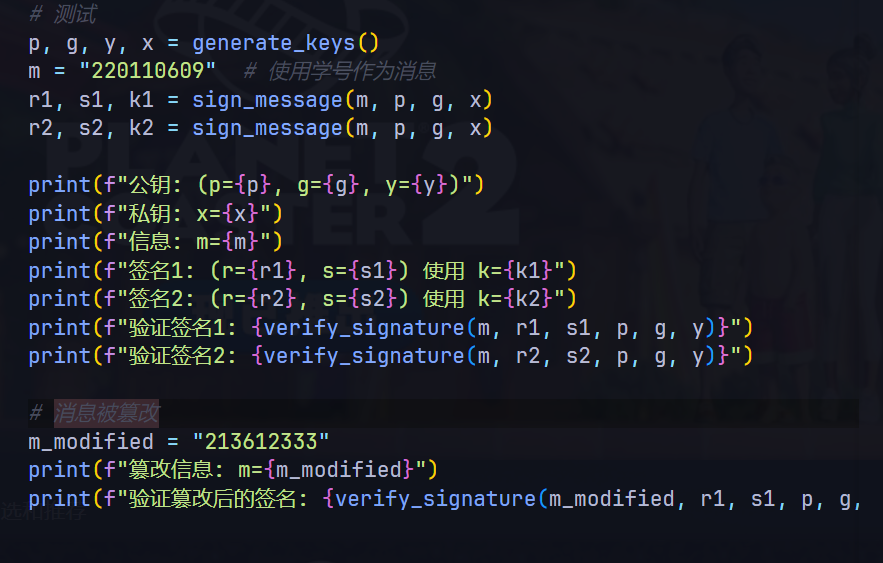
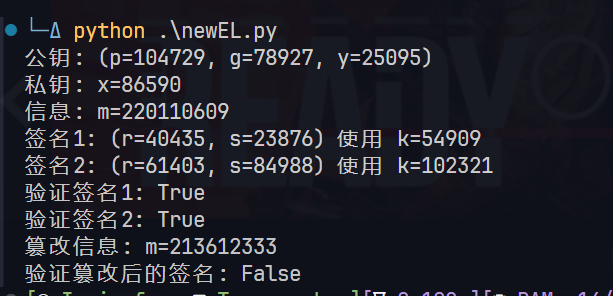
|  |
| --- |
| 哈尔滨工业大学（深圳） |
| **《密码学基础》实验报告** |
|  |
| 实验4 ElGamal 数字签名算法  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 李子韬 | | 学 号: | 220110609 | | 专 业: | 计算机科学与技术 | | 日 期: | 2023-xx-xx | |

一、根据实验内容回答如下几个问题

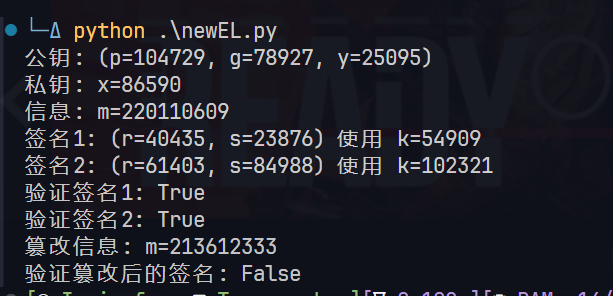
1. 截图2组，公钥和私钥相同，选取的随机值k1和k2不同，用学号作为消息m , 打印输出内容包括公钥（y,p,g）,私钥x，签名结果(r,s)以及验证结果。

输出部分：





1. 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。



1. 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，理由如下

如果k泄露，则攻击者可以轻易用下面的公式推断出私钥：

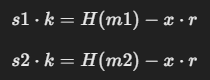


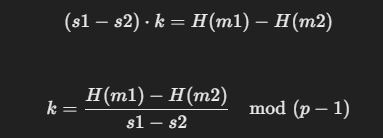
可见，攻击者可以在知道一个有效签名和消息的哈希值的情况下恢复出私钥，从而完全破坏系统的安全性。

1. 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，理由如下：

对于两个相同的k的两份签名：





这样，k就会被计算出来，从而参照上一个问题，可以解出私钥，破坏系统的安全性

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****。）*

通过这门实验课，我真切感受到密码学在实际应用中的存在，能够让密码的知识在计算机中实现是一种别样的体验。

通过AES实验，我更加深入理解对称加密的基本原理和加密模式（如ECB、CBC等）的差异，也对AES的加密流程了然于心；

RSA的实验让我真切理解了非对称加密的优缺点，激发了对数论的兴趣，为此，我专门去翻了一下数论相关的资料；

Hash长度扩展实验是一个验证实验，非常具有挑战性，能够将长度攻击的知识在框架下体验一遍，并且成功“hack”进seedlab那一刻还是很激动的；

最后的ElGamal数字签名，则是将我理论课不怎么掌握得好的部分让我做了一遍，通过这个实验，我了解到数字签名的重要性和安全机制，同时加深了对ElGamal算法的理解。

可以考虑添加椭圆曲线加密（ECC）和其他现代加密算法的实验，因为ECC在现代加密中应用广泛且更高效（而且很有挑战性）