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: 房煊梓

学　号: 210010101

专　业: 智能强基-计算机

日　期: 2023-10-30

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。

```
p=109254429199088733509421382258544586 6169
q=546272145995443667547106911292722933084
g=135675131004154478536676446735995433421
第1组
公钥(y,p,g):
y=176425554769388360296068636192011115101
p=109254429199088733509421382258544586 6169
g=135675131004154478536676446735995433421
私钥x=118117820183270876888675567043876 6198687
本次随机选取的k值为:731530881653470507739317905086912535799
消息:210010101
签名结果(r,s):
r=559980054074230406746893696848430199464
s=518078928083758523473857634190720209925
进行验证
验证通过
```

```
第2组
公钥(y,p,g):
y=176425554769388360296068636192011115101
p=109254429199088733509421382258544586 6169
g=135675131004154478536676446735995433421
私钥x=118117820183270876888675567043876 6198687
本次随机选取的k值为:332910865047118190181385553732738404 61
消息:210010101
签名结果(r,s):
r=175606701690759775005878795099730029182
s=560530128481846612870992424547114718973
进行验证
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。

```
p=109254429199088733509421382258544586616 9
q=546272145995443667547106911292722933084
g=135675131004154478536676446735995433421
第1组
公钥(y,p,g):
y=176425554769388360296068636192011115101
p=109254429199088733509421382258544586616 9
g=135675131004154478536676446735995433421
私钥x=118117820183270876888675567043876619868 7
本次随机选取的k值为:731530881653470507739317905086912535799
消息:210010101
签名结果(r,s):
r=559980054074230406746893696848430199464
s=518078928083758523473857634190720209925
进行验证
验证通过
篡改消息为:abcdefghi
进行验证
篡改后验证失败
```

```
第2组
公钥(y,p,g):
y=176425554769388360296068636192011115101
p=109254429199088733509421382258544586616 9
g=135675131004154478536676446735995433421
私钥x=11811782018327087688867556704387661986 87
本次随机选取的k值为:33291086504711819018138555373273840461
消息:210010101
签名结果(r,s):
r=17560670169075977500587879509973002918 2
s=56053012848184661287099242454711471897 3
进行验证
验证通过
篡改消息为:abcdefghi
进行验证
篡改后验证失败

Process finished with exit code 0
```

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。

使用的随机数 k 不能泄露。因为 p,H(m)和签名(r,s)是公开的，可以计算出 r^{-1} 的值。如果能获取 k 值，由$s=k^{-1}(H(m)-xr) \bmod (p-1)$，故可以转换形式为 $x=r^{-1}(H(m)-sk) \bmod (p-1)$，因此可以计算出私钥 x。如果将消息篡改为 m'，则由于 k^{-1} 可以计算，故此时可以计算出相应的 $s'=k^{-1}(H(m')-xr) \bmod (p-1)$，使得 $y^r r^{s'} \equiv g^{H(m')} \bmod p$。若篡改签名为(r,s')，验证者在收到篡改后的消息哈希值$H(m')$和篡改后的签名(r,s')后进行验证，验证可以通过。所以随机数 k 不能泄露。

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。假设签名者对发送给 A 的消息 m1 和对发送给 B 的消息 m2 使用相同的 k 进行签名，签名分别为(r,s1)和(r,s2)。由于$s1=k^{-1}(H(m1)-xr) \bmod (p-1)$，$s2=k^{-1}(H(m2)-xr) \bmod (p-1)$，则$(s1-s2)k=(H(m1)-H(m2)) \bmod (p-1)$，由于$m1 \neq m2$，故$(s1-s2) \neq 0 \bmod (p-1)$，故$k=(H(m1)-H(m2))\ (s1-s2)^{-1} \bmod (p-1)$，因此计算出 k，相当于第 3 问 k 泄露的情况，所以不安全。

二、网络与信息安全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，给出评论以及**改进的建议**。）*

本学期一共有四次密码学实验，分别为 AES 对称密码算法，RSA 公钥加密算法，Hash 长度扩展攻击和 ElGamal 数字签名，在完成这些实验的过程中，我的收获是将理论课程学到的内容真正落实到代码来执行，加深了对其中的算法的理解。对于本实验，我的建议是继续保持指导书和 PPT 中对于算法的讲解和提示，它们为实验完成提供了很好的思路。