第5章 原根和阶

引子

在密码学中, 有很多基于离散对数问题的密码算法和协议, 比如ElGamal公钥密码算法, Diffie-Hellman密钥协商算法, 美国的数字签名算法DSA等等. 学习原根的知识有助于理解离散对数问题.

进一步地，理解离散对数问题也是理解椭圆曲线密码学的基础。

5.1 原根和阶

由欧拉定理, 设$a, m \in Z, m > 1, (a, m) = 1$, 则$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$. 那么$\varphi(m)$是否是使得$a^{?} \equiv 1(\mathrm{mod}\, m)$成立的最小正整数？由经验易得, $2^3 \equiv 1(\mathrm{mod}\, 7)$, 而$\varphi(7) = 6$, 故$\varphi(m)$不是使得$a^{?} \equiv 1(\mathrm{mod}\, m)$成立的最小正整数. 那么这个最小正整数有什么性质呢？如何求这个最小的正整数呢？

原根和阶-定义

【定义5.1.1】 设$a, m \in Z, m > 1, (a, m) = 1$, 则使得

$$a^e \equiv 1(\bmod m)$$

成立的最小正整数e叫做a对模m的**阶**, 记作$\mathrm{ord}_m(a)$.

阶译自英文单词order. 该术语来自近世代数部分的群论. 也有编者把阶称为阶, 注意区别.

若a的阶$e = \varphi(m)$, 则a叫做模m的**原根**（Primitive root modulo m）. 原根又叫**本原元**或**生成元**.

原根和阶-方法?

对于正整数m, 指定整数$a, (a,m)=1$, 若由定义求a对模m的阶, 则先计算$a, a^2, \ldots, a^{\varphi(\mathrm{m})} \pmod m$的值. 由阶的定义, 使得$a^e \equiv 1 \pmod m$成立的最小正整数$e$即为$a$对模$m$的阶. 又由欧拉定理,$(a,m)=1$，$a^{\varphi(\mathrm{m})} \equiv 1 \pmod m$, 故$a$对模$m$的阶一定存在. 但对于求模$m$的原根, 则只有计算模$m$的最小简化剩余系中的所有整数$a$, 由$a$对模$m$的阶$e$来判断$a$是否为模$m$的原根.

原根和阶-例题

【例5.1.1】 若$m = 7$, 则$\varphi(7) = 6$. 与7互素的整数为1, 2, 3, 4, 5, 6. 且计算可得:

$1^1 \equiv 1$;

$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$;

$3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$;

$4^1 \equiv 1$, $4^2 \equiv 2$, $4^3 \equiv 1$;

$5^1 \equiv 5$, $5^2 \equiv 4$, $5^3 \equiv 6$, $5^4 \equiv 2$, $5^5 \equiv 3$, $5^6 \equiv 1$;

$6^1 \equiv 6$, $6^2 \equiv 1 \pmod 7$.

故对模7而言, 1, 2, 3, 4, 5, 6的阶分别为1, 3, 6, 3, 6, 2. 由原根的定义知, 3和5是模7的原根.

原根和阶-例题

【例5.1.2】 取m=14=2×7, 则$\varphi(14)$=6, 与14互素的整数为1, 3, 5, 9, 11, 13. 计算可得:

$1^1\equiv1$, $3^3\equiv-1$, $5^3\equiv-1$, $9^3\equiv1$, $11^3\equiv1$, $13^2\equiv1 \pmod{14}$.

故对模14而言, 1, 3, 5, 9, 11, 13的阶分别为1, 6, 6, 3, 3, 2. 故3, 5是模14的原根.

原根和阶-例题

【例5.1.3】 取m=15=3×5, 则$\varphi(15)$=8, 与15互素的整数为1, 2, 4, 7, 8, 11, 13, 14, 计算可得:

$1^1\equiv1$, $2^4\equiv1$, $4^2\equiv-1$, $7^4\equiv1$, $8^4\equiv1$, $11^2\equiv1$, $13^4\equiv1$, $14^2\equiv1 \pmod{15}$.

故模数15没有原根.

可以看到, 对于正整数m, 模m的原根不一定是存在的.

原根和阶-性质

【定理5.1.1】 设$a, m \in Z, m > 1, (a, m) = 1, d$为正整数, 则$a^d \equiv 1 \pmod m$的充分必要条件是$\mathrm{ord}_m(a) | d$.

证明: 先证充分性.

设$\mathrm{ord}_m(a) | d$, 则存在整数k, 使得$d = k \cdot \mathrm{ord}_m(a)$, 从而

$$a^d \equiv a^{k \times \mathrm{ord}_m(a)} \equiv (a^{\mathrm{ord}_m(a)})^k \equiv 1 \pmod m.$$

原根和阶-性质

再证必要性, 这里采用反证法.

若$a^d \equiv 1 (\bmod m)$且$\mathrm{ord}_m(a)\ d$, 则由带余除法, 有

$$d \equiv \mathrm{ord}_m(a) \cdot q + r,\ 0 < r < \mathrm{ord}_m(a).$$

从而

$$a^r \equiv a^r (a^{\mathrm{ord}_m(a)})^q \equiv a^d \equiv 1 (\bmod m).$$

而$r < \mathrm{ord}_m(a)$, 与$\mathrm{ord}_m(a)$的最小性矛盾.

原根和阶-性质

【推论】 设$a, m \in Z, m > 1, (a, m) = 1$, 则$\mathrm{ord}_m(a) | \varphi(m)$.

由欧拉定理,若 $(a, m) = 1$，则$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, 也即【定理5.1.1】中的$d$可以取值为$\varphi(m)$.

【定理5.1.1】的推论表明, $\mathrm{ord}_m(a)$必是$\varphi(m)$的因子, 故求$\mathrm{ord}_m(a)$只需计算a^d, $d | \varphi(m)$.

这也说明了为什么用Fermat小定理判断素性的Miller-Rabin是一个概率算法. 假定要判断m是否是奇素数, 选择了一个a为底数, 如果$\mathrm{ord}_m(a) | m - 1$, 则必会得到$a^{m-1} (\mathrm{mod}\, m) \equiv 1$.

原根和阶-例题

【例5.1.4】 求$\mathrm{ord}_{17}(5)$的值.

解: $\varphi(17) = 16$, 故由【推论5.1.1】知需计算$5^d \pmod{17}$, 其中d=1, 2, 4, 8, 16.

$5^1 \equiv 5$, $5^2 \equiv 8$, $5^4 \equiv 13 \equiv -4$, $5^8 \equiv 16 \equiv -1 \pmod{17}$.

所以, $\mathrm{ord}_{17}(5)=16$. 由原根的定义知, 5是模17的原根.

原根和阶-例题

【例5.1.5】 求$\mathrm{ord}_{33}(5)$的值.

解: $\varphi(33)=20$, 故由【推论5.1.1】知需计算$5^d \pmod{33}$, 其中d=1, 2, 4, 5, 10. 若计算的结果都不为1, 则$\mathrm{ord}_{33}(5)=\varphi(33)=20$.

$5^2\equiv25 \pmod{33}$, $5^4\equiv25^2\equiv(-8)^2\equiv-2 \pmod{33}$, $5^5\equiv23 \pmod{33}$, $5^{10}\equiv1 \pmod{33}$.

所以$\mathrm{ord}_{33}(5)=10$.

原根和阶-性质

【性质5.1.1】 设$a, b, m \in Z, (a, m) = 1$,

（1）若$b \equiv a \pmod m$, 则$\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

（2）$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

证（1）已知$b \equiv a \pmod m$, 所以

$b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \pmod m$.

所以$\mathrm{ord}_m(b) | \mathrm{ord}_m(a)$.

同理, $a^{\mathrm{ord}_m(b)} \equiv b^{\mathrm{ord}_m(b)} \equiv 1 \pmod m$, 所以 $\mathrm{ord}_m(a) | \mathrm{ord}_m(b)$.

故$\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

（2）由$(a^{-1})^{\mathrm{ord}_m(a)} \equiv (a^{\mathrm{ord}_m(a)})^{-1} \equiv 1 \pmod m$知$\mathrm{ord}_m(a^{-1}) | \mathrm{ord}_m(a)$;

由$aa^{-1} \equiv 1 \pmod m$知$(aa^{-1})^{\mathrm{ord}_m(a^{-1})} \equiv 1 \pmod m$;

即$(a)^{\mathrm{ord}_m(a^{-1})}(a^{-1})^{\mathrm{ord}_m(a^{-1})} \equiv 1 \pmod m$, 从而$(a)^{\mathrm{ord}_m(a^{-1})} \equiv 1 \pmod m$, 由【定理5.1.1】, $\mathrm{ord}_m(a) | \mathrm{ord}_m(a^{-1})$.

故$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

【例5.1.6】 已知整数5模17的阶为$ord_{17}(5)=16$. 因为$7^{-1}\equiv 5 \pmod{17}$, 则由【性质5.1.1】, 整数7模17的阶为16.

【定理5.1.2】 设$m > 1, (a,m) = 1$, 则

$$1 = a^0, a, a^2, \ldots, a^{\mathrm{ord}_m(a)-1}$$

模m两两不同余. 特别地, 若a是模m的原根, 则上述$\varphi(m)$个数构成模m的简化剩余系.

证明: 采用反证法. 若存在整数$k, l(0 \le l < k < \mathrm{ord}_m(a))$使得

$$a^k \equiv a^l (\mathrm{mod}\, m).$$

因$(a,m) = 1$, 故

$$a^{k-l} \equiv 1 (\mathrm{mod}\, m).$$

但$0 < k-l < \mathrm{ord}_m(a)$, 与$\mathrm{ord}_m(a)$的最小性矛盾.

再设a是模m的原根, 即$\mathrm{ord}_m(a) = \varphi(m)$, 则

$$1 = a^0, a, a^2, \ldots, a^{\mathrm{ord}_m(a)-1}$$

模m两两不同余. 故上述$\varphi(m)$个数构成模m的简化剩余系.

原根和阶-例题

【例5.1.7】 整数$\{5^k \pmod{17} \mid k=0,1,2,\ldots,15\}$组成模17的简化剩余系.

解: 由【例5.1.4】，可以看到, 集合$\{5^k \pmod{17} \mid k=0,1,2,\ldots,15\}$是$\{1,2,\ldots,16\}$的一个重新排列.

有了【例5.1.4】中的表格, 求逆元也变得更简单. 例如, 如果求$11^{-1} \pmod{17}$, 常规的方法是有欧几里德算法求解. 实际上, $11^{-1} \equiv (5^{11})^{-1} \equiv 1 \times 5^{-11} \equiv 5^{16} \times 5^{-11} \equiv 5^5 \equiv 14 \pmod{17}$. 由$11 \times 14 = 154 \equiv 1 \pmod{17}$知, 结果正确.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
5^k	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7

原根和阶-举例

【例5.1.8】 设模数$m = 18$, 整数$a = 5$, 验证定理5.1.2的结论.

解: $\varphi(18) = 6$, 计算$\{5^k \pmod{18} \mid k = 0,1,2,\dots,5\}$得下表，即$\{5^k \mid k = 0,1,2,\dots,5\}$模18两两不同余, 且都与18互素, 从而$5^k \pmod{18}$, $k = 0,1,2,\dots,5\}$组成模18的简化剩余系.

k	0	1	2	3	4	5
5^k	1	5	7	17	13	11

原根和阶-性质

【定理5.1.3】 设$a, m \in Z, m > 1, (a, m) = 1$, 则

$a^d \equiv a^k (\bmod m) \quad d \equiv k (\bmod \operatorname{ord}_m(a))$.

证明: 先证必要性, 不妨设$d > k$, 由$a^d \equiv a^k (\bmod m)$ 可得$a^{d-k} \equiv 1 (\bmod m)$,故$\operatorname{ord}_m(a) | d - k$. 故 $d \equiv k (\bmod \operatorname{ord}_m(a))$.

再证充分性, 若$d \equiv k (\bmod \operatorname{ord}_m(a))$, 则$d = k + t\, ord_m\,(a)$, 故

$a^d \equiv a^k (a^{\operatorname{ord}_m(a)})^t \equiv a^k (\text{mod m})$.

原根和阶-举例

【推论】 $a^n \equiv a^{n(\mathrm{mod}\ \mathrm{ord}_m(a))}$(mod m).

【例5.1.9】 因为ord_7 (2)=3, 所以$2^{2002} \equiv 2^{2002(\mathrm{mod}\ 3)} \equiv 2^1 = 2$(mod 7).

原根和阶-性质

【定理5.1.4】 设整数$m > 1, (a, m) = 1, d \geq 0$, 则

$\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), d)}$.

证明: 由阶的定义, 求$\mathrm{ord}_m(a^d)$也即求使得

$(a^d)^x \equiv 1 \pmod{m}$成立的最小正整数$x$.

由【定理5.1.1】,$\mathrm{ord}_m(a) | dx$, 故

$dx \equiv 0 \pmod{\mathrm{ord}_m(a)}$.

该同余方程的全部解为

$x \equiv t\frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), d)} \pmod{\mathrm{ord}_m(a)}$, t=1,...,$(\mathrm{ord}_m(a), d)$. 故最小的正整数解为$\frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), d)}$, 得证.

原根和阶-性质

【例5.1.10】 已知$\mathrm{ord}_{17}(5)=16$, $5^2=8(\mathrm{mod}\ 17)$, 所以

$$\mathrm{ord}_{17}(8)=\mathrm{ord}_{17}(5^2)=\frac{\mathrm{ord}_{17}(5)}{(\mathrm{ord}_{17}(5),2)}=\frac{16}{(16,2)}=8.$$

$$\mathrm{ord}_{17}(6)=\mathrm{ord}_{17}(5^3)=\frac{\mathrm{ord}_{17}(5)}{(\mathrm{ord}_{17}(5),3)}=\frac{16}{(16,3)}=16.$$

【推论】 设$m>1$, g是模m的原根, 整数$d\geq 1$, 则g^d是模m的原根的充要条件是$(d,\varphi(m))=1$.

证明: g是模m的原根, 故$\mathrm{ord}_m\,(g)=\varphi\,(m)$, 由【定理5.1.4】,

$$\mathrm{ord}_m(g^d)=\frac{\mathrm{ord}_m\,(g)}{(\mathrm{ord}_m\,(g),\ d)}=\frac{\varphi\,(m)}{(\varphi\,(m),d)}$$

若要g^d是原根, 则$\frac{\varphi\,(m)}{(\varphi\,(m),d)}=\varphi\,(m)$, 故

$\left(d,\varphi\,(m)\right)=1$.

由推论可知, 在知道模m的一个原根时, 可由这个原根得到所有原根.

模m的原根

【例5.1.11】 由$\text{ord}_{17}(5)=16$可知5是模17的原根，由原根5就可以求出17的所有原根.

解: 模17的所有原根为5^1, 5^3, 5^5 , 5^7, 5^9, 5^{11}, 5^{13}, 5^{15}. 即

$5^1\equiv 5 \pmod{17}$, $5^3\equiv 6 \pmod{17}$, $5^5\equiv 14 \pmod{17}$,

$5^7\equiv 10 \pmod{17}$, $5^9\equiv 12 \pmod{17}$, $5^{11}\equiv 11 \pmod{17}$,

$5^{13}\equiv 13 \pmod{17}$, $5^{15}\equiv 6 \pmod{17}$.

【定理5.1.5】 设$m > 1$, 若m有原根, 则其原根个数为$\varphi(\varphi(m))$.

证明：设m的一个原根为g. 由【定理5.1.4】的推论, 若$(d, \varphi(m)) = 1$, 则g^d是模m的原根. 由欧拉函数的定义, 小于$\varphi(m)$且与$\varphi(m)$互素的正整数的个数为$\varphi(\varphi(m))$, 得证.

【例5.1.12】 求出模25的所有原根.

解: $\varphi(25)=20$, $\varphi(\varphi(25))=\varphi(20)=8$. 故25若有原根, 则其必有8个原根.然后寻找模25的一个原根. 通过计算可得,

$2^5\equiv 7(\mathrm{mod}\ 25)$, $2^{10}\equiv 24\equiv -1(\mathrm{mod}\ 25)$.

所以2是模25的一个原根.

因为模20的简化剩余系为{1, 3, 7, 9, 11, 13, 17, 19}, 故模25的所有原根为: $2^1\equiv 2$, $2^3\equiv 8$, $2^7\equiv 3$, $2^9\equiv 12$, $2^{11}\equiv 23$,

$2^{13}\equiv 17$, $2^{17}\equiv 22$, $2^{19}\equiv 13(\mathrm{mod}\ 17)$.

即模25的原根为: 2, 3, 8, 12, 13, 17, 22, 23.

原根存在的充分必要条件

下面给出原根存在的充分必要条件.

【定理5.1.6】 模m的原根存在的充分必要条件是$m = 2, 4, p^{\alpha}, 2p^{\alpha}$. 其中$p$为奇素数.

5.1.3 素数的原根

由【定理5.1.6】, 素数的原根存在. 下面介绍一种求素数p的原根的方法.

【定理5.1.7】 设$\mathrm{ord}_p\,(g) = d, d < p-1$, 则$g^t$ $(t = 1,2,\ldots,d)$都不是模p的原根.

证明 由【定理5.1.4】, g^t对模p的阶为 $\frac{d}{(d,t)} \le d < p-1$. 所以$g^t$ $(t = 1,2,\ldots,d)$都不是模p的原根.

【定理5.1.8】 设p是素数，$\varphi(p)$的所有不同素因数为$q_1, \ldots, q_k$. 则g是模p的一个原根的充要条件是：$g^{\varphi(p)/q_i} \not\equiv 1(\bmod m), (i = 1,2, \ldots, k)$.

证明 必要性 g是模p的一个原根, 则g模p的阶是$\varphi(p)$. 因

$$0 < \frac{\varphi(p)}{q_i} < \varphi(p)$$

故$g^{\varphi(p)/q_i} \not\equiv 1(\bmod m)$.

充分性 若g是模p的阶$e < \varphi(p)$, 则有$e|\varphi(p)$, 即存在整数q, 使得$eq = \varphi(p)$. 即

$$g^{\varphi(p)/q} \equiv g^e \equiv 1(\bmod m)$$

与题设矛盾.

根据【定理5.1.7】和【定理5.1.8】, 给出一种求素数p的原根的思路. 要求模p的原根, 由【定理5.1.8】, 先判断$g = 2$是否为模p的原根. 若2不为模p的原根, 由【定理5.1.7】, 设2模p的阶d, 则2^t $(t = 1,2, \dots, d)$都不是模p的原根. 然后在1, 2, …, $p - 1$中删除2^t $(t = 1,2, \dots, d)$, 在剩下的数中选择最小的整数, 重复上述方法进行求解.

【例5.1.12】 求$p=17$的原根.

解 先求$g=2$模17的阶. 由于$\varphi(17)=16$. $16=2^4$的素因数只有$q=2$,

$$\frac{\varphi(p)}{q}=8$$

故只需计算g^8模$p=17$是否同余1.

因$2^8 \pmod{17} \equiv 1$. 所以2模17的阶为8. 即2不是模17的原根.

由【定理5.1.7】, $2^1 \pmod{17} \equiv 2$, $2^2 \pmod{17} \equiv 4$, $2^3 \pmod{17} \equiv 8$, $2^4 \pmod{17} \equiv 16$, $2^5 \pmod{17} \equiv 15$, $2^6 \pmod{17} \equiv 13$, $2^7 \pmod{17} \equiv 9$, $2^8 \pmod{17} \equiv 1$. 都不是模17的原根.

故在1, 2, ..., 16个数中还剩下3, 5, 6, 7, 10, 11, 12, 14. 接下来先求$g = 3$模17的阶. 计算得$3^1 \pmod{17} \equiv 3$, $3^2 \pmod{17} \equiv 9$, $3^4 \pmod{17} \equiv 13$, $3^8 \pmod{17} \equiv 16$, $3^{16} \pmod{17} \equiv 1$. 所以3模17的阶为16. 即3是模17的原根.

从求解过程可以看到，这种方法适合于较小的素数. 假如素数p很大, 该方法并不合适.

5.2 离散对数

设g是模为正整数m的一个原根, 则由【定理5.1.2】知$\varphi(m)$个数$g, g^2, \dots, g^{\varphi(\mathrm{m})}$是$m$的一个简化剩余系. 因此, 若$a$是一个与$m$互素的整数, 则存在唯一的一个整数$r$且$1 \leq r \leq \varphi(m)$, 使得$g^r \equiv a (mod\ m)$. 由此引出下面的定义.

离散对数-定义

【定义5.2.1】 设m是正整数, g是模m的一个原根. 对给定的整数a, 存在整数r, 使得式

$$g^r \equiv a(mod\ m) \quad （1）$$

成立, 则称r为以g为底的a对模m的一个**指标**, 记作$r = \text{ind}_g a$或ind$a$. 指标也称为**对数**或**离散对数**.

指标翻译自英文单词index. 也有书译为指数, 注意区别.

离散对数-例题

【例5.2.1】 已知5是模17的原根. 求10对模17的离散对数.

解: 先构造以5为底的阶函数表.再构造离散对数表. 可得, 10对模17的离散对数为7.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$a \equiv 5^r$	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$r=\log_g a$	16	6	13	12	1	3	15	2	10	7	11	9	4	5	14	8

离散对数-性质

【定理5.2.1】设$m > 1$, g是模m的一个原根, $(a, m)=1$, 若整数r使得$g^r \equiv a \pmod m$成立, 则r满足

$$r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

证明: 因为$(a, m)=1$, 故$g^r \equiv a \equiv g^{\mathrm{ind}_g a} \pmod{\mathrm{m}}$.

从而 $g^{r-\mathrm{ind}_g a} \equiv 1 \pmod{\mathrm{m}}$.

又知g模m的阶为$\varphi(m)$, 由【定理5.1.1】知$\varphi(m) \mid r-\mathrm{ind}_g a$.

故 $r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$.

离散对数-举例

【例5.2.2】 已知5是17的一个原根，且$r=38$，那么，由欧拉定理，计算可得

$5^{38}\equiv 5^{6}\equiv 2 \pmod{17}$.

查例5.2.1中的表可知，$\mathrm{ind}_5 2=6$，故

$38 \pmod{\varphi(17)} \equiv 38 \pmod{16} \equiv 6 = \mathrm{ind}_5 2$.

离散对数-举例

设g是模m的一个原根. 若已知$y \equiv g^x \pmod{m}$, 求x是困难的. 这被称为离散对数问题(Discrete logarithm Problem, DLP). 求离散对数是困难问题, 到目前为止，最好的求解离散对数算法的时间复杂度是亚指数级的.

5.3离散对数在密码学中的应用

离散对数问题在密码学中的应用, 主要包括了ElGamal密码算法、Diffie-Hellman密钥协商算法、数字签名标准(DSS)等. 这里我们介绍ElGamal密码算法, 以及DSS参数选取时用到的本章的相关知识.

5.3.1 ELGamal密码算法

ELGamal密码算法是一个非对称加密算法, 由ELGamal在1985提出. 既可以用于加密, 也可以用于签名, 其安全性依赖于离散对数问题. ELGamal数字签名算法的一个变体就是数字签名标准（DSS）. 下面给出ELGamal算法的描述.

（1）构造全局变量

选择一素数p, 模p的一个原根g, 随机选取x, g和x都小于p, 然后计算$y \equiv g^x \pmod p$.

公开密钥是$\{y, g, p\}$, 其中g, p可以为一组用户共享. 私有密钥是$\{x, g, p\}$.

（2）加密算法

将明文信息M表示成$\{0,1,\ldots,p-1\}$范围内的数, 然后秘密选择随机数k，计算:

$C_1 \equiv g^k \pmod p$, $C_2 \equiv My^k \pmod p$.

密文为(C_1, C_2).

（3）解密算法

计算$\mathrm{M} \equiv C_1^{-x}\, C_2 \pmod p$.

由公钥密码算法的要求可知, 密码分析者在知道用户公钥的情况下, 计算出对应的私钥在计算上是困难的. 也就是说, 通过选择合适的参数, 密码分析者知道$\{y, g, p\}$, 也知道$y \equiv g^x \pmod p$, 要得到x在计算上是困难的. 密码分析者知道$\{C_1, g, p\}$, 也知道$C_1 \equiv g^k \pmod p$, 要得到k在计算上也是困难的. 这样，密码分析者在知道密文(C_1, C_2)时，不能解密得到消息M.

【例5.3.1】 用户A选取$p = 41$, 因6是模41的一个生成元, 取$g = 6$, 又取私钥$x = 4$, 计算$y \equiv g^x \pmod p \equiv 25$. 公布$(p, g, y) = (41, 6, 25)$, 保密$x = 4$.

若用户B欲向A发送秘密信息$m = 13$,他先取得A的公钥$(p, g, y) = (41, 6, 25)$, 然后选取随机整数$k = 19$, 计算

$C_1 \equiv g^k \pmod p = 6^{19} \pmod{41} \equiv 34.$

$C_2 \equiv My^k \pmod p =\equiv 13 \times 25^{19} \pmod{41} \equiv 13 \times 23 \equiv 12.$

B发送$(C_1, C_2) = (34,12)$给A.

A在接收到B发送给自己的信息$(C_1, C_2) = (34,12)$后, 计算

$C_1^{-x}\, C_2 (\bmod p) = 34^{-4} \times 12 (\bmod 41) \equiv 25 \times 12\ (\bmod 41) \equiv 13.$

从这里可以看到, 当p取值很大的时候, 加密和解密的主要运算还是模幂运算.

5.3.2 数字签名标准的参数选取

1991年8月, NIST颁发了一个通告, 提出将数字签名算法DSA用于数字签名标准DSS中. 1994年, 在考虑了公众的建议后, 该标准最终颁布.

数字签名算法(DSA)的安全性是基于求解离散对数困难性的基础之上的, 它是Schnorr和ElGamal签名算法的变体.

算法的参数选取过程描述如下:

（1）p是L比特长的素数，L的长度为512到1024且是64的倍数.

（2）q是160比特长且为$p-1$的素因子. $g \equiv h^{\frac{p-1}{q}} \pmod p$, 其中$h, g$是整数, $1 < h < p-1$, 且要求g大于1.

（3）x是签名者的私钥, 由签名者选取的随机数, 要求是小于q的正整数;

$y \equiv g^x \pmod p$为签名者的公钥.

签名者公开(p, q, g, y), 保密x.

在参数选取的第（2）步, 算法没有直接选取模p的原根, 因为求任意指定素数p的原根不容易. 由$g \equiv h^{\frac{p-1}{q}} \pmod p$可知, $g^q \equiv h^{p-1} \equiv 1 \pmod p$. 因$q$是素因子, 故$g$对模$p$的阶等于$q$.

理论上讲, 由于g对模p的阶为q而不是$\varphi(p) = p - 1$, $g^1, g^2, \ldots, g^q$这个集合远小于模p的简化剩余系. 但由于q是一个长度为160比特的素数, 这个集合仍然足够大, 可以保证密码分析者由$y \equiv g^x \pmod p$求出x是困难的.

作业