《现代密码学》第七章

公钥密码（二）

上节内容回顾

- 对称密码体制面临的问题
- 公钥密码体制的发展
- 单向陷门函数及构造

本节主要内容

- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

本节主要内容

- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

RSA加密算法及其应用

RSA算法是1978年由R.Rivest, A.Shamir和L.Adleman 提出的一种用数论难题构造的公钥密码体制。

R L Rivest, A Shamir, L Adleman, "On Digital Signatures and Public Key Cryptosystems", Communications of the ACM, vol 21 no 2, pp120-126, Feb 1978

RSA加密算法及其应用

1） 密钥的产生

① 选两个安全的大素数p和q。

② 计算$n=p\times q$，$\varphi(n)=(p-1)(q-1)$，其中$\varphi(n)$是n的欧拉函数值。

③ 选一整数e，满足$1<e<\varphi(n)$，且$\gcd(\varphi(n),e)=1$。

④ 计算d，满足$d\cdot e\equiv 1 \mod \varphi(n)$，即$d$是$e$在模$\varphi(n)$下的乘法逆元。因$e$与$\varphi(n)$互素，故它的乘法逆元存在且唯一。

⑤ $\{e,n\}$为公开密钥，$\{d,n\}$为秘密密钥。

RSA加密算法及其应用

2） 加密

加密时首先将明文分组，使得每个分组m值小于n，即分组长度小于$\log_2 n$。然后对每个明文分组m，作加密运算：

$$c \equiv m^e \bmod n$$

3） 解密

对每个密文分组的解密运算：$m \equiv c^d \bmod n$

RSA加密算法及其应用

4）正确性

证明： 若m与n互素，由加密过程知$c \equiv m^e \bmod n$，所以

$$c^d \bmod n \equiv m^{ed} \bmod n \equiv m^{k\varphi(n)+1} \bmod n$$

由Euler定理知 $m^{\varphi(n)} \equiv 1 \bmod n$,

所以 $m^{k\varphi(n)} \equiv 1 \bmod n$,

进而 $m^{k\varphi(n)+1} \equiv m \bmod n$,

即 $c^d \bmod n \equiv m$.

RSA加密算法及其应用

5) 实例

- ① 密钥产生

Bob选p=7，q=17. 求$n=p\times q$=119，$\varphi(n)=(p-1)(q-1)$=96.
取e=5，满足$1<e<\varphi(n)$，且$\gcd(\varphi(n),e)=1$，
因为$77\times5=385=4\times96+1$，所以满足$d\cdot e=1 \bmod 96$的$d$为77，
因此Bob的公开密钥为{5，119}，秘密密钥为{77，119}.

- ② 加密

设Alice加密明文$m=19$给Bob，则加密过程为
$c\equiv19^5 \bmod 119\equiv2476099 \bmod 119\equiv66$;

- ③ 解密

Bob用私钥解密密文66，过程为 $m\equiv66^{77}\bmod 119\equiv19$.

RSA加密算法及其应用

6）安全性

整数分解问题：已知n是两个大素数的乘积，求n的素分解；

如果RSA加密算法的模数n被成功地分解为$p \times q$，则获得$\varphi(n)=(p-1)(q-1)$，从而攻击者能够从公钥e解出私钥d，即$d \equiv e^{-1} \bmod \varphi(n)$，完全破译.

RSA加密算法及其应用

- 至今还未能证明分解大整数就是NPC问题，也许有尚未发现的多项式时间分解算法.
- 随着人类计算能力的不断提高，原来被认为是不可能分解的大数已被成功分解.

例如RSA-129（即n为129位十进制数，大约428个比特）已在网络上通过分布式计算历时8个月于1994年4月被成功分解，RSA-130 已于1996年4月被成功分解.

RSA-768 has 232 decimal digits and was factored on December 12, 2009 by Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Joppe W. Bos, Dag Arne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann

RSA加密算法及其应用

- 分解算法的进一步改进

过去分解算法都采用二次筛法，如对RSA-129的分解. 而对RSA-130的分解则采用了一个新算法，称为推广的数域筛法，该算法在分解RSA-130时所做的计算仅比分解RSA-129多10%.

综上所述，*在使用RSA算法时对其密钥的选取要特别注意其大小。估计在未来一段比较长的时期，密钥长度介于1024比特至2048比特之间的RSA是安全的.*

RSA加密算法及其应用

7）安全参数

- **|p-q|要大**

因为 $\frac{(p+q)^2}{4}-n=\frac{(p+q)^2}{4}-pq=\frac{(p-q)^2}{4}$，

如果$|p-q|$小，则 $(p-q)^2/4$ 也小；因此$(p+q)^2/4$ 稍大于n，即$(p+q)/2$稍大于$n^{1/2}$。那么

① 顺序检查大于$n^{1/2}$的每一整数x，直到找到一个x使得x^2-n是某一整数（记为y）的平方。

② 由$x^2-n=y^2$，得$n=(x+y)(x-y)$，可得n的分解.

RSA加密算法及其应用

- ***p*-1和*q*-1都应有大素因子**

设攻击者截获密文c，可如下进行重复加密：

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

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

$$\cdots$$

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

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

RSA加密算法及其应用

若 $c^{e^{t+1}} \equiv c(\bmod n)$ ，即 $\left(c^{e^t}\right)^e \equiv c(\bmod n)$ ；

又因为 $m^e \equiv c(\bmod n)$ ，所以 $c^{e^t} \equiv m(\bmod n)$，即在重复加密的倒数第2步就可以恢复出明文$m$.

$$\because c^{e^{t+1}} \equiv c(\bmod n), \quad \therefore \gcd(e^{t+1}-1,(p-1)(q-1)) = d > 1;$$

$$\because e^{t+1}-1 \equiv 0 \bmod d, \quad \therefore \gcd(t+1,\phi(d)) = g > 1$$

为使t大，p-1和q-1都应有大的素因子

RSA加密算法及其应用

- 不选取太小的加密指数

若选取较小的e指数(e. g.，$e=3$)，

如果要加密的明文$m<n^{1/e}$，则加密后的密文$c<n$；

攻击者直接求$c^{1/e}$(密文c的e次方根)，就可恢复真正的明文m。

RSA加密算法及其应用

- 不同用户需使用不同的模数

RSA的共模攻击：

若系统中用户共用一个模数n，而拥有不同的e和d;

若存在同一明文（设为m）分别用不同的公钥（$e1$和$e2$）加密，

$$c1 = m^{e1} \bmod n \; ; \quad c2 = m^{e2} \bmod n$$

设攻击者截获n、$e1$、$e2$、$c1$和$c2$，$\gcd(e1,e2)=1$，则他可以恢复m。

RSA加密算法及其应用

算法：因为$e1$和$e2$互质，故用Euclidean算法能找到r和s，满足：

$$r * e1 + s * e2 = 1$$

则

$$(c1)^r * (c2)^s = (m^{e1})^r * (m^{e2})^s \bmod n$$

$$= m^{r * e1 + s * e2} \bmod n = m \bmod n$$

RSA加密算法及其应用

为保证RSA算法足够安全，参数须满足下面几个基本要求：

- 需要选择足够大的素数p，q，$|p-q|$较大，且$(p-1)$和$(q-1)$没有小的素因子；
- e对所有用户可以是相同的，建议使用$e=2^{16}-1=65535$;
- 解密指数比较大，$d>n^{1/2}$?
- 不同用户不共用模数n.

RSA算法

8）RSA的计算问题

- RSA的加密与解密的模幂运算

$66^{77} \bmod 119 =$

$1.27316015002712725024996823827 45e+140 \bmod 119$

首先，用模运算的性质：

$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

减小中间运算结果.

RSA算法

幂运算的快速算法

例如：求x^{16}，直接计算的话需做15次乘法。

然而如果重复对每个部分结果做平方运算即求x，x^2，x^4，x^8，x^{16}则只需4次乘法。

求a^t可如下进行，其中a，t是正整数：

将t表示为二进制形式$b_k b_{k-1} \ldots b_0$，即

$$t=b_k 2^k+b_{k-1}2^{k-1}+\ldots+b_1 2+b_0$$

因此

$$a^t=\left(\cdots\left(\left(\left(a^{b_k}\right)^2 a^{b_{k-1}}\right)^2 a^{b_{k-2}}\right)^2\cdots a^{b_1}\right)^2 a^{b_0}$$

RSA算法

例：求a^{19}

$19=1\times2^4+0\times2^3+0\times2^2+1\times2^1+1\times2^0$

所以

$$a^{19}=((((a^1)^2a^0)^2a^0)^2a^1)^2a^1$$

练习：求a^7和a^8，并统计快速运算法的运算次数.

RSA算法

- RSA的解密运算

加密很快，指数小；解密比较慢，指数较大．利用中国剩余定理CRT，加快计算速度.

- CRT 对RSA解密算法生成两个解密方程，即：

$$M_1 = M \bmod p = (C \bmod p)^{d \bmod (p-1)} \bmod p$$

$$M_2 = M \bmod q = (C \bmod q)^{d \bmod (q-1)} \bmod q$$

- 解方程组

$$M = M_1 \bmod p ;$$

$$M = M_2 \bmod q .$$

- 利用CRT，具有唯一解：

$$M = [(M_2 + q - M_1)u \bmod q]\, p + M_1.$$

其中 $p.u \bmod q = 1$.

RSA加密算法及其应用

9） RSA的应用--PKCS1 v2.0: OAEP

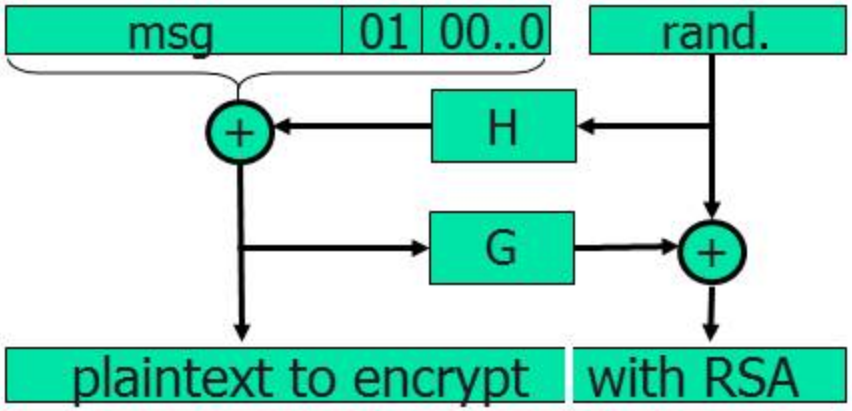
RSA的选择密文攻击:

攻击者是将希望解密的目标密文C作一下伪装r^eC，让拥有私钥的实体解密。然后，脱去伪装就可得到目标密文所对应的目标明文:

$(r^eC)^d = r^{ed} * C^d \bmod n = r * M \bmod n$，所以

$$M = (r^eC)^d * r^{-1} \bmod n \ .$$

RSA加密算法及其应用



- 解密过程检测填充是否正确，若不正确则拒绝解密；
- H和G函数通常使用SHA-256算法.

本节主要内容

- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

ElGamal加密算法

- Diffie-Hellman 密钥交换协议的变形；
- *T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Information Theory, vol IT-31(4), pp469-472, July 1985.*

ElGamal加密算法

1）密钥生成

① 选择一大素数p, 选取Z_p^*的生成元g;

② 任选小于p的随机数x，计算$y \equiv g^x \bmod p$;

③(y, g, p)为公开密钥，(x, g, p)为秘密密钥.

2）加密：设待加密明文为M.

① 随机选一整数k，$0<k<=p-1$;

② 计算密文对：$C=\{C_1,C_2\}$, 发送给接收者.

$$C_1 \equiv g^k \bmod p, \quad C_2 \equiv y^k M \bmod p.$$

ElGamal加密算法

3）解密过程:设收到的密文对为(C_1,C_2).

计算明文:

$$M=\frac{C_2}{C_1^{\,x}}\bmod p$$

4）正确性

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

ElGamal加密算法

5）实例

- 密钥生成.

  Bob选择公开参数p=97 及生成元g=5；

  选择秘密密钥x=58，计算并发布公钥$y=5^{58}= 44 \bmod 97$.

- 加密. Alice 待加密明文为M=3.

  首先得到 Bob的公开密钥 y=44;

  选择随机 k=36 并计算:$K=44^{36}=75 \bmod 97$;

  计算密文对: $C_1 = 5^{36} = 50 \bmod 97$;

  $C_2 = 75*3 \bmod 97 = 31 \bmod 97$.

  发送 {50,31} 给Bob .

- 解密: Bob 解密密文{50,31}.

  首先恢复分母 $K= C_1^{x} = 50^{58}=75 \bmod 97$.

  计算 $K^{-1} = 22 \bmod 97$.

  恢复明文 $M = 31*22 = 3 \bmod 97$.

ElGamal加密算法

有限域上离散对数问题：

已知（Z_p，+，*）是一个有限域，g为Z_p^*的生成元，$y \in Z_p$，求x使得

$$y=g^x \bmod p.$$

如果求有限域离散对数问题是容易的，则获得公钥攻击者能够解出x，ElGamal加密算法完全破译.

本节主要内容

- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

椭圆曲线密码体制简介

椭圆曲线密码体制（elliptic curve cryptography, ECC）被IEEE公钥密码标准P1363采用.

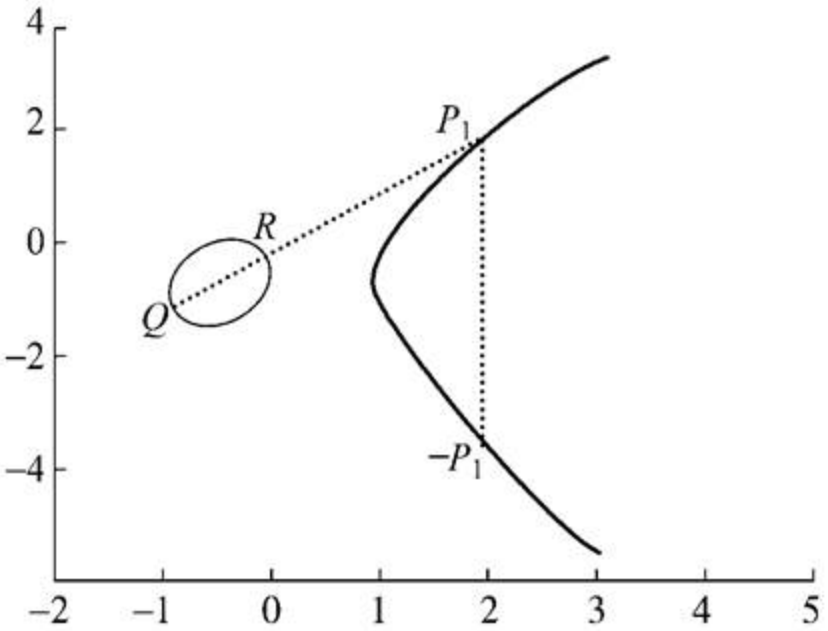
GM/T 0003-2012 《SM2椭圆曲线公钥密码算法》

椭圆曲线是以下形式的三次方程定义的曲线：

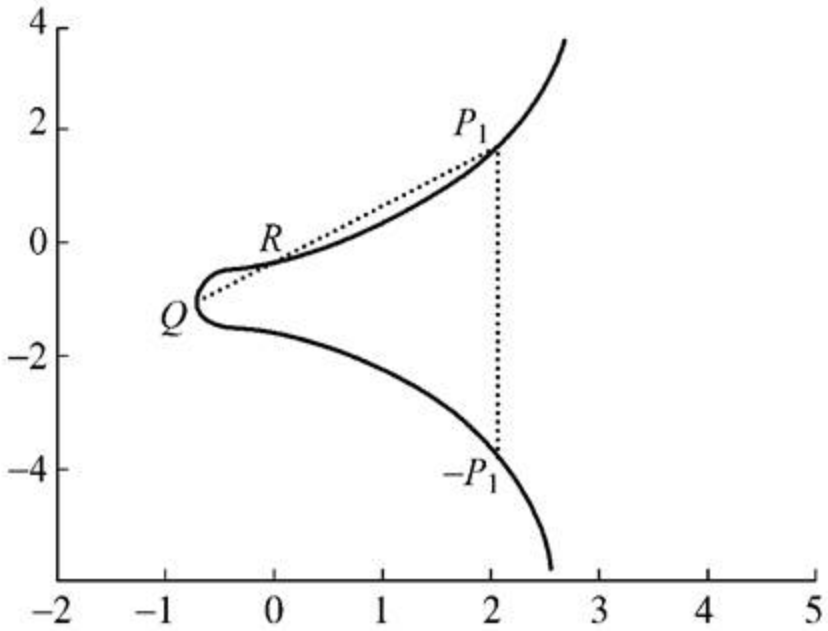
$$y^2+axy+by=x^3+cx^2+dx+e$$

其中a,b,c,d,e是满足某些简单条件的实数. 定义中包括一个称为无穷点的元素，记为O.

椭圆曲线密码体制简介



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



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

椭圆曲线的两个例子

椭圆曲线密码体制简介

椭圆曲线关于x轴对称，定义椭圆曲线上的加法律（加法法则）如下：

①O为加法单位元，即对椭圆曲线上任一点P，有$P+O=P$.

② 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和R的直线与椭圆曲线交于P_1（这一交点是唯一的，除非所做的直线是Q点或R点的切线，由$Q+R+P_1=O$得$Q+R=-P_1$.

椭圆曲线密码体制简介

③ 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.

④设$P_1=(x,y)$是椭圆曲线上的一点（如图所示），它的加法逆元定义为$P_2=-P_1=(x, -y)$.

以上定义的加法具有一般数域加法运算的一般性质，如交换律、结合律等.

椭圆曲线密码体制简介

有限域上的椭圆曲线指曲线方程定义式中，所有系数都是有限域GF(p)中的元素（其中p为大素数）.

最为常用的曲线是

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

$$(a,b \in GF(p),\ 4a^3 + 27b^2 \pmod{p} \neq 0).$$

例： $p=23$， $a=b=1$， $4a^3+27b^2 \pmod{23} \equiv 8 \neq 0$

则方程为$y^2 \equiv x^3 + x + 1$.

椭圆曲线密码体制简介

设$E_p(a,b)$表示上面方程所定义的椭圆曲线上的点集$\{(x,y)|0\le x<p,0\le y<p，\ x,y\in Z\}\cup O$.

例：$E_{23}(1,1)$由下表给出（表中不包含O）.

(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)

椭圆曲线密码体制简介

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：

$$x_3\equiv\lambda^2-x_1-x_2(\mathrm{mod}\ p)$$

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

其中

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

椭圆曲线密码体制简介

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

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \equiv 11 \bmod 23$$

$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \bmod 23$$

$$y_3 = 11(3-17) - 10 = -164 \equiv 20 \bmod 23$$

所以$P+Q=(17,20)$，仍为$E_{23}(1,1)$中的点.

椭圆曲线密码体制简介

若求$2P$则

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

$$x_3 = 6^2 - 3 - 3 = 30 \equiv 7 \bmod 23$$

$$y_3 = 6(3-7) - 10 = -34 \equiv 12 \bmod 23$$

所以$2P=(7,12)$，仍为$E_{23}(1,1)$中的点.

椭圆曲线密码体制简介

椭圆曲线上的离散对数问题：在椭圆曲线构成的Abel群$E_p(a,b)$上考虑方程$Q=kP$, 其中$P,Q\in E_p(a,b)$, $k<p$. 已知P, Q，求k?

1）利用椭圆曲线实现ElGamal密码体制

- 密钥生成
  - 选取一条椭圆曲线$E_p(a,b)$，取$E_p(a,b)$的一个生成元G，$E_p(a,b)$和G作为公开参数.
  - 用户A选x_A作为秘密钥，并以$P_A=x_AG$作为公开钥.

椭圆曲线密码体制简介

- 加密运算

用户Bob若想向Alice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：

$$C_m=\{kG, P_m+kP_A\}=\{c_1,c_2\}$$

- 解密运算

Alice解密时，以密文对中的第二个点减去用自己的秘钥与第一个点的倍乘，即

$$c_2 - xc_1 = P_m+kP_A-x_AkG=P_m+k(x_AG)-x_AkG = P_m$$

椭圆曲线密码体制简介

2）实例：

取p=23，$E_p(1,1)$，即椭圆曲线为$y^2 \equiv x^3+x+1$. $E_p(1,1)$的一个生成元是G=(1,7)，共有28个元素.

$2G$=(7,11), $3G$=(18,20),$4G$=(17,20),$5G$=(0,1),

$6G$=(12,19),$7G$=(11,3),$8G$=(13,7), $9G$=(9,16),

$10G$=(6,19),$11G$=(19,5),$12G$=(5,19),$13G$=(3,10),

$14G$=(4,0),$15G$=(3,13),$16G$=(5,4),$17G$=(19,18),

$18G$=(6,4),$19G$=(9,7),$20G$=(13,16), $21G$=(11,20),

$22G$=(12,4),$23G$=(0,22),$24G$=(17,3),$25G$=(18,3),

$26G$=(7,12),$27G$=(1,16),$28G$=O.

设Alice的秘密密钥为x_A=5，公开密钥为P_A=(0,1).

椭圆曲线密码体制简介

- 假定Bob待加密的明文嵌入到椭圆曲线上的点 P_m=(0,22). 首先获取Alice的公钥，对该点进行加密：

① Bob 选取随机数k=3, 计算kG= 3(1,7)=(18,20).

② kP_A= 3(0,1)=(3,13), P_m+kP_A= (3,13)+ (0,22) = (6,19).

③ 密文为{(18,20), (6,19)}.

- Alice接收到密文{(18,20), (6,19)}, 用自己的私钥解密

① 计算 x_A·(18,20) = 5(18,20) = (3,13),

② 然后用第二个点减去上面点的差：

P_m =(6,19)-(3,13)= (6,19)+[- (3,13)]

= (6,19)+(3, -13)= (6,19)+(3,10)= (0,22).

③ 恢复明文为(0, 22) .

椭圆曲线密码体制简介

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.

保持和RSA体制同样安全强度的前提下可缩短密钥长度

RSA	512	768	1024	2048	2^{1000}
ECC	106	132	160	211	600

本节主要内容

- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

THE END!