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: 吴梓滔

学　号: 220110430

专　业: 计算机科学与技术


日　期: 2024-11-06

一、根据实验内容回答如下几个问题

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。

```
PS C:\Users\83923\Desktop\CryLab> & C:/Users/83923/AppData/Local
t/WindowsApps/python3.8.exe c:/Users/83923/Desktop/CryLab/elgama
------1 生成密钥------
p:  13338156247297579847
g:  5
y:  13300497261906607799
x:  9301005707853832664
------2 第一次签名------
消息:  220110430
本次签名使用的k:  7478345774336244055
第一次 r:  6486074893180203325
第一次 s:  5124698739661771070
------3 第二次签名------
本次签名使用的k:  11711821653427898 75
第二次 r:  125795263832788205 73
第二次 s:  105372766572050394 04
------4 验证第一次签名结果------
要验证的消息:  220110430
验证成功
------5 验证第二次签名结果------
验证成功
```

用同一组密钥，用不同随机数 k 进行了两次签名，分别进行验证。

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。

```
验证成功
PS C:\Users\83923\Desktop\CryLab> & C:/Users/83923/AppDa
t/WindowsApps/python3.8.exe c:/Users/83923/Desktop/CryLa
------1 生成密钥------
p:  17104134114375556343
g:  5
y:  13099211669268261750
x:  11178417401388052000
------2 第一次签名------
消息:  220110430
本次签名使用的k:  11040804375943106975
第一次 r:  41772351503731919 21
第一次 s:  45009226215973576 92
------3 第二次签名------
本次签名使用的k:  19454048922129439 69
第二次 r:  135467513591435442 25
第二次 s:  98993555671570608 64
------4 验证第一次签名结果------
要验证的消息:  220110431
验证失败
------5 验证第二次签名结果------
验证失败
```

收到的消息 m 被改，两次验证均失败。

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。

随机数不可以泄露。如果 k 被攻击者知晓，由于 p 和 g 是公开的，攻击者可以直接算出$r = g^k$,此时只要攻击者截获了一组发送的信息 m 及其前面$sig(m) = (r, s)$，攻击者可以通过$k \cdot s = H(m) - xr \ mod(p-1)$,由于 k、s、r 和算法 H 均为攻击者已知，攻击者可以求出$xr \ mod(p-1) = x \cdot g^k mod(p-1)$,由于已知$g^k$，求出它的逆也是容易的，将逆元$r^{-1}$乘上去，就恢复出了私钥 x。

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。当两份消息用相同 k 值签名，意味着 k，r 相同。当攻击者截获这两个消息组，会得到

$$s_1 = k^{-1}H(m_1) - xr \ mod(p-1)$$

$$s_2 = k^{-1}H(m_2) - xr \ mod(p-1)$$

两式相减，可以消去 xr，从而先求出 k 值。求出 k 值后，按照 3 中的步骤可以得到私钥 x。

二、密码学基础实验课程的收获和建议（**必填部分**）

*（关于本学期密码学实验的收获与体会，以及**你的意见和建议**。）*

通过实验，理解了密码学算法的具体实现，并且自己实现了几个算法，感觉自己很厉害。实验中具体实现一些基础的数学算法，比如有限域运算、扩展欧几里得算法、素数检测，对理解理论课中抽象的数学原理有巨大的帮助。通过编程实现了解了对消息进行加密的一个完整过程。