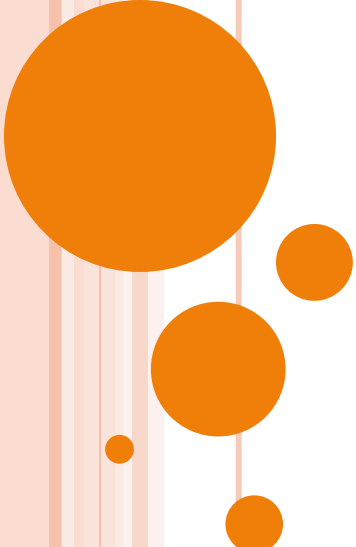


公开（非对称）密码算法之 *ELGAMAL*密码体制



范明钰
信息安全研究中心

三类数学难题—回顾

- ◆ **大整数分解**问题 (*The Integer Factorization Problem*, RSA体制)
- ◆ **有限域的乘法群**上的离散对数问题 (*The Discrete Logarithm Problem*, ElGamal体制)
- ◆ **椭圆曲线**上的离散对数问题 (*The Elliptic Curve Discrete Logarithm Problem*, 类似的ElGamal体制)

ElGamal

- 安全性基于离散对数
- 是Diffie-Hellman key distribution scheme 的变形
- published in 1985 by ElGamal: 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.
- 缺点：增加了消息长度（2倍）

补充—离散对数

◆ 运算

◆ 构造

◆ 难题

离散对数 (运算)

◆ (模n)指数 (幂) 运算

对任意整数 n , 定义集合 Z_n^* 如下:

$$Z_n^* = \{a : 1 \leq a \leq n-1, \gcd(a, n) = 1\}$$

显然, Z_n^* 中含有 $\phi(n)$ 个元素: 因为 Z_n^* 对模 n 的乘法构成群。
由Euler定理, 对任意的 $a \in Z_n^*$ 有

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

定义 a 的 (模 n) 阶 $\text{ord}_n(a)$ 为:

$$\text{ord}_n(a) = \min \{m : m \geq 1, a^m \equiv 1 \pmod{n}\}$$

例子: Z_{19}^* 中所有元素的幂次表

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	16

离散对数 (构造)

对某个 $a \in Z_n^*$, 若

$$\text{ord}_n(a) = \phi(n)$$

则称 a 是 Z_n^* 的 **本原根 (本原元)**

由前面 Z_{19}^* 的 **幂表** 可知: 2, 3, 10, 13, 14, 15 均是 Z_{19}^* 的 **本原根**

Z_n^* 中本原根的存在性:

当 $n = 2, 4, p^e, 2p^e$ 时, Z_n^* 存在本原根,

这里的 p 是奇素数。以下我们均假设 $n = p$

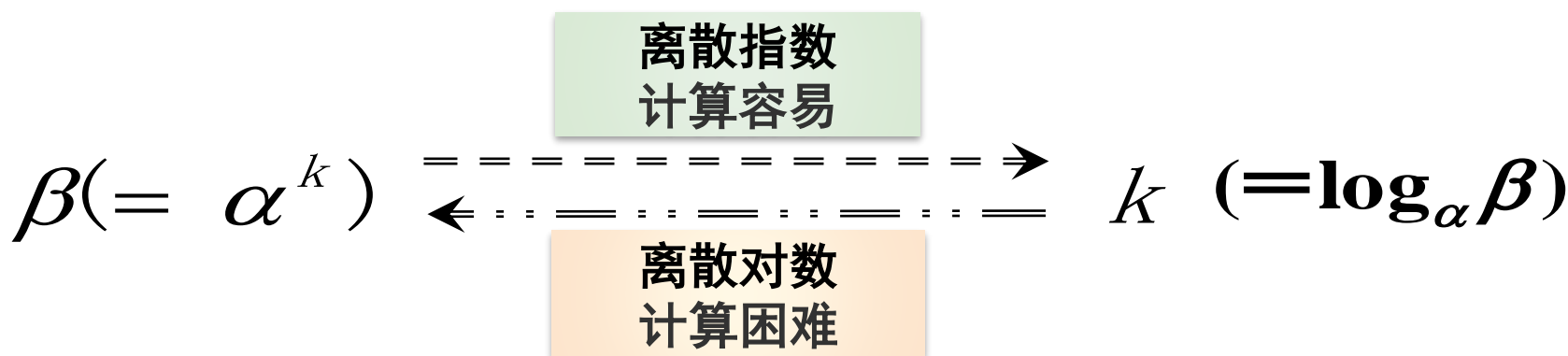
离散对数 (难题)

◆ (模n)离散对数运算

给定 Z_p^* 及其一个本原根 α

对 $\forall \beta \in Z_p^*$, \exists 唯一的整数 k , $1 \leq k \leq p-1$, 使得

$$\beta = \alpha^k \pmod{p}$$



离散对数（计算例子）

例 $Z_7^* = (1, 2, 3, 4, 5, 6)$

3 和 5 都是 Z_7^* 的一个生成元。 $\log_3 6 = ?$ $\log_3 6 = 3$

$\log_5 2 = ?$ $\log_5 2 = 4$

$$1^1 = 1$$

$$2^1 = 2; 2^2 = 4; 2^3 = 8 \equiv 1$$

$$3^1 = 3; 3^2 = 2; 3^3 = 2 \times 3 = 6; 3^4 = 6 \times 3 \equiv 4; 3^5 = 4 \times 3 \equiv 5; 3^6 = 5 \times 3 \equiv 1$$

$$4^1 = 4; 4^2 = 2; 4^3 = 2 \times 4 \equiv 1$$

$$5^1 = 5; 5^2 = 4; 5^3 = 4 \times 5 \equiv 6; 5^4 = 6 \times 5 \equiv 2; 5^5 = 2 \times 5 \equiv 3; 5^6 = 3 \times 5 \equiv 1$$

$$6^1 = 6; 6^2 = 36 \equiv 1$$

ElGamal 密码体制

1. 体制描述

2. 例子

3. 安全性

ElGamal 密码体制—描述

1. 体制描述

确定公共参数:

选择大素数 p , $\alpha \in \mathbb{Z}_p^*$ 是本原根, 将 p 和 α 公开

确定公私钥对:

随机且秘密地选择整数 d , $0 \leq d \leq p-2$, 计算

$$\beta = \alpha^d \bmod p$$

p, α, β --公开密钥 (公钥)

d --保密密钥 (私钥)

ElGamal 密码体制--加解密

加密变换： 对于任意明文 $m \in \mathbb{Z}_p^*$ ，发方秘密随机地

选取整数 $k, 1 < k < p - 1$

密文： $(c_1, c_2) = (\alpha^k \bmod p, m\beta^k \bmod p)$

解密变换： 对任意密文 $(c_1, c_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$

明文： $m = c_2 (c_1^d)^{-1} \bmod p$

ElGamal密码体制—证明

解密变换的正确性证明：

$$\begin{aligned}\text{因为 } c_1 &= \alpha^k (\text{mod } p), \\ c_2 &= m\beta^k (\text{mod } p) \\ &= m(\alpha^d)^k (\text{mod } p)\end{aligned}$$

$$\begin{aligned}\text{所以 } c_2(c_1^d)^{-1} &\equiv m\beta^d(\alpha^{dk})^{-1} (\text{mod } p) \\ &\equiv m\alpha^{dk}(\alpha^{dk})^{-1} (\text{mod } p) \\ &\equiv m (\text{mod } p)\end{aligned}$$

ElGamal密码体制 一例子

例子-1

确定公共参数：对 $p=19$, 有

$$Z_{19}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$$

$\alpha = 2$ 是 Z_{19}^* 的一个本原根

确定（用户B的）公私钥对：

用户B秘密地选择整数 $d=10$ ，计算

$$\beta = \alpha^d \bmod p = 2^{10} \bmod 19 = 17$$

$p=19, \alpha=2, \beta=17$ —— 公钥

10 —— 私钥

ElGamal密码体制 一例子

例子-2

加密： 用户 A 加密发送明文 $m=11$ 给用户 B，

A 选择一个随机数 $d = 7, 1 < d < 19 - 1$ ，并计算

$$c_1 = \alpha^d \bmod p = 2^7 \bmod 19 = 14$$

$$c_2 = m\beta^d \bmod p = 11 \times 17^7 \bmod 19 = 17$$

A 将 $(c_1, c_2) = (14, 17)$ 发送给 B；

解密： B 收到密文后 $(c_1, c_2) = (14, 17)$ ，计算：

$$\begin{aligned} m &= c_2 (c_1^d)^{-1} \bmod p \\ &= 17 \times (14^7)^{-1} \bmod 19 \\ &\equiv 17 \times 4 \equiv 11 \bmod 19 \end{aligned}$$

加解密计算例子

- ◆ 选择 $p=97$ 及本原根 $a=5$
- ◆ 收方选择 秘密钥 $x_B=58$ ，计算并发布公钥 $y_B=5^{58}=44 \pmod{97}$
- ◆ 若发方要加密 $M=3$ 给收方，发方工作：
 - 首先获得收方的公开密钥 $y_B=44$
 - 选择随机 $k=36$ 计算: $K=44^{36}=75 \pmod{97}$
 - 计算密文对:
 - $C_1 = 5^{36} = 50 \pmod{97}$
 - $C_2 = 75 \cdot 3 \pmod{97} = 31 \pmod{97}$
- ◆ 收方收到 $\{50,31\}$ ，收方工作：
 - 计算 $K=50^{58}=75 \pmod{97}$
 - 计算 $K^{-1} = 22 \pmod{97}$
 - 计算明文 $M = 31 \cdot 22 = 3 \pmod{97}$

ELGAMAL体制---密钥建立

密钥生成

双方选取大素数 p 及本原元 $a \bmod p$

收方选秘密密钥 x_B

计算 $y_B = a^{x_B} \bmod p$

ElGamal密码体制—分析

3. 安全性

▲ ElGamal算法的安全性基于
在循环群 Z_p^* 上求离散对数问题是困难

目前关于离散对数的分析方法有：

Shanks算法

Pohlig-Hellman算法

指标计算法

量子计算机可以快速求解离散对数问题，但量子计算机从理论研究到实际应用，还会有相当长的时间

ElGamal密码体制

3. 安全性

- ▲ 实用时，素数 p 至少为700位十进制数（2048 bit），而且要求 $p-1$ 至少有一个大的素因子。
- ▲ ElGamal加密算法是一种随机算法，随机数 k 不能暴露，也不能重用。
- ▲ 假设用同一个 k 来加密两个消息 m_1, m_2 ，所得到的密文分别为 $(a_1, b_1)(a_2, b_2)$ ，则 $b_1/b_2 = m_1/m_2$ ，故若 m_1 已知， m_2 可以很容易地计算出来。

算法分析

- ◆ *D.Bleichenbache* “*Generating ElGamal Signatures Without Knowing the Secret Key*”中提到了攻击方法和对策
- ◆ ElGamal的安全性主要依赖于 p 和 d ，若选取不当则签名容易伪造，应保证 d 对于 $p-1$ 的大素数因子不可约
- ◆ 签名算法的安全性主要依赖于乘法群上的离散对数计算。素数 p 必须足够大，且 $p-1$ 至少包含一个大素数因子以抵抗Pohlig & Hellman算法的攻击
- ◆ 明文应采用信息的HASH值(如SHA算法)
- ◆ 美国*DSS*(*Digital Signature Standard*)的*DSA*(*Digital Signature Algorithm*)算法是经ElGamal算法演变而来

ELGAMAL签名方案

ElGamal 加密算法是不可交换的
存在一个相关的签名算法
安全性是基于计算离散对数的困难性
方案的密钥生成是相同的:
有个共享的素数 p , 公开的本原根 a
每个用户选择一个随机数作为私钥 x
计算各自的公开密钥: $y = a^x \bmod p$
公钥是 (y, a, p)
私钥是 (x)

ELGAMAL方案小结

选择

一个素数 p , p 的一个原根 α , 一个整数 d , 令 $\beta = \alpha^d$, 公开 $\{p, \alpha, \beta\}$, 保密 d .

明文信息 x

加密: 秘密选择随机数 k , 计算将 $(\alpha^k \bmod p, x\beta^k \bmod p)$ 作为密文

解密: $(x\beta^k)((\alpha^k)^d)^{-1} \equiv x\alpha^{dk} \times \alpha^{-dk} \equiv x \bmod p$

信息有扩张

实现参考

- ◆ <http://www.hackchina.com/cont/11646>

作业

1. 参考前面所列的 Z_{19}^* 中所有元素的幂次表, 构造 Z_{17}^*

中所有元素的幂次表。

2. 说明3是 Z_{17}^* 的一个生成元。计算

$$\log_3 5 = ?$$

$$\log_3 (-7) = ?$$

$$\log_3 7 = ?$$

$$\log_3 16 = ?$$

3. 按照ElGamal密码体制中小例子的步骤, 在 Z_{17}^* 中若取

$\alpha=3, d=9, k=11, m=13$, 完成加密和解密。

1题答案:

Z_{17}^* 中所有元素的幂次表

a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

2题答案: $\log_3 5 = 5$ $\log_3 (-7) = 3$
 $\log_3 7 = 11$ $\log_3 16 = 8$

3题答案: $\beta = \alpha^d \bmod p = 3^9 \bmod 17 = 14$
 $c_1 = \alpha^k \bmod p = 3^{11} \bmod 17 = 7$
 $c_2 = m \beta^k \bmod p = 13 \cdot 14^{11} \bmod 17 = 11$
 $(c_1, c_2) = (7, 11)$

$$\begin{aligned} m &= c_2 (c_1^d)^{-1} \bmod p \\ &= 11 (7^9)^{-1} \bmod 17 \\ &= 11 \cdot 12 \bmod 17 = 13 \end{aligned}$$

下次内容

◆ 椭圆曲线密码算法：ECC