

### ElGamal 数字签名实验



### 实验目的

- > 了解数字签名的过程(签名过程和认证过程)
- > 掌握 ElGamal 算法的密钥生成过程
- > 掌握 ElGamal 算法的数字签名方案



#### 实验内容

本次实验需要大家完成 ElGamal 数字签名算法,推荐大家用 Java 或者 Python 实现,**签名的信息 m 是你的学号,需要随机生成两次不同的 k 进行签名并验证** 签名,并且验证下假设消息 m 在传送过程中被修改的情况。

- 1. 需要将公钥(p, g, y)和私钥 x 以及每次使用的随机数 k 打印输出;
- 2. 用学号作为消息 m , 并打印输出随机生成两次不同的 k 的签名信息和签名验证的结果;
- 3. 验证签名时,可以假设消息 m 被篡改的情况,要输出验证签名不通过的信息。
- 4. Hash 算法建议用SHA256, 先对消息 m 进行 Hash 运算, 然后再进行签名。



ElGamal密码算法是一种不确定性公钥加密算法,它的安

全性是基于有限域上计算离散对数问题的困难性。

### 实验原理

#### > 密钥生成

- ◆选择大素数p,  $g \in \mathbb{Z}_p^*$  是一个生成元, p 和 g 是公开的;
- ◆ 随机选择整数 x, 1 < x < p 1, 计算  $y = g^x \mod p$

公钥就是 (*y, p, g* )

私钥是随机数✗



对于消息m, 首先随机选取整数k,  $1 \leq k \leq p-1$ , 然后计算:

$$r = g^k \mod p$$
,  $s = k^{-1}(H(m) - xr) \mod (p-1)$ 

则m的签名为(r, s), 其中H为Hash函数。

注意: k 与p-1互素,即 gcd(k, p-1)=1; k-1 是 k mod p-1的逆。

### 实验原理---验证算法

接收方在收到消息加和签名(r,s)后,验证

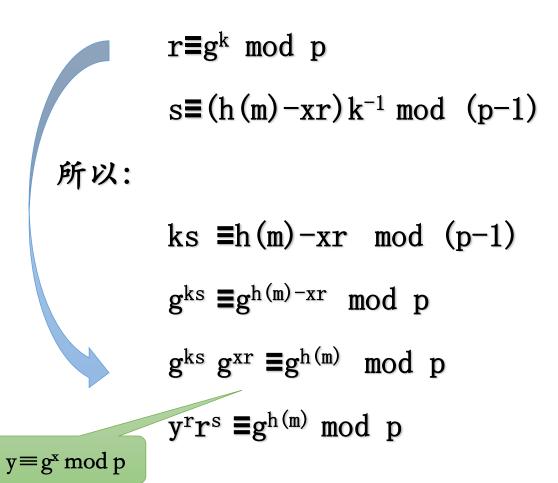
$$y^r r^s \equiv g^{H(m)} \mod p$$

如果等式成立,则(r,s)是消息m的有效签名;反之,则是无效签名。



#### 实验原理---ElGamal签名的正确性

#### 因为:



## HWORLD PHYSICS HARM BOURDARY PHYSICS HARM BO

#### 举个例子

◆选择 p = 467, g = 2, x = 127,则有 y = g<sup>x</sup> mod p = 2 <sup>127</sup> mod 467 = 132 mod 467 = 132

即: 公钥为(467, 2, 132), 私钥为 127

◆假设消息 m 的 Hash 值 H (m) = 100, 选择的随机数 k = 213, 这 里满足 gcd (213,466) =1

其中k-1 = 213-1 = 431 mod 466 = 431

◆计算签名: r = 2<sup>213</sup> mod 467 = 29 mod 467 = 29, s = (100 – 127\* 29) \*431 mod 466 = 51

消息m的签名 (r, s) 为 (29, 51)

◆验证签名,首先计算 H (m) = 100 验证 132<sup>29</sup> \* 29<sup>51</sup> mod 467 = 189 = 2<sup>100</sup> mod 467

## HISTORY PHYSICS HISTORY CONTRICTORY CONTRI

#### 实验步骤

- 1. 用 SHA256 计算消息 m 的 Hash值;
- 2. 生成 ElGamal 算法的公钥 (p, g, y) 和私钥 x ;
- 3. 随机生成满足条件的 k , 1≤k≤p-1 并且 k 与 p-1 互素;
- 4. 计算签名 (r, s);
- 5. 验证签名(一次 m 正常,一次 m 异常也就是修改学号的至少一位),输出验证结果。



#### 实验要求

- 提交内容
- ① 实验结果截图
- 截止时间
- 一周内提交至HITsz Grader 作业提交平台,具体截止日期参考平台发布。
  - 登录网址:: http://grader.tery.top:8000/#/login
  - 推荐浏览器: Chrome
  - 初始用户名、密码均为学号,登录后请修改

# 请同学们开始实验!

