现代密码学
Modern Cryptography

张方国
中山大学计算机学院

Office: Room 305, IM School Building
E-mail: isszhfg@mail.sysu.edu.cn
HomePage: https://cse.sysu.edu.cn/content/2460

第十八讲 DLP（一）

第6章 公钥密码学和离散对数

- ElGamal密码体制
- 离散对数的算法
- 通用算法的复杂度下界
- 有限域
- 椭圆曲线
- 实际中的离散对数算法
- ElGamal体制的安全性

ElGamal密码体制

离散对数问题

对于一个n阶元素$\alpha \in G$，其中G是一个有限乘法群。定义

$$< \alpha > = \{\alpha^i : 0 \le i \le n-1\}$$

显然，$< \alpha >$是G的一个子群，也是一个n阶循环群。

实例1：取G为有限域Z_p(p为素数)的乘法群，α为模p的本原元。这时有$n = | < \alpha > | = p-1$。

离散对数问题 实例：乘法群$(G, \cdot)$，一个n阶元素$\alpha \in G$和元素$\beta \in < \alpha >$。

问题：找到唯一的整数a，$0 \le a \le n-1$，满足

$$\alpha^a = \beta$$

我们将这个整数a记为$\log_\alpha \beta$，称为β的离散对数。

DLP密码体制

密码学中的离散对数具有如下的性质：求解离散对数（可能）是困难的，而其他逆运算指数运算可以应用平方-乘的方法有效地计算。换句话说，在适当的群G中，指数函数是单向函数。

当一个群G满足如下性质时，可用于构造密码体制：

- 1，群元素可以（用计算机）紧致的表示；
- 2，群运算可以有效的执行；
- 3，DLP(给定 g, h=g^a, 计算a)是困难的。

ElGamal密码体制

密码体制6.1 Z_p^*上的ElGamal公钥密码体制

设p是一个素数，使得$(Z_p^*,\cdot)$上的离散对数问题是难处理的，令$\alpha \in Z_p^*$是一个本原元。令$\mathscr{P} = Z_p^*$，$\mathscr{C} = Z_p^* \times Z_p^*$，定义

$$K = \{(p,\alpha,a,\beta) : \beta \equiv \alpha^a (\mod p)\}$$

p,α,β是公钥，a是公钥。

加密: 对$K = (p,\alpha,a,\beta)$，以及一个（秘密）随机数$k \in Z_{p-1}$，定义

$$e_K(x,k) = (y_1,y_2)$$

其中$y_1 = \alpha^k \mod p$且$y_2 = x\beta^k \mod p$

解密: 对$y_1,y_2 \in Z_p^*$，定义

$$d_K(y_1,y_2) = y_2(y_1^a)^{-1} \mod p$$

ElGamal密码体制

在ElGamal密码体制中，加密运算是随机的，因为密文既依赖于明文x又依赖于Alice选择的随机数k。所以，对于同一个明文，会有许多可能的密文。

ElGamal密码体制的工作方式可以非正式地描述如下：明文x通过乘以β^k"伪装"起来，产生y_2。值α^k也作为密文的一部分传送。Bob知道私钥a，可以从α^k计算出β^k。最后用y_2除以β^k除去伪装，得到x。

例6.1 设$p = 2579$，$\alpha = 2$。α是模p的本原元。令$a = 765$，所以$\beta = 2^{765} \mod 2579 = 949$。

假定Alice现在想要传送消息$x = 1299$给Bob。比如$k = 853$是她选择的随机数。那么她计算

$$y_1 = 2^{853} \mod 2579 = 435$$

$$y_2 = 1299 \times 949^{853} \mod 2579 = 2396$$

当Bob收到密文$y = (435, 2396)$后，它计算$x = 2396 \times (435^{765})^{-1} \mod 2579 = 1299$，正是Alice加密的明文。

ElGamal密码体制

分析：1）如果Oscar能计算$a = \log_{\alpha} \beta$，那么ElGamal密码体制就是不安全的，因为那时Oscar可以像Bob一样解密密文。因此，ElGamal密码体制安全的一个必要条件就是Z_p^*上的离散对数问题是难处理的。

2) 对于这种形式的离散对数问题，不存在已知多项式时间的算法。为了防止已知的攻击，p应该至少取300个十进制位，$p-1$应该具有至少一个较大的素数因子。

离散对数的算法

最基本的算法：穷举搜索算法，总时间需要$O(n)$；和查表法，需要$O(n)$步预先计算和$O(n\log n)$存储空间解决。

- Shanks算法，需要时间为$O(m)$，存储空间为$O(m)$。其中$m=\lceil\sqrt{n}\rceil$。
- Pollard ρ离散对数算法，时间复杂度为$O(\sqrt{n})$。
- Pohlig-Hellman算法，时间复杂度为$O(c\sqrt{q})$；
- 指数演算法，时间复杂度为$O(e^{(1+o(1))\sqrt{In\ p\ In\ In\ p}})$。

穷搜索方法

小步大步方法

Pohlig-Hellman方法

Pollard pho方法

指标计算（指数演算）法

通用算法复杂度下界

$\Omega(\sqrt{(n)})$是阶为素数n的（子）群中离散对数问题的任何通用算法的一个复杂度下界。