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. 补充说明：Hash 算法不是必须的，如果不对消息 m 进行 Hash 运算， 那么算法使用中就可以将 H(m) 换成 m。

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，　$1 < \mathrm{x} < p-1$，计算

$$y = g^{\mathrm{x}} \bmod p$$

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，$1 \leqslant k \leqslant p-1$，然后计算：

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

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 mod 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

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

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

因为有 $s = k^{-1}(H(m) - xr) mod (p-1)$

所以有 $rx + sk = H(m) mod (p-1)$

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

举个例子

◆选择 p = 467， g = 2， x = 127， 则有 $y = g^x \bmod p = 2^{127} \bmod 467 = 132 \bmod 467 = 132$

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

◆计算签名：$r = 2^{213} \bmod 467 = 29 \bmod 467 = 29$， $s = (100 - 127 * 29) * 431 \bmod 466 = 51$

消息m的签名（r, s）为 （29，51）

◆验证签名，首先计算 H（m） = 100

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

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. 补充说明：Hash 算法不是必须的，如果不对消息 m 进行 Hash 运算， 那么算法使用中就可以将 H(m) 换成 m。

实验要求

- **请把电子版实验报告及源代码打包成一个zip上传到系统中，命名格式如下：**

  压缩包：“学号_姓名_密码学基础_实验4”

http://10.249.12.98:8000/#/login

请同学们开始实验！