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

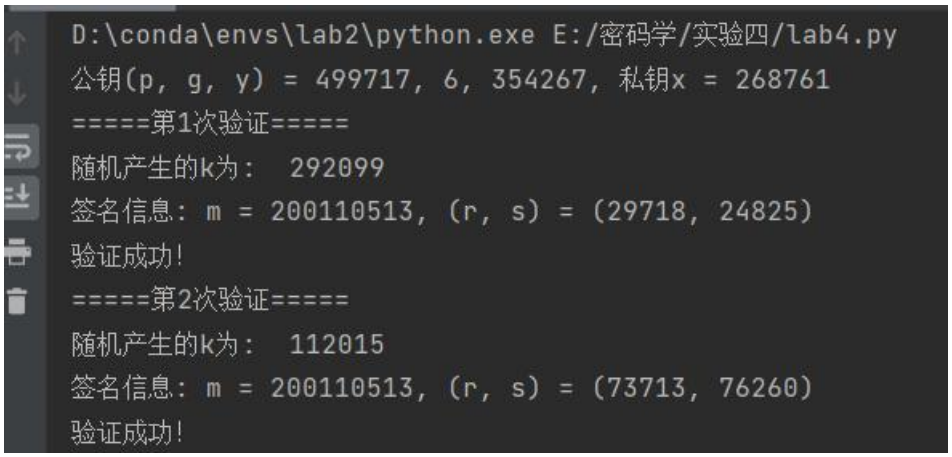
姓　名: 宗晴

学　号: 200110513

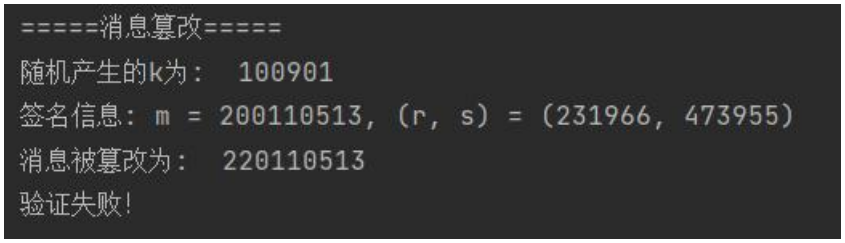
专　业: 计算机科学与技术

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。

不能。因为$s = k^{-1}(H(m) - xr) \bmod (p-1)$，又 s、r、p、m 均可知，所以若 k 泄漏，那么可以求解出私钥 x，就可以进行签名的伪造。

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。因为若用相同的 k 值来签名不同的两份消息，那么$s_1 = k^{-1}(H(m_1) - xr_1) \bmod (p-1)$，$s_2 = k^{-1}(H(m_2) - xr_2) \bmod (p-1)$，将两式左右对应相除，即可求解出私钥 x，就可以进行签名的伪造。