原根与指数

网络空间安全学院 胡丽琴

原根与指数

主要内容

一 指数

二 原根

三 Diffie-Hellman密钥协商

1 指数

指数

- Euler定理：设m是大于1的整数，a是满足$(a,m)=1$的整数，则

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m).$$

- 那么，$\varphi(m)$是使得$a^k\equiv 1(\mathrm{mod}\ m)$的最小正整数吗？

指数

- 例如：$a=2$，$m=7$，$\varphi(m)=6$，即$2^6\equiv1(\mathrm{mod}\ 7)$.

- 事实上，我们在计算2^{52}天后是星期几时，有计算出$2^3\equiv1(\mathrm{mod}\ 7)$.

- 如何寻找最小正整数k使得$a^k\equiv1(\mathrm{mod}\ m)$，以及这样的最小正整数有哪些性质呢？

● 原根与指数

定义5.1.1 设$m>1$是整数，a是与m互素的正整数，则使得

$$a^e \equiv 1 (\mathrm{mod}\ m)$$

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

如果a模m的指数是$\varphi(m)$，则a叫做模m的**原根**。

指数

- 例如：对于任意的m，$\mathrm{ord}_m(1)=1$.

- 例 $\mathrm{ord}_2(-1)=1$，当$m>2$时，$\mathrm{ord}_m(-1)=2$.

- 例 $\mathrm{ord}_7 2=3$，$\mathrm{ord}_{11}(2)=?$ $\mathrm{ord}_{17}(3)=?$
- $\mathrm{ord}_{11}(2)=10$，$\mathrm{ord}_{17}(3)=16$

指数

- **例：** 模7的指数表

$1^1 \equiv 1 \pmod 7$　$2^3 \equiv 1 \pmod 7$　$3^6 \equiv 1 \pmod 7$

$4^3 \equiv 1 \pmod 7$　$5^6 \equiv 1 \pmod 7$　$6^2 \equiv 1 \pmod 7$

a	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

- 与7互素的整数a模7的指数有什么性质？

指数

- **例：** 模10的指数表

$1^1 \equiv 1 \pmod{10}$　$3^4 \equiv 1 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$　$9^2 \equiv 1 \pmod{10}$

a	1	3	7	9
$\mathrm{ord}_{10}(a)$	1	4	4	2

● 指数练习

例

- **例** 给出整数$m=9$和$m=8$的模m指数表，并判断是否存在原根。

a	1	2	4	5	7	8
$\mathrm{ord}_9(a)$	1	6	3	6	3	2

a	1	3	5	7
$\mathrm{ord}_8(a)$	1	2	2	2

● 指数性质

- **定理5.1.1** 设$m>1$是整数，a是与m互素的整数，则整数d使得

$$a^d \equiv 1 \pmod{m}$$

成立的充要条件$\mathrm{ord}_m(a) | d$。

- 分析：设$d = \mathrm{ord}_m(a) \times q + r$, $0 \le r < \mathrm{ord}_m(a)$, q, $r \in \mathbf{Z}$，则：

$$a^d \equiv a^{\mathrm{ord}m(a)\times q+r} \equiv a^r \equiv 1 \pmod{m},$$

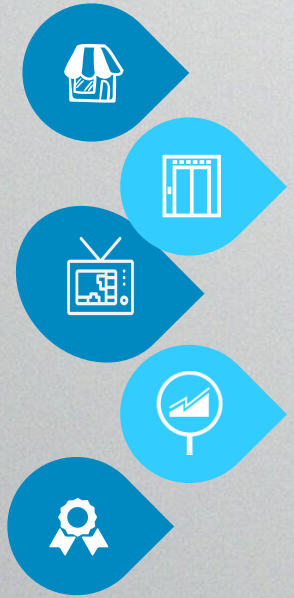
由指数定义，$\mathrm{ord}_m(a)$最小，所以$r=0$。

指数性质

- **推论1** 设$m>1$是整数，a是与m互素的整数，则$\mathrm{ord}_m(a)|\varphi(m)$。

- **证明：** 5是模3与模6的原根，也是模3^2，2×3^2的原根。

● 指数性质



- $\varphi(3)=2$， $\varphi(6)=\varphi(3)\varphi(2)=2$

  $\varphi(3^2)=9-3=6$，$\varphi(2\times3^2)=\varphi(2)\varphi(3^2)=6$

  - $5\equiv 2(\mathrm{mod}\ 3)$ $5^2\equiv1(\mathrm{mod}\ 3)$，所以5是模3的原根；
  - $5\equiv -1(\mathrm{mod}\ 6)$ $5^2\equiv1(\mathrm{mod}\ 6)$，所以5是模6的原根；
  - $5\equiv 5(\mathrm{mod}\ 9)$ $5^2\equiv -2(\mathrm{mod}\ 9)$ $5^3\equiv -1(\mathrm{mod}\ 9)$ $5^4\equiv 4(\mathrm{mod}\ 9)$

    $5^5\equiv 2(\mathrm{mod}\ 9)$ $5^6\equiv 1(\mathrm{mod}\ 9)$，所以5是模9的原根；
  - $5\equiv 5(\mathrm{mod}\ 18)$ $5^2\equiv 7(\mathrm{mod}\ 18)$ $5^3\equiv -1(\mathrm{mod}\ 18)$ $5^4\equiv -5(\mathrm{mod}\ 18)$ $5^5\equiv -7(\mathrm{mod}\ 18)$ $5^6\equiv 1(\mathrm{mod}\ 18)$，所以5是模18的原根。

● 指数性质

例题

- **例** 计算整数5模17的指数$ord_{17}(5)$.
- 解：$\varphi(17)=16$，16的因数只有1、2、4、8、16，所以只需要

$5\equiv 5(\mathrm{mod}\ 17)$ $5^2\equiv 8(\mathrm{mod}\ 17)$

$5^4\equiv 13(\mathrm{mod}\ 17)$ $5^8\equiv 16\equiv -1(\mathrm{mod}\ 17)$,

$5^{16}\equiv 1(\mathrm{mod}\ 17)$,

因此，$ord_{17}(5)=16=\varphi(17)$，所以5是模17的原根。

指数

练习 计算整数3模19的指数$\mathrm{ord}_{19}(3)$

● 指数性质

- **推论2** 设p是奇素数，且$(p-1)/2$也是素数。如果$a>1$是一个不被p整除的整数，且不是模p的二次单位根，则

$$\mathrm{ord}_p(a)=p-1 \text{或} (p-1)/2.$$

- **例** 计算整数39和7模17的指数。

- $\mathrm{ord}_{17}(39)=16$，$\mathrm{ord}_{17}(7)=16$
- $39\equiv 5 \pmod{17}$，$7\times 5\equiv 1 \pmod{17}$

指数

- **性质5.1.1** 设$m>1$是整数，a是与m互素的整数。
  - 若$b\equiv a(\mathrm{mod}\ m)$，则$\mathrm{ord}_m(b)=\mathrm{ord}_m(a)$；
  - 设a^{-1}使得$a^{-1}a\equiv 1(\mathrm{mod}\ m)$，则$\mathrm{ord}_m(a^{-1})=\mathrm{ord}_m(a)$。
- **例：** 5模17的指数$\mathrm{ord}_{17}(5)=16$，即：5是模17的原根，求所有5的幂次(模17)。
- 什么规律？

指数性质

定理5.1.2 设$m>1$是整数，a是与m互素的整数，则

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

模m两两不同。特别地，当a是模m的原根，即$\mathrm{ord}_m(a)=\varphi(m)$时，这个$\varphi(m)$数组成模$m$的简化剩余系。

指数性质

- **例** 计算$2^{2002}(\mathrm{mod}\ 7)$.
  - $2^3\equiv 1(\mathrm{mod}\ 7)$，$2002\equiv 1(\mathrm{mod}\ 3)$，所以$2^{2002}\equiv 2^1\equiv 2(\mathrm{mod}\ 7)$。
- **定理5.1.3** 设$m>1$是整数，a是与m互素的整数，则

$$a^d\equiv a^k(\mathrm{mod}\ m)$$

的充分必要条件是

$$d\equiv k(\mathrm{mod}\ \mathrm{ord}_m(a)).$$

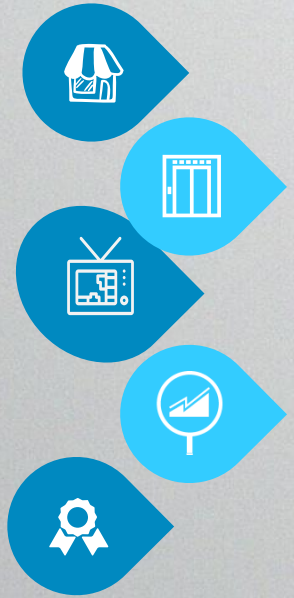
● 指数性质

- **例** 5模17的指数$\mathrm{ord}_{17}(5)=16$，那么$\mathrm{ord}_{17}(5^2)=?$ $\mathrm{ord}_{17}(5^3)=?$
- **定理5.1.4** 设$m>1$是整数，a是与m互素的整数，$d\geq 0$为整数，则

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

- **推论** 设$m>1$是整数，g是模m的原根，$d\geq 0$为整数，则g^d是模m的原根当且仅当$(d,\varphi(m))=1$.

● 指数性质



- **定理5.1.5** 设$m>1$是整数，g是模m的原根，$d\geq 0$为整数，则模m有$\varphi(\varphi(m))$个原根。
- 哪$\varphi(\varphi(m))$个原根？
- **例** 求出模17的所有原根。

● 指数性质

例题

- **例** 计算整数5模17的指数$\mathrm{ord}_{17}(5)$.

解： $\varphi(17)=16$，$\varphi(\varphi(17))=\varphi(16)=8$。所以，模17共有8个原根。

已知5是模17的一个原根。

模16的简约剩余系为：1,3,5,7,9,11,13,15，所以模17的所有原根为：5^1, $5^3\equiv 6 \pmod{17}$, $5^5\equiv 14 \pmod{17}$, $5^7\equiv 10 \pmod{17}$, $5^9\equiv 12 \pmod{17}$, $5^{11}\equiv 11 \pmod{17}$, $5^{13}\equiv 3 \pmod{17}$, $5^{15}\equiv 7 \pmod{17}$.

指数性质

- **例** 考虑模7的指数：2模7的指数

  $\mathrm{ord}_7(2)=3$，$\mathrm{ord}_7(6)=2$，

  $\mathrm{ord}_7(2\times6)=\mathrm{ord}_7(5)=?$

- **定理5.1.6** 设$m>1$是整数，a, b都是与m互素的整数，则$(\mathrm{ord}_m(a), \mathrm{ord}_m(b))=1$当且仅当$\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\mathrm{ord}_m(b)$。

● 指数性质

- **例** 求模23的原根。
- **解**：计算整数2模23的指数：$ord_{23}(2)=11$，2不是模23的原根，但是$23/ord_{23}(2)=2$，$(2,11)=1$，$ord_{23}(-1)=2$。所以，-2是模23的原根。

● 指数性质

- **定理5.1.7** 设m, n都是大于1的整数，a是与m, n互素的整数，则
  - 若$n|m$，则$\mathrm{ord}_n(a)|\mathrm{ord}_m(a)$;
  - 若$(m,n)=1$，则$\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$.
- **推论** 设p, q是两个不同的奇素数，a是与pq互素的整数。则

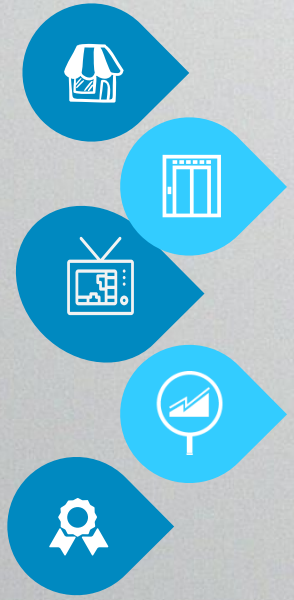
$$\mathrm{ord}_{pq}(a)=[\mathrm{ord}_p(a),\mathrm{ord}_q(a)]$$

指数性质

- **例** 计算3模28的指数$ord_{28}(3)$。
- **解：** $\varphi(28)=\varphi(4)\,\varphi(7)=2\times6=12$

  本来需要计算$3^2 \pmod{28}$、$3^3 \pmod{28}$、$3^4 \pmod{28}$、$3^6 \pmod{28}$，但是因为$ord_7(3)=6$，$ord_4(3)=2$，$(4, 7)=1$，所以$ord_{28}(3)=[6,2]=6$。

● 指数性质



- **例** 计算3模49的指数$\mathrm{ord}_{49}(3)$。

- 解：$\varphi(49)= 49-7=42$，42的因数为1,2,3,6,7,12,14,42，因为$\mathrm{ord}_{7}(3)=6$，所以$6|\mathrm{ord}_{49}(3)$，因为$3^{6}\equiv 81\times 9\equiv -17\times 9\equiv -3\times 2\equiv -6(\mathrm{mod}\ 49)$，所以$\mathrm{ord}_{49}(3)= 42$.

● 指数性质

定理

- **定理5.1.8** 设m, n都是大于1的整数，且$(m,n)=1$，则对与mn互素的任意整数a_1, a_2，存在整数a使得

$$\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)].$$

- **定理5.1.9** 设$m>1$是整数，则对与m互素的任意整数a, b，存在整数c使得

$$\mathrm{ord}_m(c)=[\mathrm{ord}_m(a),\mathrm{ord}\ \mathrm{ord}_m(b)].$$

指数性质

定理5.1.10 设$m>1$是整数，$a_1, a_2, \ldots, a_{\varphi(m)}$是模$m$的简化剩余系，$e$是使得

$$a_k^e \equiv 1 (\mathrm{mod}\ m),\ 1 \le k \le \varphi(m)$$

成立的最小正整数，则存在整数a使得

$$e=\mathrm{ord}_m(a)=[\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \ldots, \mathrm{ord}_m(a_{\varphi(m)})].$$

● 指数性质

- **定义5.1.2** 定理5.1.10中的最小正整数e叫做模m的**简化剩余系指数**，记作

$$e=\mathrm{ord}((\mathbf{Z}/m\mathbf{Z})^*).$$

当$m=p$是素数时，我们有

$$e=\mathrm{ord}((\mathbf{Z}/p\mathbf{Z})^*)=\mathrm{ord}((\mathbf{F}_p)^*)=\varphi(p).$$

- **定理5.1.10** 设$m>1$是整数，则模m存在原根的充要条件是

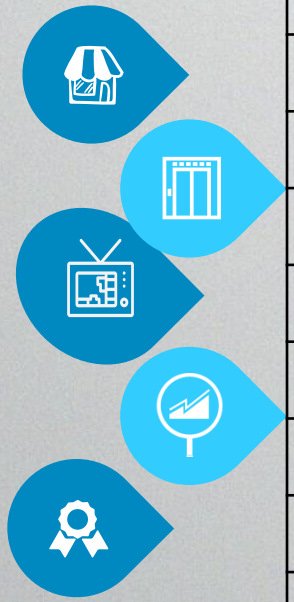
$$\mathrm{ord}((\mathbf{Z}/m\mathbf{Z})^*)=\varphi(m).$$

● 指数性质

定义

- **例** 设整数$m=80$，求整数$e=\mathrm{ord}((\mathbf{Z}/m\mathbf{Z})^*)$.
- **解**：$m=80=2^4\times5$，设$m_1=2^4$，$m_2=5$，则$(m_1,m_2)=1$，对任意与m互素的整数a，有$\mathrm{ord}_m(a)=\mathrm{ord}_{m_1m_2}(a)=[\mathrm{ord}_{m_1}(a),\mathrm{ord}_{m_2}(a)]$。
  - 模5存在原根2和3。所以$\mathrm{ord}_5(a)=4$。而$\mathrm{ord}((\mathbf{Z}/2^4\mathbf{Z})^*)=4$，$\mathrm{ord}_5(b)=4$。
  - 因此，存在c使得$\mathrm{ord}_m(c)=[\mathrm{ord}_{m_1}(a),\mathrm{ord}_{m_2}(b)]=4$.

指数性质



a	$\mathrm{ord}_{41}(a)$	a	$\mathrm{ord}_{41}(a)$	a	$\mathrm{ord}_{41}(a)$	a	$\mathrm{ord}_{41}(a)$
1	1	11	40	21	20	31	10
2	20	12	40	22	40	32	4
3	8	13	40	23	10	33	20
4	10	14	8	24	40	34	40
5	20	15	40	25	10	35	40
6	40	16	5	26	40	36	20
7	40	17	40	27	8	37	5
8	20	18	5	28	40	28	8
9	4	19	40	29	40	39	20
10	5	20	20	30	40	40	2

● 指数性质

定理

- 记$\mathbf{F}_d=\{a|(a,m)=1, \mathrm{ord}_m(a)=d\ , 1\le a\le m-1\}$，我们有

$\mathbf{F}_1=\{1\}$，$\mathbf{F}_2=\{40\}$，$\mathbf{F}_4=\{9,32\}$，$\mathbf{F}_8=\{3,14,27,38\}$，

$\mathbf{F}_5=\{10,16,18,37\}$，$\mathbf{F}_{10}=\{4,23,25,31\}$，

$\mathbf{F}_{20}=\{2,5,8,20,21,33,36,39\}$，

$\mathbf{F}_{40}=\{6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35\}$

它们的并集构成模m的简化剩余系，且

$|\mathbf{F}_1|=1=\varphi(1)$，$|\mathbf{F}_2|=1=\varphi(2)$，$|\mathbf{F}_4|=2=\varphi(4)$，$|\mathbf{F}_8|=4=\varphi(8)$，

$|\mathbf{F}_5|=4=\varphi(5)$，$|\mathbf{F}_{10}|=4=\varphi(10)$，$|\mathbf{F}_{20}|=8=\varphi(20)$，$|\mathbf{F}_{40}|=16=\varphi(40)$.

2 原根

原根存在条件

- 模7指数表

a	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

- 模9指数表

a	1	2	4	5	7	8
$\mathrm{ord}_9(a)$	1	6	3	6	3	2

- 模8指数表

a	1	3	5	7
$\mathrm{ord}_8(a)$	1	2	2	2

● 原根存在条件

- 问：对于什么样的正整数m，模m的原根是存在？
- **定理5.2.1** 若p是奇素数，则模p的原根存在。
- **定理5.2.2** 若p是奇素数，g是模p的一个原根，则g或$g+p$是模p^2的原根。

● 原根存在条件

- **定理5.2.3** 设p是奇素数，则对任意的正整数α，模p^{α}的原根存在。更确切地说，如果g是模p^2的原根，则g是模p^{α}的原根。
- **定理5.2.4** 设p是奇素数，$\alpha \geq 1$是正整数，g是模p^{α}的一个原根，则g与$g+p^{\alpha}$中的奇数是模$2p^{\alpha}$的原根。

原根存在条件

- **定理5.2.3** 设p是奇素数，则对任意的正整数α，模p^{α}的原根存在。更确切地说，如果g是模p^2的原根，则g是模p^{α}的原根。

- **定理5.2.4** 设p是奇素数，$\alpha \geq 1$是正整数，g是模p^{α}的一个原根，则g与$g+p^{\alpha}$中的奇数是模$2p^{\alpha}$的原根。

● 原根性质

性质

- **定理5.2.5** 设a是一个奇数，则对任意整数$\alpha\geq 3$，有

$$a^{\varphi(2^\alpha)/2}=a^{2^{\alpha-2}}\equiv 1(\mathrm{mod}\ 2^\alpha).$$

- **定理5.2.6** 设$\alpha\geq 3$是一个整数，则

$$\mathrm{ord}_{2^\alpha}(5)=2^{\alpha-2}=\varphi(2^\alpha)/2.$$

● 指数性质

- **定理5.2.7** 模m的原根存在的充要条件是m=2, 4, p^{α}, $2p^{\alpha}$。

- **定理5.2.8** 设$m>1$，$\varphi(m)$的所有不同素因数是$q_1, \ldots, q_k$，则g是模m的一个原根的充要条件是

$$g^{\varphi(m)/q_i} \neq 1 (\mathrm{mod}\ m),\ i=1, \ldots, k.$$

● 原根计算

定理

- **例** 求模41的所有原根。
- **解：** 首先，找出模41的一个原根g，然后写出模$\varphi(41)$的简化剩余系：

1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39

共$\varphi(\varphi(41))=16$个数。最后得到模41的所有原根$g^i \pmod{41}$，i跑遍模$\varphi(41)$的简化剩余系元素。

● 原根计算

- 寻找模41的原根g。

因为$\varphi(m)=\varphi(41)=40=2^3\times5$，所以$\varphi(m)$的素因数为$q_1=2$，$q_2=5$。进而，$\varphi(m)/q_1=20$，$\varphi(m)/q_2=8$.

这样，只需验证g^{20}，g^8是否模m同余于1。

对2,3,…逐个验证得到：

$$2^8\equiv10,\ 2^{20}\equiv1,\ 3^8\equiv1,\ 4^8\equiv18,\ 4^{20}\equiv1,$$

$$5^8\equiv18,\ 5^{20}\equiv1,\ 6^8\equiv10,\ 6^{20}\equiv40(\mathrm{mod}\ 41),$$

所以6是模41的原根。

原根计算

- 当d遍历模$\varphi(41)$的简化剩余系时，6^d遍历模41的所有原根。

$6^1\equiv10,\ 6^3\equiv11,\ 6^7\equiv29,\ 6^9\equiv19,\ 6^{11}\equiv28,$

$6^{13}\equiv24,\ 6^{17}\equiv26,\ 6^{19}\equiv34,6^{21}\equiv35,\ 6^{23}\equiv30,$

$6^{27}\equiv12,\ 6^{29}\equiv22,6^{31}\equiv13,\ 6^{33}\equiv17,\ 6^{37}\equiv15,$

$6^{39}\equiv7 \pmod{41}.$

● 原根计算

- **例** 求模$m=41^2=1681$的原根。
- **解：** 已知6是模41的一个原根，所以，6或$6+41=47$是模$41^2=1681$的一个原根。

事实上，我们有

$$6^{40}\equiv 124\equiv 1+41\times 3\neq 1 \pmod{41^2},$$

$$47^{40}\equiv 1518\equiv 1+41\times 37\neq 1 \pmod{41^2}$$

因此，6和47都是模$m=41^2=1681$的原根。它们也都是模p^{α}的原根。

原根计算

- **例** 求模$m=2\times41^2=3362$的原根。
- **解：** 6和47都是模$41^2=1681$的原根。所以$6+41^2=1687$和47是模$m=2\times41^2=3362$的原根。

3

Diffie-Hellman密钥协商

离散对数问题

- 离散对数问题
  - 已知有限循环群$G=\langle g\rangle=\{g^k, k=\ldots, -2, -1, 0, 1, 2, \ldots\}$及其生成元$g$，和群的阶$n=|G|$，则有如下数学难题：
- 给定整数a计算元素$h=g^a$很容易；
- 给定元素h，计算整数x, $0\leq x\leq n-1$, 使得$g^x=h$非常困难。

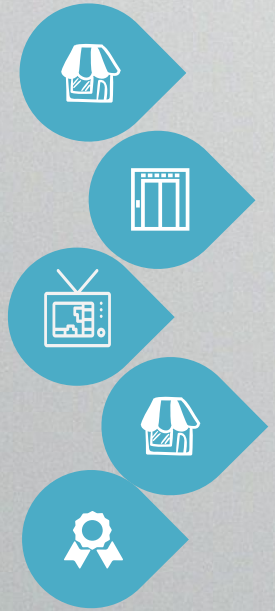
● 离散对数问题

例

- **例：**设p=20000000000000002559($\approx 2^{65}$)，g=11是$\mathbf{F}_p$*的生成元。
- 对于整数a=20050714，可快速计算$h=g^a$；
- 求整数x，使得$g^x \equiv 14158167154104328392 \pmod{p}$。

● EIGamal公钥密码体制

- EIGamal公钥密码体制的安全性基于离散对数问题的安全性，它可用于加密，也可用于签名及建立共同的密钥。



- EIGamal公钥密码体制的具体描述如下：

➢ 使用者产生公钥和私钥

✓ 随机产生一个大素数p和模p的一个原根g；

✓ 随机选取整数a，$1<a<p-1$，作为私钥，计算$g^a \pmod p$作为公钥

✓ 使用者A的公钥是(p, g, g^a)，私钥是a。

ElGamal公钥密码体制

- ElGamal公钥加密/解密
  - B将加密的信息发送给A，A解密
- 加密过程。B做如下事情：
  - 得到确认的A的公钥(p, g, g^a)；
  - 将信息表示为整数m，$0<m<p$；
  - 秘密的随机选取整数k, $1<k<p-1$；
  - 计算$u \equiv g^k \pmod p$和$v \equiv m(g^a)^k \pmod p$
  - 将密文$c=(u,v)$发送给A。

● ElGamal公钥密码体制

- 解密过程。为了将密文恢复成明文，A做如下事情：
  - 运用私钥a，计算$u^{p-1-a} \pmod p$
  - A计算$u^{p-1-a} \times v$，并由它恢复原明文消息。
- 分析：$u^{p-1-a} \times v \equiv g^{(p-1)k-ak} \times m \times g^{ak} \equiv m \pmod p$，所以A可以正确解密，得到B需要发送的明文。

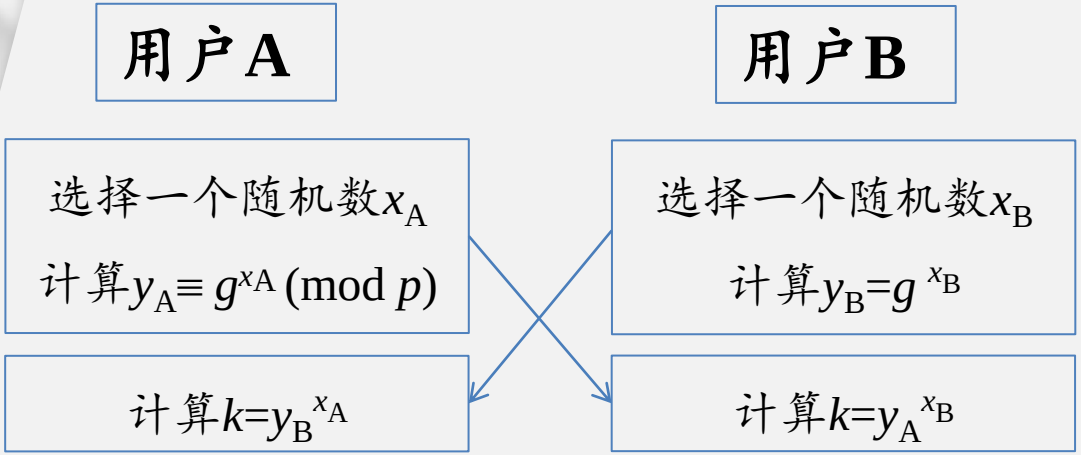
Diffie-Hellman密钥协商

- 实体A和实体B希望达成一个随机产生的共同密钥。
- 公开知道的消息是群G以及具有已知大阶的元$a \in G$

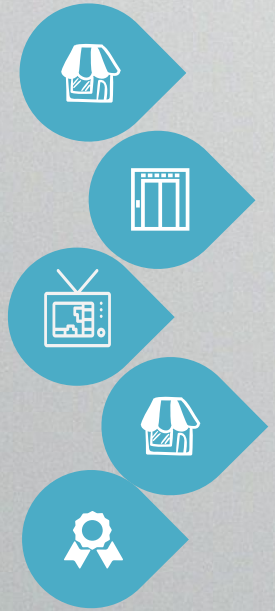
Diffie-Hellman密钥协商

D-H

- 实体A和实体B约定一个只有两个人知道的共同密钥的过程如下图所示。



Diffie-Hellman密钥协商



- Diffie-Hellman算法：
- 实体A秘密选定一个随机整数X_A，$1 \leq X_A \leq p-2$，并计算$y_A \equiv g^{x_A} \pmod{p}$发送给实体B;
- 类似地，实体B秘密选定一个随机整数X_B, $1 \leq X_B \leq p-2$，并将$y_B \equiv g^{x_B} \pmod{p}$发送给实体A；
- 然后A和B分别计算$k \equiv (Y_B)^{X_A} \pmod{p}$和$k \equiv (Y_A)^{X_B} \pmod{p}$；
- 计算出的k就是共享密钥。

Diffie-Hellman密钥协商

- 假设A和B选取公共参数p=97，以及模p的原根g=5；
  - A选取秘密参数X_A=36；
  - B选取秘密参数X_B=58；

试计算A与B的共享密钥。

● Diffie-Hellman密钥协商

例

- **解：** $Y_A \equiv 5^{36} \pmod{97} \equiv 50$，$Y_B \equiv 5^{58} \pmod{97} \equiv 44$。在交换$Y_A, Y_B$后，A和B分别计算
  - $k \equiv (Y_B)^{X_A} \equiv 44^{36} \equiv 75 \pmod{97}$,
  - $k \equiv (Y_A)^{X_B} \equiv 50^{58} \equiv 75 \pmod{97}$.