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: 杨行

学　号: 200111325

专　业: 计算机科学与技术

日　期: 2022-11-01

1、 截图 2 组，公钥和私钥相同，选取的值 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。

第一部分：

生成密钥，输出内容包括公钥（y,p,g）,私钥 x

```
请输入需要加密的明文：
20011325
生成的明文的Hash值：100721959929124013483408697702845239258677917100734918167589403589506715945642
1.密钥生成  2.进行签名  3.进行验证 4.退出
1
大素数：22735953235379755250827100383021340464809431131288405875271284899244183396274768801931635525969845893784362896312108138586242785175731127701519305571985499
本原根：85559964209246135315567395762029328608483142578729120023461338866719509501568703746219129376495739918723789081223102700774282539291698291199631278293265 97
publicKey:22353278063270652541934582699123402737904937251110280876461777698526792519839439027281993711806038376801907323594248458873927137344487998861974520626020501
privateKey:13077878522833139377271876341189018448918511075999766363876278543999642284164923982855050424193122770877497779437149359119220771340214725602917167126939654
1.密钥生成  2.进行签名  3.进行验证 4.退出
2
```

第二部分：

使用随机数进行签名

输出内容包括选取的值 k1 和 k2，对应的签名结果(r,s)

```
1.密钥生成  2.进行签名  3.进行验证 4.退出
2
k1:818543803637397791665844515136977200450818071493215266946607748706584295098173573 29
签名信息r:37184013511050387363542519075568344075582219945696512469158938899409051475041444304031785358913705261603086153978421110259889367328532293036945777650725
签名信息s:20621493734287818235485437071866534504047558766454224594569499966303824492411553504899643534767429729516477830001406371577430541579833770717745444942604 82
**********
k2:867248698343600287266727437454834524857132812028247107624076940714317572512217726894440537451479040451244394639550164958643129721527757
签名信息r:191286715292965526119707022808410268906295965424474904462649042783554085444595492643435256313625679723790254716529880249230158469453092475811057124480822 71
签名信息s:190845897151377389235254357657033797495109644397060449587099167002150034042878522546845905880758379908678069015727640680854953642297936596298135121131443 74
**********
1.密钥生成  2.进行签名  3.进行验证 4.退出
3
```

第三部分：

进行验证，输出内容为验证结果

```
**********
1.密钥生成  2.进行签名  3.进行验证 4.退出
3
开始模拟传输数据
是否发动篡改攻击（Y/N?）
N
当前的k：818543803637397791665844515136977200450818071493215266946607748706584295098173573 29
验证成功!
当前的k：867248698343600287266727437454834524857132812028247107624076940714317572512217726894440537451479040451244394639550164958643129721527757
验证成功!
```

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。

假设进行了篡改。输出验证失败的信息采用 1 的 k 值和公私钥。

```
验证成功!
1.密钥生成  2.进行签名  3.进行验证 4.退出
3
开始模拟传输数据
是否发动篡改攻击（Y/N?）
Y
请输入篡改的明文:
20011112323
当前的k：818543803637397791665844515136977200450818071493215266946607748706584295098173573 29
验证失败，存在篡改可能!
当前的k：867248698343600287266727437454834524857132812028247107624076940714317572512217726894440537451479040451244394639550164958643129721527757
验证失败，存在篡改可能!
原信息:200111325     对应的哈希值：deae9becc8b36d5d91dad4c67adf8b0417893ec98fd60270215df15480550aaa
篡改的信息：20011112323     对应的哈希值：c51dc1a2339483039fc9fbe48bb4f456b6de5acb35f9d5dfb9de4f3ee0b2b98b
```

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。

答：不能，因为在签名过程存在计算式$s = k^{-1} * (H(m) - x * r) mod(p-1)$，由于 s，r 和 m 是需要发送的信息，p 是公开的信息。在攻击者知道使用的哈希函数的情况下或者接受信息者有意图的话，计算式对于他们只有 x 未知，可以通过计算一个一次同余方程得到私钥 x,从而伪造签名。

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。

答：不安全，用相同的 k 值签名不同的两份信息，会得到如下两个关系式：

$$\begin{cases} s_1 = k^{-1} * (H(m_1) - x * r) mod(p-1) \\ s_2 = k^{-1} * (H(m_2) - x * r) mod(p-1) \end{cases}$$

进而可得$\begin{cases} ks_1 = (H(m_1) - x * r) mod(p-1) \\ ks_2 = (H(m_2) - x * r) mod(p-1) \end{cases}$

即$k(s_1 - s_2) = (H(m_1) - H(m_2)) \, mod(p-1)$（除 k 外，都已知）

故而 k 可得，由思考题 3 可知，私钥 x 在 k 已知时可以解方程求出，

故不安全。