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。

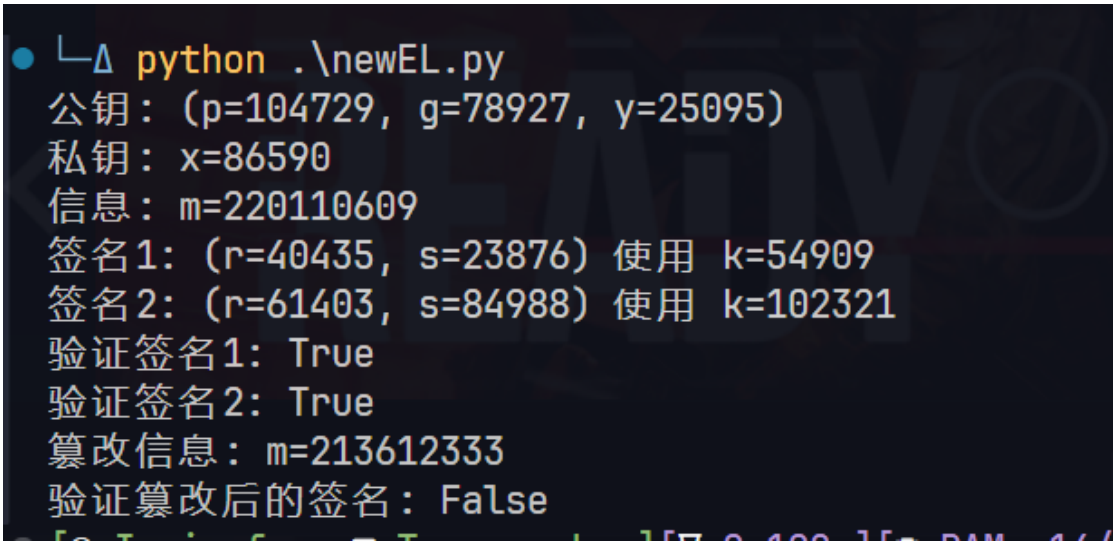
输出部分：

```python
# 测试
p, g, y, x = generate_keys()
m = "220110609"  # 使用学号作为消息
r1, s1, k1 = sign_message(m, p, g, x)
r2, s2, k2 = sign_message(m, p, g, x)

print(f"公钥: (p={p}, g={g}, y={y})")
print(f"私钥: x={x}")
print(f"信息: m={m}")
print(f"签名1: (r={r1}, s={s1}) 使用 k={k1}")
print(f"签名2: (r={r2}, s={s2}) 使用 k={k2}")
print(f"验证签名1: {verify_signature(m, r1, s1, p, g, y)}")
print(f"验证签名2: {verify_signature(m, r2, s2, p, g, y)}")

# 消息被篡改
m_modified = "213612333"
print(f"篡改信息: m={m_modified}")
print(f"验证篡改后的签名: {verify_signature(m_modified, r1, s1, p, g,
```

```
└─Δ python .\newEL.py
公钥: (p=104729, g=78927, y=25095)
私钥: x=86590
信息: m=220110609
签名1: (r=40435, s=23876) 使用 k=54909
签名2: (r=61403, s=84988) 使用 k=102321
验证签名1: True
验证签名2: True
篡改信息: m=213612333
验证篡改后的签名: False
```

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，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：

$$k \cdot s = H(m) - x \cdot r \mod (p-1)$$

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。

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，理由如下：

对于两个相同的 k 的两份签名：

$$s1 \cdot k = H(m1) - x \cdot r$$

$$s2 \cdot k = H(m2) - x \cdot r$$

$$(s1 - s2) \cdot k = H(m1) - H(m2)$$

$$k = \frac{H(m1) - H(m2)}{s1 - s2} \mod (p-1)$$

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）