即椭圆曲线为 $y^2 \equiv x^3 - x + 188$, $E_p(-1,188)$ 的一个生成元是 $G=(0,376)$, A的公开钥为 $P_A=(201,5)$ 。假定B已将欲发往A的消息嵌入到椭圆曲线上的点 $P_m=(562,201)$, B选取随机数 $k=386$, 由 $kG=386(0,376)=(676,558)$,
 $P_m+kP_A=(562, 201)+386(201,5)=(385,328)$,
得密文为 $\{(676,558),(385,328)\}$ 。

可见ECC加密, 密文长度是对应明文长度的2倍!

椭圆曲线密码体制的优点

与基于有限域上离散对数问题的公钥体制（如**Diffie-Hellman**密钥交换和**ElGamal**密码体制）相比，椭圆曲线密码体制有如下优点。

(1) 安全性高

攻击有限域上的离散对数问题可以用指数积分法，其运算复杂度为 $O(\exp(\sqrt[3]{(\log p)(\log \log p)^2}))$ ，其中 p 是模数（为素数）。而它对椭圆曲线上的离散对数问题并不有效。目前攻击椭圆曲线上的离散对数问题的方法只有适合攻击任何循环群上离散对数问题的大步小步法，其运算复杂度为 $O(\exp(\log \sqrt{p_{\max}}))$ ，其中 p_{\max} 是椭圆曲线所形成的Abel群的阶的最大素因子。因此，椭圆曲线密码体制比基于有限域上的离散对数问题的公钥体制更安全。

(2) 密钥量小

由攻击两者的算法复杂度可知，在实现相同的安全性能条件下，椭圆曲线密码体制所需的密钥量远比基于有限域上的离散对数问题的公钥体制的密钥量小。

(3) 灵活性好

有限域 $\text{GF}(q)$ 一定的情况下，其上的循环群（即 $\text{GF}(q) - \{0\}$ ）就定了。而 $\text{GF}(q)$ 上的椭圆曲线可以通过改变曲线参数，得到不同的曲线，形成不同的循环群。因此，椭圆曲线具有丰富的群结构和多选择性。

正是由于椭圆曲线具有丰富的群结构和多选择性，并可在保持和RSA/DSA体制同样安全性能的前提下大大缩短密钥长度（目前160比特足以保证安全性），因而在密码领域有着广阔的应用前景。下面给出了椭圆曲线密码体制和RSA/DSA体制在保持同等安全的条件下各自所需的密钥的长度。

表 4-9 ECC 和 RSA/DSA 在保持同等安全的条件下所需的密钥长度（单位为比特）

RSA/DSA	512	768	1024	2048	21000
ECC	106	132	160	211	600

作业：page 247,第4大题（2），（3），（5），（7）

作业：

【一】 在ElGamal加密体制中，设素数 $p=71$ ，本原根 $g=7$ ，

(1) 如果接收方B的公开钥是 $y_B=3$ ，发送方A选择的随机整数 $k=2$ ，求明文 $M=30$ 所对应的密文。

(2) 如果A选择另一个随机整数 k ，使得明文 $M=30$ 加密后的密文是 $C=(59, C_2)$ ，求 C_2 。

【二】椭圆曲线 $E_{11}(1,6)$ 表示 $y^2 \equiv x^3 + x + 6 \pmod{11}$ ，求其上的所有点。

【三】已知点 $G=(2,7)$ 在椭圆曲线 $E_{11}(1,6)$ 上，求 $2G$ 和 $3G$ 。

【四】利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是 $E_{11}(1,6)$ ，生成元 $G=(2,7)$ ，接收方A的秘密钥 $n_A=7$ 。

(1) 求A的公开钥 P_A 。

(2) 发送方B欲发送消息 $P_m=(10,9)$ ，选择随机数 $k=3$ ，求密文 C_m 。

(3) 显示接收方A从密文 C_m 恢复消息 P_m 的过程。

椭圆曲线在模 p 下的运算规则

- 加法规则:

(i) 对所有点 $\mathbf{P} \in E_p$, 则 $\mathbf{P} + \mathbf{0} = \mathbf{0} + \mathbf{P} = \mathbf{P}$, $\mathbf{P} + (-\mathbf{P}) = \mathbf{0}$

(ii) 令 $\mathbf{P} = (x_1, y_1) \in E_p$ 和 $\mathbf{Q} = (x_2, y_2) \in E_p$, 且 $\mathbf{P} \neq -\mathbf{Q}$, 则

$\mathbf{P} + \mathbf{Q} = \mathbf{R} = (x_3, y_3) \in E_p$, 其中:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

椭圆曲线在模 p 下的运算规则(续)

(iii) 如果 s 和 t 为整数, 则对所有的点 $P \in E_p$ 而言,

$$(s+t)P = sP + tP$$

- 乘法规则:

(i) 如果 k 为整数, 则对所有的点 $P \in E_p$ 而言,

$$kP = P + P + \dots + P$$

(ii) 如果 s 和 t 为整数, 则对所有的点 $P \in E_p$ 而言,

$$s(tP) = (st)P$$

椭圆群的构造

- $E_p(a,b)$ 表示模 p 下的椭圆曲线上的整数点，再加上 0 。
- $E_p(a,b)$ 的生成过程
 - (i)对 $x=0,1,\dots,p-1$,计算 $x^3+ax+b(\bmod p)$
 - (ii)对于上一步骤得到的每一结果确定它是否有一个模 p 的平方根，如果没有，则 $E_p(a,b)$ 中没有具有与该结果相应 x 坐标的点。如果有，就有两个平方根 y 和 $p-y$ ，从而点 (x,y) 和 $(x,p-y)$ 都是 $E_p(a,b)$ 的点（如果 $y=0$,只有 $(x,0)$ 一个点）。
- 如取 $p=23,a=b=1$,有 $4*1^3+27*1^2 \pmod{23} = 8 \neq 0$ ，则 $y^2=x^3+x+1$ 是椭圆曲线。 $E_{23}(1,1)$ 是一个模23的椭圆群。

椭圆群的构造(续)

例如: $x=7$.

$$y^2 = 7^3 + 7 + 1 \pmod{23} = 343 \pmod{23} = 6 \pmod{23} = 121 \pmod{23}$$

$351 = (6 + 5 \cdot 23) \pmod{23} = 11^2 \pmod{23}$

$$y = 11 \pmod{23}$$

$$y = -11 \pmod{23} = 12 \pmod{23} \\ = (-11 + 23) \pmod{23} = 12 \pmod{23}$$

(0, 1)	(5, 4)	(9, 16)	(17, 3)
(0, 22)	(5, 19)	(11, 3)	(17, 20)
(1, 7)	(6, 4)	(11, 20)	(18, 3)
(1, 16)	(6, 19)	(12, 4)	(18, 20)
(3, 10)	(7, 11)	(12, 19)	(19, 5)
(3, 13)	(7, 12)	(13, 7)	(19, 18)
(4, 0)	(9, 7)	(13, 16)	

椭圆群运算举例

- $P=(3,10)$, $Q=(9,7)$, 求: $R=(x_3,y_3)=P+Q=?$

$$\lambda = (7-10) / (9-3) = (-3) / 6 = (-1) / 2 = 11 \pmod{23}$$

$$x_3 = 11^2 - 3 - 9 = 109 = 17 \pmod{23}$$

$$y_3 = 11 * (3 - (-6)) - 10 = 89 = 20 \pmod{23}$$

$$R=(17,20)$$

- 计算 $2P$

$$\lambda = (3(3^2) + 1) / (2*10) = 5/20 = 1/4 = 6 \pmod{23}$$

$$x_3 = 6^2 - 3 - 3 = 30 = 7 \pmod{23}$$

$$y_3 = 6 * (3 - 7) - 10 = -34 = 12 \pmod{23}$$

$$2P=(7,12)$$

椭圆曲线密码的公私钥对

密钥对生成:

- 选择一个椭圆曲线 $E: y^2 = x^3 + ax + b \pmod{p}$, 构造一个椭圆群 $E_p(a, b)$ 。
- 在 $E_p(a, b)$ 中挑选生成元点 $G = (x_1, y_1)$, G 应使得满足 $nG = O$ 的最小的 n 是一个非常大的素数。
- 选择一个小于 n 的整数 n_A 作为其私钥, 然后产生其公钥 $P_A = n_A G$;

注: 公开的信息: (E, G, n, P_A)

$|E_p|$ 表示椭圆群 $E_p(a, b)$ 的元素个数, n 是 $|E_p|$ 的素因子。

$$p + 1 - 2\sqrt{p} \leq |E_p| \leq p + 1 + 2\sqrt{p}$$

椭圆曲线密码的加密

加密算法:

(1)将 m 编码成一个数 $m < p$, 在椭圆群 $E_p(a, b)$ 中选择一点

$$P_t = (x_t, y_t)$$

将 m 映射为椭圆曲线
上的一个点 $P_t(x, y)$

(2)在区间 $[1, n-1]$ 内选取一个随机数 k , 计算点 $(x_1, y_1) = kG$ 。

(3)依据接受方的公钥 P_B 计算点 $(x_2, y_2) = kP_B$ 。

(4)计算密文 $C = m \cdot x_t + y_t$ 。

(5)传送加密数据 $\{kG, P_t + kP_B, C\}$ 给接受方。

椭圆曲线密码的解密

解密算法:

(1)接受方接受加密数据 $\{kG, P_t+kP_B, C\}$ 。

(2)接受方使用自己的私钥 n_B 作如下计算:

$$P_t+kP_B - n_B (kG) = P_t+k(n_B G) - n_B (kG)=P_t$$

(3)计算 $m=(C - y_t)/x_t$ ，得明文 m 。

椭圆曲线密码的离散对数问题

- 椭圆曲线密码的离散对数问题是指已知群中的 G 和 P ，求方程 $P=kG$ 中 k 值的问题。

如对基于 F_{23} 的椭圆群 $y^2=x^3+9x+17$ ，求 $P=(4, 5)$ 对于 $G=(16, 5)$ 的离散对数，最直接的方法就是计算的 G 倍数，直到找到 P 。

$$\begin{aligned} G &= (16, 5) & 2G &= (20, 20) & 3G &= (14, 14) & 4G &= (19, 20) \\ 5G &= (13, 10) & 6G &= (7, 3) & 7G &= (8, 7) & 8G &= (12, 17) & 9G &= (4, 5) \end{aligned}$$

因此， P 关于 G 的离散对数是 9 ，对于大素数构成的群 E ，这样计算离散对数是不现实的，事实上现在也没有更好的算法来解离散对数问题。

ECC 的小结

- 安全性能更高（**160**位等同**RSA**的**1024**位）

在保持同等安全的条件下所需的密钥长度(单位为比特)

RSA/DSA	512	768	1024	2048	21000
ECC	106	132	160	211	600

- 计算量小，处理速度快
- 存储空间占用小
- 带宽要求低
- 应用前景非常好，特别在移动通信、无线设备上的应用。

引言

- 公钥密码学的出现极大地促进了网络信息安全理论与技术的发展，从其诞生之日起，就一直是持续的研究热点。

较好地解决了密钥传递和不可否认的问题。

- 如何保护用户公钥的真实性是公钥密码系统中的一个重要问题。

公钥证书较好地解决了公钥的真实性问题，使得PKI能够为网络用户提供较好的安全服务。但公钥证书的管理和维护需要付出巨大的计算、通信和存储代价。

基于身份加密（IBE）概述

最初是在**1984**年，由密码学权威**Shamir**提出了基于身份加密（**IBE, Identity-based Encryption**）方案的概念，其初衷是简化电子邮件系统中的证书管理。当**Alice**要给地址是“**Bob@abc.com**”的**Bob**发邮件时，她只需用公钥“**Bob@abc.com**”加密消息即可，而无需通过其他途径获取**Bob**的公钥证书；**Bob**收到加密消息之后向一个可信第三方证实自己的身份，可信第三方将**Bob**的私钥送给**Bob**，他用该私钥解密消息。在**IBE**中，公钥可以是任意的关于用户身份的字符串；用户向可信第三方认证自己的身份并获得私钥，该过程可以在收到加密消息之前也可在之后完成；

基于身份的公钥体制的基本思想

基于身份的密码系统中，用户的公钥是一些公开的可以**唯一**确定用户身份的信息，一般这些信息称为用户的身份(ID)。在实际应用中，用户的身份可以是姓名、电话号码、身份证号码、IP 地址、电子邮件地址等作为公钥。用户的私钥通过一个被称作私钥生成器PKG (Private Key Generator) 的可信任第三方进行计算得到。可信第三方可以像PKI中的CA一样为多个用户服务。

在这个系统中，用户的公钥是一些公开的身份信息，其他用户不需要在数据库中查找用户的公钥，也不需要公钥的真实性进行检验。

实现基于身份的密码系统的前提条件

- 当**种子密钥** s (PKG的秘密信息---主密钥) 已知时, 能容易地计算出任何可能的公钥所对应的**私钥**。
- 用有种子密钥 s 产生的一些公私钥对计算种子密钥 s 是**困难问题**。

基于身份的加密方案 (举例)

对任意 $a, b \in \mathbb{Z}$, 任意 $P, Q \in G_1$,
 $e(aP, bQ) = e(P, Q)^{ab}$ 。

● 初始化

输入安全参数 k , 生成两个阶为素数 q 的群 G_1, G_2 , 一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 以及 G_1 的一个生成元 P ; 随机选取 $s \in \mathbb{Z}_q^*$, 计算 $P_{\text{pub}} = sP$, 选择安全的 Hash 函数 H_1 和 H_2 。

● 公私钥对生成

输入 $ID \in \{1, 0\}^*$, 计算 $Q_{ID} = H_1(ID)$, 输出私钥 $d_{ID} = sQ_{ID}$, 其中 s 是 PKG 的主密钥。

基于身份的加密方案 (举例)续

● 加密过程

以公钥ID对消息M加密。随机选取 $r \in \mathbb{Z}_q^*$ ，计算

$$Q_{ID} = H_1(ID), \quad g_{ID} = e(Q_{ID}, P_{pub}) \in G_2^*,$$

输出密文 $C = (rP, M(+H_2(g_{ID}^r)))$ 。

● 解密过程

输入用公钥ID加密的密文 $C = (U, V)$ ，计算并输出

$$M = V(+H_2(e(d_{ID}, U)))$$

注： $U = rP$ ， $V = M(+H_2(g_{ID}^r))$

加解密算法的正确性

$$\begin{aligned} V \oplus H_2(e(d_{ID}, U)) &= m \oplus H_2((g_{ID})^r) \oplus H_2(e(sQ_{ID}, rP)) \\ &= m \oplus H_2((g_{ID})^r) \oplus H_2(e(Q_{ID}, P)^{rs}) \\ &= m \oplus H_2((g_{ID})^r) \oplus H_2(e(Q_{ID}, sP)^r) \\ &= m \oplus H_2((g_{ID})^r) \oplus H_2((g_{ID})^r) \\ &= m \end{aligned}$$

IBE的小结

优点:

- 基于身份的加密方案天生就是密钥托管的;
- 不需要对证书进行管理。

不足:

- 身份确认本来就是一件复杂的事情, 尤其用户数量很大。
也就是说, **IBE适合应用于用户群小的场合。**
- 可信第三方如何安全地将用户的**私钥**送到用户的手中。

公钥密码的优点(与对称密码相比)

- 密钥分发简单。
- 需秘密保存的密钥量减少。
- 可以满足互不认识的人之间私人谈话的保密性要求。
- 可以实现数字签名和认证的功能。

公钥密码的不足(与对称密码相比)

- 公钥密码算法比对称密码算法慢。
- 公钥密码算法提供更多的信息对算法进行攻击，如公钥密码算法对选择明文攻击是脆弱的，尤其明文集比较小时。
- 有数据扩展。
- 公钥密码算法一般是建立在对一个特定的数学难题求解上，往往这种困难性只是一种设想。

本讲的主要内容

- 公钥密码体制的简介
- 背包问题
- **RSA**算法
- **ElGamal**算法
- **ECC**算法
- **IBE**算法

谢谢！

