



哈爾濱工業大學(深圳)

HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

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。



实验原理

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 , $g \in Z_p^*$ 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

$$y = g^x \bmod p$$

公钥就是 (y, p, g)

私钥是随机数 x



实验原理---签名算法

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

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

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 $k \bmod p-1$ 的逆。



实验原理---验证算法

接收方在收到消息 m 和签名 (r, s) 后，验证

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

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。


$$r \equiv g^k \pmod{p}$$

$$s \equiv (h(m) - xr) k^{-1} \pmod{p-1}$$

$$k_s \equiv h(m) - x r \pmod{p-1}$$

$$g^{ks} \equiv g^{h(m)-xr} \pmod{p}$$

$$g^{ks} g^{xr} \equiv g^{h(m)} \pmod{p}$$

$$y^r r^s \equiv g^{h(m)} \pmod{p}$$

$$y \equiv g^x \pmod{p}$$



即：公钥为(467, 2, 132)，私钥为 127

其中 $k^{-1} = 213^{-1} = 431 \pmod{466} = 431$

消息m的签名 (r, s) 为 (29, 51)

验证 $132^{29} * 29^{51} \bmod 467 = 189 = 2^{100} \bmod 467$



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 ， $1 \leq k \leq p-1$ 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！

