3. RSA的实现

- RSA的硬件实现，其最快速度也是DES的1/1000，512bit的RSA大约为1MB/s，软件实现的速度只有DES的软件实现的1/100，因此在速度上RSA是无法与对称密码体制相比的。
- 目前RSA体制主要用在密钥交换和认证
- 512bit的RSA软件实现可达20KB/s。
- 如果选e=65537时，运算速度可大大加快，这是因为65537的二进制表示中只有两个1，可极大地减少运算量。

- 1)素性检测
- 在RSA的具体实现时，首先要求两个大素数。
- 会不会因为用户的增加而导致会有两个人选择了同样的素数呢？素数是否会被因为更换而用完？
- 素数定理：不超过N的素数大约有N/lnN个，
- 以1024bit来看，它作为两个长度接近512bit的素数乘积被产生。大约有$2^{512}/512$个这样的素数，即大约有$t=10^{151}$个，每对素数形成一个模，则有$C(10^{151}, 2)=10^{300}$个不同的模，而对于给定的模，又可以有许多密钥对可选。 10^{300}个模的概念是，如果给地球上每个人每天10个新模，则可持续(按70亿$=7\times10^{9}$人口算，$10^{300}/2.6\times10^{13})3.84\times10^{287}$年.
- 若要求素数长度在512bit则上述数据为$2^{512}/512-2^{511}/511=2^{511}(2/512-1/511)= 2^{511}\times0.0019=2^{502}$,故在此要求下给地球上每个人每天10个新模，也可持续3×10^{284}年
- 因此不必担心两个人选择同样素数的情况发生，和素数被用完的情况。

- 能切实可行地产生大素数？
- 根据素数定理，如果随机选择一个整数p，则p是素数的概率是(p/lnp)/p=1/lnp。
- 若要求512bit的素数，则有1/lnp≈1/354，若规定是随机选择奇整数，则概率为1/177。
- 适当长度的177个随机奇整数中有一个是素数。
- 因此产生大素数是确实可行的。
- 检测素数的方法有概率测试法。

- 概率测试法就是对给定的大整数进行检验，每次都输出一个结果Yes或No。
- 一种是输出Yes表示该数是素数的概率为0.5，输出No则表示该数肯定不是素数。
- 若N通过了r次检验(即输出都是Yes)，则它不是素数的概率将为2^{-r},当r足够大时，几乎可认为N是素数。
- Solovay-Strassen检验法和Miller-Rabin检验法都是利用这一原理构造的。
- 另一种是输出Yes表示该数肯定是素数，输出No则表示该数不是素数概率为0.5，由于按此方法得到的数一定是素数，故也称这类方法为确定性检验法。

- **Solovay-Strassen检验法的方法是,如果要检验m是否为素数，则在{1,2,…m-1}中随机取n，并验证(n,m)是否等于1，和Jacobi符号J(m,n)是否等于$n^{(m-1)/2} \bmod m$。**
- **这里J(m,n)=** $\left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)$ $(m=p_1p_2\ldots p_r)$

$$\left(\frac{n}{p_i}\right)=\begin{cases}1 & n\text{是}p_i\text{的平方剩余}\\ -1 & n\text{是}p_i\text{的非平方剩余}\end{cases}$$

所谓平方剩余问题就是指，对于给定的一个奇数n和整数a，决定a是否为模n的平方剩余，即判定$x^2=a \bmod n$是否有解，若有解，则a是mod n的平方剩余，否则a是模n的非平方剩余。

- 若m为素数，则有(n,m)=1且J(m,n)= $n^{(m-1)/2} \bmod m$。
- 若m不是素数，则等式$J(m,n)=n^{(m-1)/2} \bmod m$可能成立可能不成立。
- 有结论：对于奇合数，至多有一半使等式成立，即至多有0.5 的概率使上述等式成立。
- 若随机选择100个整数进行检验，上式均成立，则m不是素数的概率小于$2^{-100}=10^{-30}$，因此可认为m是素数。

(1)如果 n 是奇数， $m_1=m_2 \bmod n$， 则 $\left(\frac{m_1}{n}\right)=\left(\frac{m_2}{n}\right)$。

(2)如果 n 是奇数，则 $\left(\frac{2}{n}\right)=\begin{cases}1 & 若 n\equiv\pm1 \bmod 8\\ -1 & 若 n\equiv\pm3 \bmod 8\end{cases}$

(3)如果 n 是奇数，则 $\left(\frac{m_1m_2}{n}\right)=\left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$。

特别当 $m=2^k t$(t 为奇数)，则 $\left(\frac{m}{n}\right)=\left(\frac{2}{n}\right)^k\left(\frac{t}{n}\right)$

(4)如果 m 和 n 是奇数，则 $\left(\frac{m}{n}\right)=\begin{cases}-\left(\frac{n}{m}\right) & 若 m\equiv n\equiv 3 \bmod 4\\ \left(\frac{n}{m}\right) & 否则\end{cases}$

应用上述 4 个特性，可以在多项式时间内计算 Jacobi 符号。

- Miller-Rabin检验法也是一个多项式时间算法，它比Solovay-Strassen检验法快，执行一次的错误概率最多为1/4。
- 对于奇整数n的Miller-Rabin素性测试算法如下：
- (1)令$n-1=2^k m$，m是奇数；
- (2)对i=1 to t do
- ①选择随机整数a(2≤a≤n-2)；
- ②计算$b \equiv a^m \bmod n$;
- ③If $b \equiv 1 \bmod n$，then n是素数 and 返回,else 令j=1
- ④If j=k then n是合数，算法终止
- ⑤If $b \equiv -1 \bmod n$, then n是素数 and 返回，
- else 计算$b \equiv b^2 \bmod n$, j=j+1,goto ④

- 确定性检验法是通过对给定的大整数进行检验，下面介绍一种确定性检验法。
- 采用了基于Pocklington定理的特殊情形，并将其改造为一递归算法加以实现
- 定理的特殊情形的描述：
- 定理：设n=2RF+1，其中F的真分解为F=，如果存在整数a满足:$a^{n-1}\equiv 1 \bmod n$，且$(a^{(n-1)/q_j}-1,n)=1(\ j=1,\ldots r)$,

那么 n 的每一个素因子 p 具有 $p=mF+1$ 的形式，其中 $m^{\geq}1$。更进一步，如果 $F>\sqrt{n}$ 或者 F 为奇数且 $F>R$，那么 n 是素数。

- 函数 PrimeTest(a)对较小的整数 a 进行有效地素性判别，当且仅当 a 是素数时返回 TRUE，
- 当且仅当 a 不能被小于等于 b 的素数除尽时，函数
- TrialDivision(a,b)返回值为 TRUE。
- 函数 CheckLemmal(n,a,q)验证所给参数是否满足引理
- 中的条件，满足时可知 n 是素数，返回 TRUE。
- 函数 GenRelativeSize 根据条件概率分布，可以从区
- 间[0.5,1]中选择一个值作为相对规模。
- 函数 Power2 用于 2 的幂运算。
- 试除判定法的边界 g 被设定为某一常数 c_opt 的 k^2
- 倍，其中 c_opt 的最优值可通过试验来确定，这里取
- 为 0.1。
- 常数 margin 保证了 R 的取值范围应该足够大，以保
- 证该区间内至少包含一些成功的 R。
- 算法可用来生成几乎随机的可证安全素数

- 密钥的产生涉及求剩余类环的乘法逆
- 对任意的正整数n,Z_n是交换环(剩余类环)对Z_n中任意一个元素，存在关于模n逆元的条件是该数与n互质。
- 用Euclidean算法。

2)快速加密解密方法

然后先做预计算

$$\left.\begin{aligned} a^2 &= a\cdot a \\ a^4 &= a^2\cdot a^2 \\ &\vdots \\ a^{2^{r-1}} &= a^{2^{r-2}}\cdot a^{2^{r-2}} \end{aligned}\right\} r-1\text{次乘法}$$

$$a^b = a^{b_0+2b_1+\cdots+2^{r-1}b_{r-1}} = a^{b_0}(a^2)^{b_1}\cdots(a^{2^{r-1}})^{b_{r-1}}$$

$$(a^{2^i})^{b_i} = \begin{cases} 1 & b_i = 0 \\ a^{2^i} & b_i = 1 \end{cases}$$

然后根据b_i=1取出相应的与其他项相乘，最多需r-1次乘法。故整个幂运算最多需要2r-2次模乘法运算，即$2\lceil \log n \rceil$-2次模乘法运算。

- 为了提高RSA算法的解密速度，解密时可以按下面方法进行计算：
- 设密文$c=m^e \bmod n, n=pq$。
- 设$c_1 \equiv c \bmod p$, $c_2 \equiv c \bmod q$,
- $d_1 \equiv d \bmod (p-1)$, $d_2 \equiv d \bmod (q-1)$,
- $m_1 \equiv c_1^{d1} \bmod p$,
- $m_2 \equiv c_2^{d2} \bmod q$。
- c_1、c_2、d_1和d_2是容易计算的，由此可以求得有m_1和m_2。
- 由中国剩余定理解同余方程组$m \equiv m_1 \bmod p$, $m \equiv m_2 \bmod q$,就可求出m。
- 该方法可提高解密速度4-8倍。

- 3)中国剩余定理
- 称$x\equiv b_1 \bmod m_1$为同余式方程，满足该式的每个x都是该方程的解。
- 如对于同余式方程$x\equiv 4 \bmod 7$，对任意的整数k，4+7k都是此方程的解。
- 需要求n个同余式方程$x\equiv b_1 \bmod m_1, x\equiv b_2 \bmod m_2, \ldots, x\equiv b_n \bmod m_n$的共同解，这就是所谓的联立同余式问题。
- 该问题有共同解的充要条件是$(m_i,m_j)|(b_i,b_j)$，这里$i\neq j$，$i,j=1,2,\ldots n$。

- 定理A：若存在a，满足n个同余式方程$x \equiv b \bmod m_i (i=1,2,\ldots n)$，即$a \equiv b \bmod m_i (i=1,2,\ldots n)$，则有$a \equiv b \bmod \mathrm{lcm}(m_1,m_2,\ldots,m_n)$。
- 定理B(中国剩余定理)：设$m_1,m_2,\ldots,m_n$是两两互素的正整数，则$x \equiv b_i \bmod m_i (i=1,2,\ldots n)$在模$m_1 m_2 \ldots m_n$下有唯一解。
- 证明：令$M=m_1 m_2 \ldots m_n$，$M_j=M/m_j$，求y_j满足$M_j y_j \equiv 1 \bmod m_j (j=1,2,\ldots n)$。
- 因为$(M_j,m_j)=1$，故解y_j是存在的。
- 令$x=b_1 M_1 y_1+b_2 M_2 y_2+\ldots+b_n M_n y_n \bmod M$。
- 证明该表达式就是$x \equiv b_i \bmod m_i (i=1,2,\ldots n)$在模$m_1 m_2 \ldots m_n$下的解。

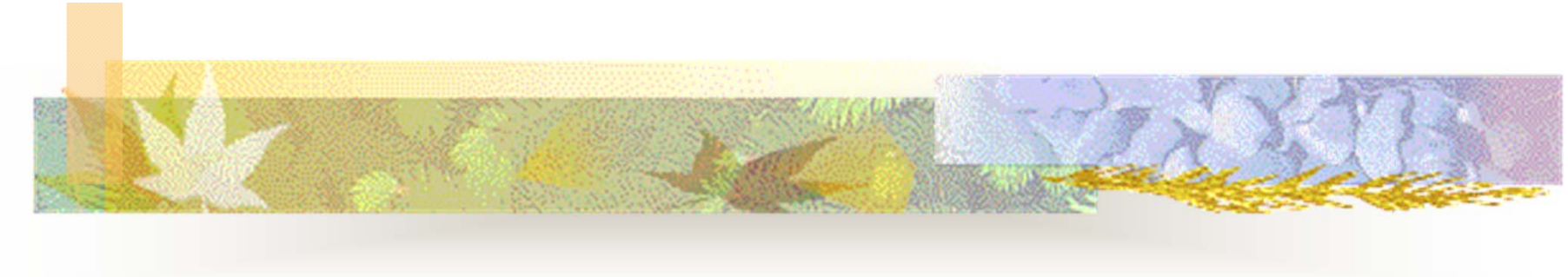
$$\begin{cases} x = 1 \bmod 2 \\ x = 2 \bmod 3 \\ x = 3 \bmod 5 \end{cases}$$

- 4)Euclidean算法
- 用来求最大公因子gcd(n,b),令$r_0=n$, $r_1=b$
- $r_0=q_1r_1+r_2$ $0<r_2<r_1$
- $r_1=q_2r_2+r_3$ $0<r_3<r_2$
- ……
- $r_{m-2}=q_{m-1}r_{m-1}+r_m$ $0<r_m<r_{m-1}$
- $r_m=q_mr_m$
- 该算法可以确定最大公因子$gcd(n,b)=r_m$
- 若$r_m=1$，则说明n,b互质
- 为了计算出b关于模n的逆，需要改进

- 在上面方案中，$q_j=[r_{j-1}/r_j]$,当$r_j\neq0$
- 引进2个数列，$t_0,t_1,\ldots,t_m$,和$s_0,s_1,\ldots s_m$
- $t_0=0,\ t_1=1,\ t_j=t_{j-2}-q_{j-1}t_{j-1}(j>1)$
- $s_0=1,\ s_1=0,\ s_j=s_{j-2}-q_{j-1}s_{j-1}(j>1)$
- 定理：对于$0\leq j\leq m$,有$r_j=s_jr_0+t_jr_1$
- 推论：若$gcd(n,b)=1$,则$b^{-1}\bmod n=t_m\bmod n$

3.5.3 ElGamal密码体制

ElGamal于1984年提出了这一体制，它是基于离散对数问题的公钥密码体制。



- (1)密钥的产生：随机选取一个大素数p，且p-1有大素数因子，
- 在p-1阶循环群中选一本原元a，用户B可在Z_p^*中任取元素SK作为秘密密钥，并计算
- $PK=a^{SK} \bmod p$，将PK作为其公开钥，与p和a一起公开。
- (2)加密过程
- 任何用户要向用户B发送明文消息m(m<p)，可用其公开钥进行加密，并增加一随机数，
- 其加密过程如下
- i)0与p-1之间随机取一整数k
- ii)计算$y_1=a^k \bmod p$
- $y_2=mPK^k \bmod p$
- iii)取(y_1,y_2)作为m的密文发给B。

- (3)解密过程：
- 用户B对传来的密文(y_1,y_2)的解密很简单，计算$y_2(y_1^{SK})^{-1} \bmod p$，即为明文m。
- 该系统的特点是，由于密文由明文和随机数来确定，故是非确定性加密，
- 对同一明文在不同时刻发送，因随机数k不同而给出不同的密文，
- 明文m是通过乘以PK^k来掩盖的。
- 缺陷是由于把a^k也作为密文传送出去，
- 密文信息比明文信息扩大一倍。

- 作为合法接收者，由于知道秘密密钥，故容易计算y_1^{SK}和其在Z_p^*的逆，从而得到明文m。
- 任何不知道SK的人，则要想由(y_1,y_2)求出m，
- 一种攻击手段就是解离散对数问题，而目前的有效算法都是p的指数级，
- 因此只要p取得足够大，通常应为150位以上(十进制)。

- 另一种攻击手段就是设法求出SK的部分位，然后再进行穷尽随机搜索，
- 为保证安全性就要保证尽可能少的密钥位被求出。
- 当$p-1=2^s t$(t为奇数)，容易计算SK的最低s位。
- 应使s小，这就要求t尽可能大，
- 通常希望p-1有一个大的素因子。

3.5.4 椭圆曲线体制

- ElGamal是建立于离散对数在Z_p^*难解基础上的公钥密码体制，如果我们把Z_p^*推广到一般乘法群上，就可建立在一般乘法群上的加密体制。
- 1.一般乘法群上的离散对数问题
- 设(G,*)为有限群，$\alpha \in G$，H是由α生成的子群，$H=\{\alpha^i | i \geq 0\}$，
- 设$\beta \in H$，在$Z_{\|H\|}^*$中找唯一整数a，使得$\alpha^a=\beta$，用$log_\alpha \beta$表示a。

- (1)密钥的产生：用户B随机选取$\alpha \in G$，构造α的生成子群H，$Z_{||H||}^{*}$上随机选整数a作为秘密密钥，并计算$\beta=\alpha^{a} \in H$，将β作为其公开钥，与α一起公开。
- (2)加密过程
- 任何用户要向用户B发送明文消息$m(m \in H)$，可用其公开钥进行加密，并增加一随机数，其加密过程如下
- i)0与||H||-1之间随机取一整数k
- ii)在群(G,*)上计算$y_1=\alpha^{k} \in H$
- $y_2=m*\beta^{k} \in H$
- iii)取(y_1,y_2)作为m的密文发给B。

- (3)解密过程：
- 用户B对传来的密文(y_1,y_2)的解密很简单，在群$(G,*)$上计算$y_2(y_1^{SK})^{-1}\in H$ ，即为明文m。
- 能用作密码体制的乘法群应确保离散对数在该群上是难解的。
- 此外应保证该群到有限加法群上的同构映射是难找到的或是不容易计算的。
- 在有限加法群上的离散对数问题是容易解的，而任何有限群都同构于某个有限加法群。

- 但对于任意素数p，没有一个通用有效算法计算同构映射，因此是有可能构造出安全的密码系统的。
- 目前通常考虑在$GF(p^n)$上建立，研究较多的是$GF(2^n)$，穷尽搜索的复杂性为，

$$e^{1.098+\sqrt[3]{n(\ln n)^2}}$$

- 对于大的n(n>800)，要求n至少有一个大的素因子，否则有可能被攻破。

- 2.椭圆曲线
- 1985年，Neil Koblitz和Victor Miller分别独立提出了椭圆曲线密码体制(ECC)，依据是定义在椭圆曲线点群上的离散对数问题的难解性，
- 用来建立密码体制和数字签名体制，还可建立密钥的公开交换体制。
- 主要介绍Z_p上的椭圆曲线(p是大于3的素数)，

- 定义在域F上的曲线是满足Weierstrass方程的点$(x,y)\in F^2$的集合。所谓Weierstrass方程就是如下形式：
- $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$
- 其中系数$a_i\in F(i=1,2,3,4,6)$。如果方程平滑，即$f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$的两个偏导数不同时为零。则该方程就确定了一条椭圆曲线。

- 如果知道域F的特征，则可以简化方程的一般形式。
- 如果char(F)≠2，则可以令$y'=y-(a_1x-a_3)/2$，
- 原方程可以化为一条同构曲线：
- $y^2=x^3+a'_2x^2+a'_4x+a'_6$

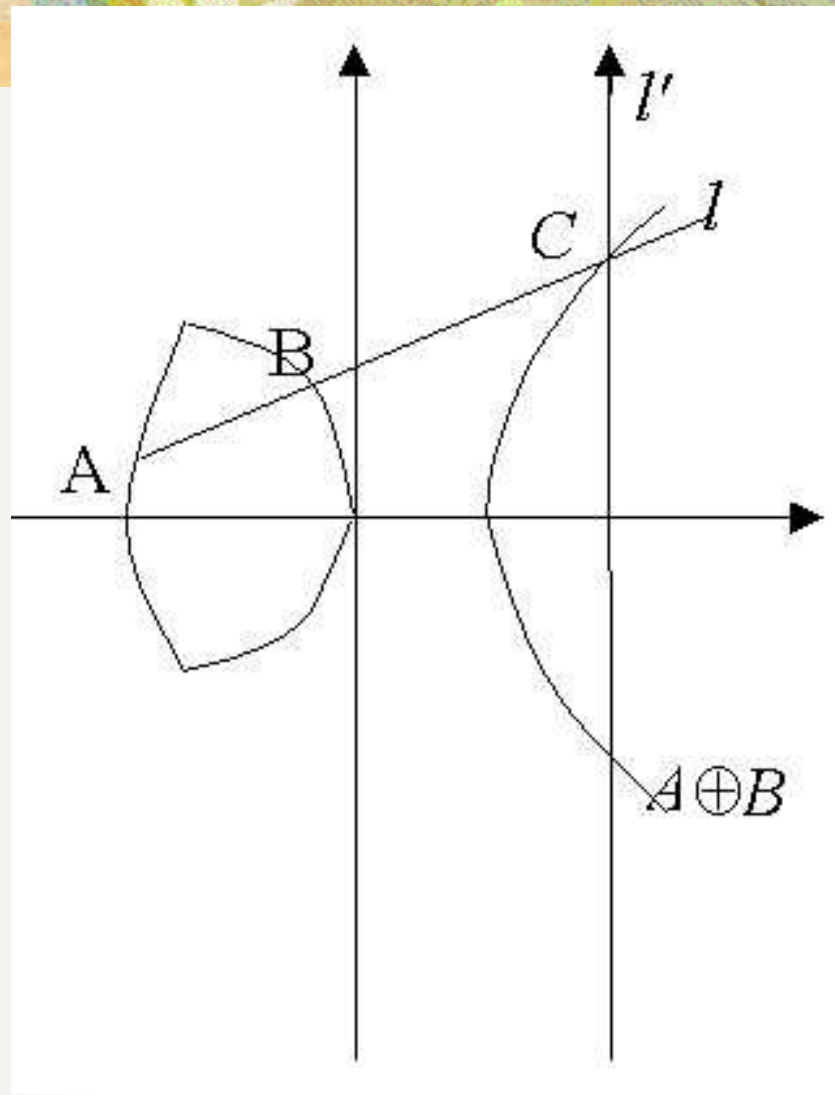
- 如果char(F)≠2，char(F)≠3，进一步代换：
- 令$x'=(2x-3a'_2)/36$, $y''=y'/216$,
- 则化成下面的形式（不再用x'，y''）：
- $y^2=x^3+ax+b$
- 如果多项式x^3+ax+b没有重根，则该曲线是平滑的，即该曲线定义了一条椭圆曲线。
- 而多项式x^3+ax+b没有重根，等价于判别式$4a^3+27b^2\neq 0$

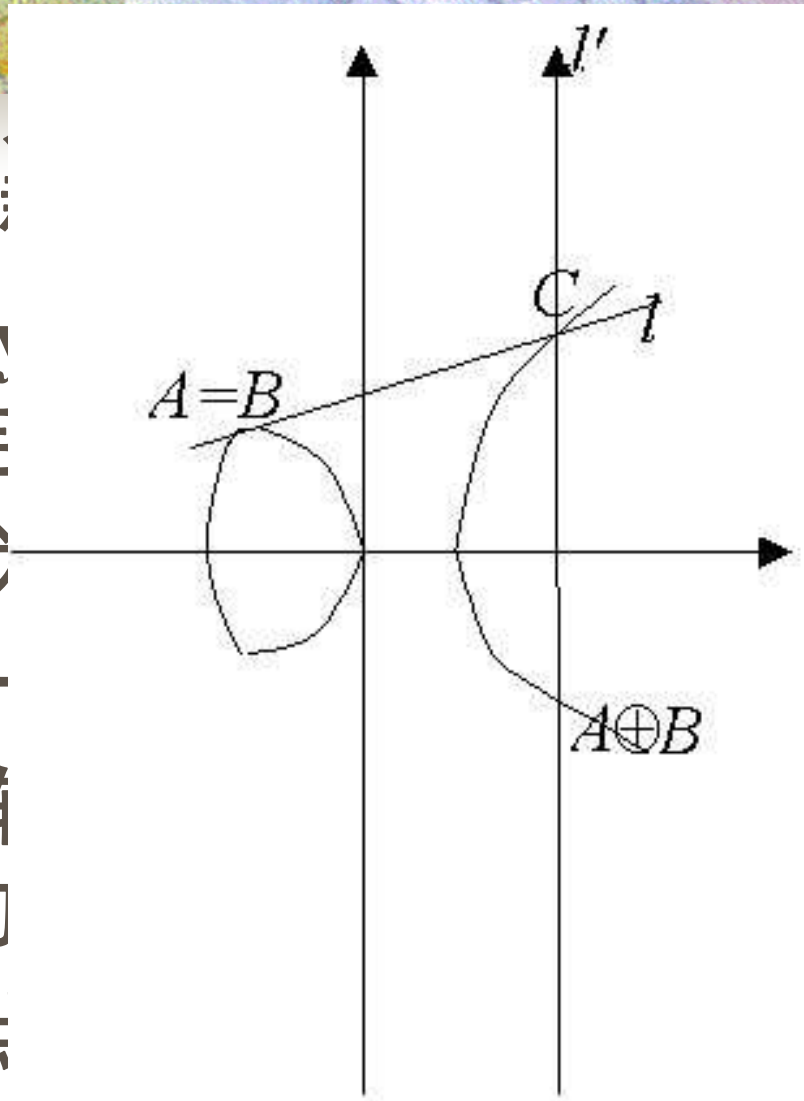
- 如果char(F)=2则有两种情况：
- Weierstrass方程中的$a_1=0$或者$a_1\neq 0$。
- 若$a_1=0$，做代换：$(x,y)\rightarrow(x+a_2,y)$，生成下面形式的曲线：
- $y^2+a'_3y=x^3+a'_4x+a'_6$，称为超奇异曲线
- 若$a_1\neq 0$，做代换：$(x,y)\rightarrow(a_1^2x+a_3/a_1, a_1^3y+(a_1^2a_4+a_3^2)/a_1^3)$，生成下面形式的曲线：
- $y^2+xy=x^3+a'_2x^2+a'_6$，称为非奇异曲线

- 定义3.2：Z_p上的椭圆曲线是由曲线方程$y^2=(x^3+ax+b) \bmod p$所确定的所有曲线上的点$(x,y)(x,y \in Z_p)$连同一个称为无穷远点O一起组成的集合，记为$E_{Z_p}(a,b)$。这里参数$a,b \in Z_p$，满足$4a^3+27b^2 \neq 0 \bmod p$。
- 已有结论表明，$E_{Z_p}(a,b)$的元素个数范围是

$$p+1-2\sqrt{p} \leq |E(Z_p)| \leq p+1+2\sqrt{p}$$

- 例：设E为Z_{11}上的椭圆曲线$y^2=x^3+x+6$，
- 如何确定椭圆曲线的点，对每个$x\in Z_{11}$,计算$t=x^3+x+6 \bmod 11$，然后考察其值是否为某个数的平方，当然这是在模11下的。也就是所谓的模11平方剩余。
- 利用Euler准则来判断是否为平方剩余。
- 定理(Euler准则)：设p为素数，则对任意$x\in Z_p^*$，x是平方剩余当且仅当 $x^{(p-1)/2}=1 \bmod p$
- 事实上$x^{(p+1)/2}=x \bmod p$
- 对素数$p\equiv 3 \bmod 4$,模p的平方剩余的平方根是$\pm t^{(p+1)/4} \bmod p$
- 则本例为$\pm t^{(11+1)/4} \bmod 11=\pm t^3 \bmod 11$
- 例：x=0,t=6, $6^{(11-1)/2}=6^5=7 \bmod 11$
- 例：x=2,t=5, $5^{(11-1)/2}=5^5=1 \bmod 11$
- $\pm 5^{(11+1)/4}=\pm 5^3=\pm 3*5=\pm 4$,即4，7
- 故
- $E(Z_{11})=\{(2,4),(2,7),(3,5),(3,6),(5,2),(5,9),(7,2),(7,9),(8,3),(8,8),(10,2),(10,9),O\}$
- 即$E(Z_{11})$有13个元素，


l′
C
l
B
A
A⊕B


l′
C
l
A=B
A⊕B

- (1)当A≠B，因为*l*是A和B的连线，所以*l*的方程是$y=kx+c$，其中$k=(y_2-y_1)/(x_2-x_1)$，$c=y_1-kx_1$
- 将它代入椭圆曲线方程：
- $(kx+c)^2=x^3+ax+b$，
- (2)当A=B，则椭圆曲线方程关于x求导，得：
- $y'|_{x=x1}=(3x_1^2+a)/2y_1=k$。
- 则直线方程*l*为$y-y_1=k(x-x_1)$。
- 即$y=kx+(y_1-kx_1)$。
- 令$c=y_1-kx_1$，则方程可表达为$y=kx+c$。
- 将它代入椭圆曲线方程：
- $(kx+c)^2=x^3+ax+b$

- 关于运算⊕我们有
- ①对$\forall P \in E(Z_p)$，$O \oplus P = P$。
- ②对$\forall (x_1,y_1),(x_2,y_2) \in E(Z_p)$，
- 若$x_1 \neq x_2$，则
- $(x_1,y_1) \oplus (x_2,y_2) = (k^2 - x_1 - x_2, -y_1 + k(x_1 - x_3))$。其中$k = (y_1 - y_2)/(x_1 - x_2)$, $x_3 = k^2 - x_1 - x_2$
- 若$x_1 = x_2, y_1 = y_2$,则$(x_1,y_1) \oplus (x_1,y_1) = (k^2 - 2x_1, -y_1 + k(x_1 - x_3))$，其中$k = (3x_1^2 + a)/2y_1$, $x_3 = k^2 - 2x_1$,
- 若$x_1 = x_2, y_1 = -y_2$,则$(x_1,y_1) \oplus (x_2,y_2) = O$
- 容易证明$(E(Z_p), \oplus)$为Abel群，其单位元是O，而对$\forall (x,y) \in E(Z_p)$，其逆元$-(x,y) = (x,-y)$。
- $E(Z_{11})$中除单位元O外，其他元素都是E的生成元

- 有限域F_q上的椭圆曲线点群与有限域上的乘法群F_q^*有很多相似之处，它们都是Abel群且元素个数比较接近。
- 但前者有一个重要优势，在给定的有限域F_q上，可以构造很多不同的椭圆曲线点群，有许多不同的群阶可选择，
- 提供了丰富的有限Abel群资源，这在密码应用中有很重要的意义。

- 用$E_p(a,b)$表示在曲线$y^2=x^3+ax+b$上生成的交换群，其中域$F=Z_p$。
- 如果$p=2 \bmod 3$，且$a=0$，则$E_p(0,b)$是阶为$p+1$的循环群$(0<b<p)$
- 下面给出一种椭圆曲线上的RSA体制，该系统是基于椭圆曲线$E_N(0,b)$的。
- $N=pq$公开，素数p,q保密，使用的椭圆曲线为$E_N(0,b)$。且满足$p=2 \bmod 3$, $q=2 \bmod 3$
- 明文空间和密文空间都是$E_N(0,b)$。
- $|E_N(0,b)|=lcm(p+1,q+1)$

- 公开密钥 $e \in Z_{|E_N(0,b)|}$，并且 $\gcd(e, |E_N(0,b)|)=1$。
- 秘密密钥d满足$ed = 1 \bmod |E_N(0,b)|$
- 加密算法：设$m=(m_x,m_y)$是椭圆曲线上的点，$c=em$
- 解密算法：$m=dc$
- 椭圆曲线上的RSA体制安全性取决于N的分解难度

- p=239.q=401,N=95839
- $|E_N(0,b)|=lcm(p+1,q+1)=16080$
- 随机取e=5891，则d=12971，公开N和e。
- 若要加密明文(66321,24115),
- 计算密文:

c=em=5891(66321,24115)=(79227,19622)

- 解密时,
- 计算：

dc=12971(79227,19622)= (66321,24115)

- 3.椭圆曲线密码体制(ECC)
- 可以在椭圆曲线点群$E(F_q)$上定义离散对数问题。
- 定义3.3：设$E(F_q)$为椭圆曲线点群，$P \in E(F_q)$，x为正整数，$Q=xP \in E(F_q)$，其中xP表示x个P进行“⊕”运算。由P和Q确定x，就称为椭圆曲线离散对数问题。
- 椭圆曲线离散对数问题目前还没有有效算法，普遍认为椭圆曲线离散对数问题比整数分解问题和Z_p^*上的离散对数问题要难，
- 有可能利用椭圆曲线离散对数问题建立更加安全的公钥密码体制。

- 在椭圆曲线上建立密码体制的基本方法是：
- 选取有限域F_q和定义在F_q上的椭圆曲线$E(F_q)$，并取$E(F_q)$上的一个阶为素数n的点(x_P,y_P)，有限域F_q、点(x_P,y_P)和椭圆曲线参数a、b作为系统的公共信息；
- 系统中的每个用户可在{1,2,…n-1}中任选一个整数d_i作为秘密密钥，在$E(F_q)$上计算$e_i=d_i(x_P,y_P)$，e_i就是用户的公开密钥。
- 建立椭圆曲线上的ElGamal密码体制：
- 当用户A要向用户B发送信息m，
- 先将m转换成$E(F_q)$的元素m'，
- 在{1,2,…n-1}中随机选取数k，
- 分别计算$y_1=k(x_P,y_P)$,$y_2=m'\oplus ke_B$，
- 把(y_1,y_2)送给B；
- B收到(y_1,y_2)后，计算$y_2-d_By_1=m'$,再转换成m。

- 例：在上例的椭圆曲线$E(Z_{11})$中取点$(x_P,y_P)=(2,7)$，用户B选择随机整数d=5，A将明文$m=(10,2)\in E(Z_{11})$加密送给B，
- $e=5(2,7)=(((2,7)\oplus(2,7))\oplus((2,7)\oplus(2,7))\oplus(2,7)$
- $=((5,2)\oplus(5,2))\oplus(2,7)=(10,2)\oplus(2,7)=(3,6)$
- 该方法存在一个问题：
- 要求明文空间由椭圆曲线中的点构成，而目前并没有一个高效的确定性算法来产生E中的点。
- Menezes和Vanstone提出了一个改进方案，使得可以允许明文、密文不必是椭圆曲线上的点，

- 令E为是Z_p上的椭圆曲线，它包含一个循环子群H，并且在H上离散对数问题是难处理的，明文$m \in Z_p^* \times Z_p^*$，密文$c \in E \times Z_p^* \times Z_p^*$。
- 取H上的生成元(x,y)，把Z_p、点(x,y)和椭圆曲线参数a、b作为系统的公共信息；
- 系统中的每个用户可在{1,2,…|H|-1}中任选一个整数d_i作为秘密密钥，在E上计算$e_i=d_i(x,y)$，e_i就是用户的公开密钥；
- 用户A要向用户B发送信息$m=(m_1,m_2) \in Z_p^* \times Z_p^*$，先在{1,2,…|H|-1}中随机选取数k，分别计算$y_0=k(x,y),(c_1,c_2)=ke_B$,
- $y_1=c_1m_1 \bmod p, y_2=c_2m_2 \bmod p$,
- 并把(y_0,y_1,y_2)送给B；
- B收到(y_0,y_1,y_2)后，计算$(c_1,c_2)=d_By_0, m_1=y_1c_1^{-1} \bmod p$, $m_2=y_2c_2^{-1} \bmod p$。

- 例：同前例一样取点$(x_P,y_P)=(2,7)$，用户B选择随机整数d=5，用户A要将明文m=(9,2)加密送给B

- 作业：p110　11,12,13
- 补充：1.证明：对于$0\le j\le m$,有$r_j=s_jr_0+t_jr_1$
- 2.证明：若gcd(n,b)=1,则
- $b^{-1}\mathrm{mod}n= t_m\mathrm{mod}n$
- 3.密钥的产生:A随机选取两个大素数P和Q，且它们与(P-1)和(Q-1)互素，并计算P‘和Q’，使得
- PP‘=1mod(Q-1),QQ’=1mod(P-1)。
- A公布N=PQ为自己的公开密钥
- 加密:当用户B要向A发送信息M时，就可利用N进行加密：密文$C=M^N\mathrm{mod}N$
- 解密：用中国剩余定理求M,使得M满足$C^{P‘}\mathrm{mod}Q=M$, $C^{Q’}\mathrm{mod}P=M$。
- 证明：解密算法的正确性。

- project 2：编程实现64bit的RSA(包括素数和密钥对产生),实现传送SDES加密算法所要用的密钥，并与SDES算法一起形成传送SDES加密算法，然后用SDES加密算法加密的完整体系。
- 提供:说明文档,源码,可执行程序,通过加密实验,给出运行结果.
- 递交时间：必须在12月11日24点之前，网上上传