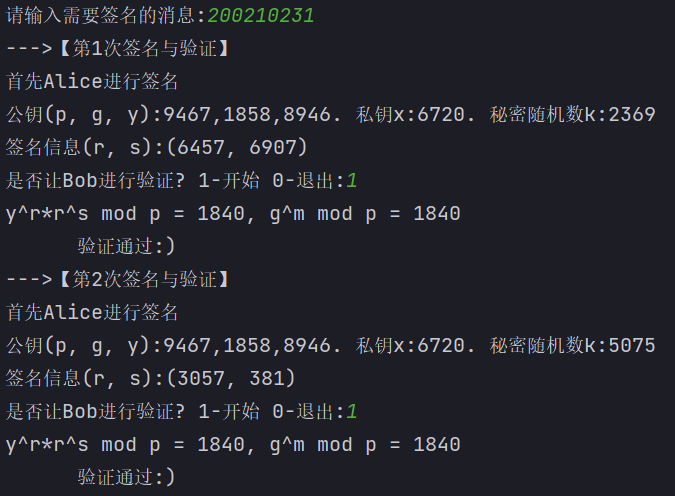
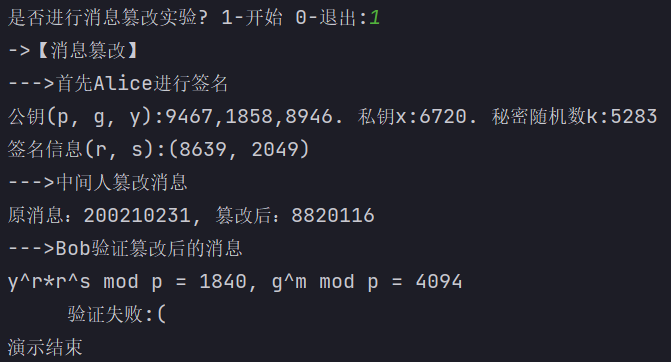
|  |
| --- |
| 哈尔滨工业大学（深圳） |
| **《密码学基础》实验报告** |
|  |
| 实验4 ElGamal 数字签名算法  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 王木一 | | 学 号: | 200210231 | | 专 业: | 计算机科学与技术 | | 日 期: | 2022-10-31 | |

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。



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。

因为：

当k被敌手知道，以下公式中



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。

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。

因为：

假设现有两份消息使用相同k进行签名，签名结果如下：

其实

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。