|  |
| --- |
| 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: | XXX | | 学 号: | XXXXXXXXX | | 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。
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。
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。
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。

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****。）*