**实验七** **RSA数字签名算法**

**姓名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_学号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **运行截图**
2. *截取两组测试结果（明文为test.txt文件中的内容）：对于test.txt改变前后的情况，截图中的内容包括明文的摘要和对应的签名后的结果，以及签名验证结果。*

1. **【选做】总结**

*对RSA数字签名算法的理解，如果不用HASH函数处理，会有什么问题？实验过程总结、感受、建议等等。*