哈尔滨工业大学（深圳）

《密码学基础》实验报告

实验 4 ElGamal 数字签名算法

学　院: 计算机科学与技术

姓　名: 王木一

学　号: 200210231

专　业: 计算机科学与技术

日　期: 2022-10-31

1、 截图 2 组，公钥和私钥相同，选取的随机值 k1 和 k2 不同，用学号作为消息 m，打印输出内容包括公钥（y,p,g）,私钥 x，签名结果(r,s)以及验证结果。

```
请输入需要签名的消息:200210231
--->【第1次签名与验证】
首先Alice进行签名
公钥(p, g, y):9467,1858,8946. 私钥x:6720. 秘密随机数k:2369
签名信息(r, s):(6457, 6907)
是否让Bob进行验证? 1-开始 0-退出:1
y^r*r^s mod p = 1840, g^m mod p = 1840
      验证通过:)
--->【第2次签名与验证】
首先Alice进行签名
公钥(p, g, y):9467,1858,8946. 私钥x:6720. 秘密随机数k:5075
签名信息(r, s):(3057, 381)
是否让Bob进行验证? 1-开始 0-退出:1
y^r*r^s mod p = 1840, g^m mod p = 1840
      验证通过:)
```

2、 假设收到的消息 m 被篡改了，打印输出 发送时的消息 m 和接收后被篡改的消息 m’ 以及验证签名失败的结果，并截图，公钥、私钥以及 k 都可以用上面 1 中用到的值。

```
是否进行消息篡改实验? 1-开始 0-退出:1
->【消息篡改】
--->首先Alice进行签名
公钥(p, g, y):9467,1858,8946. 私钥x:6720. 秘密随机数k:5283
签名信息(r, s):(8639, 2049)
--->中间人篡改消息
原消息：200210231, 篡改后：8820116
--->Bob验证篡改后的消息
y^r*r^s mod p = 1840, g^m mod p = 4094
     验证失败:(
演示结束
```

3、 思考 1，用 ElGamal 方案计算一个签名时，使用的随机数 k 能不能泄露？请给出你的思考并分析原因。

不能。

因为：

当 k 被敌手知道，以下公式中

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

仅 x 未知，敌手可轻易算出私钥 x。这样敌手就可以构造出正确的消息签名对，进行冒充。

4、 思考 2，如果采用相同的 k 值来签名不同的两份消息，这样是否安全？请给出你的思考并分析原因。

不安全。

因为：

假设现有m_1, m_2两份消息使用相同 k 进行签名，签名结果如下：

$$r_1 = g^k \bmod p \quad s_1 = k^{-1}(H(m_1) - xr_1) \bmod (p-1)$$

$$r_2 = g^k \bmod p \quad s_2 = k^{-1}(H(m_2) - xr_2) \bmod (p-1)$$

其实$r_1 = r_2$

$$\frac{s_1}{s_2} = \frac{H(m_1) - xr_1}{H(m_2) - xr_2} \bmod (p-1)$$

上面的公式只有私钥 x 未知，可以很快算出。这样敌手就可以构造出正确的消息签名对，进行冒充。