西安电子科技大学

**应用密码学与网络安全 课程实验报告**

**实验名称 计算机与网络安全实验**

计算机科学与技术 学院 班

成 绩

姓名 学号

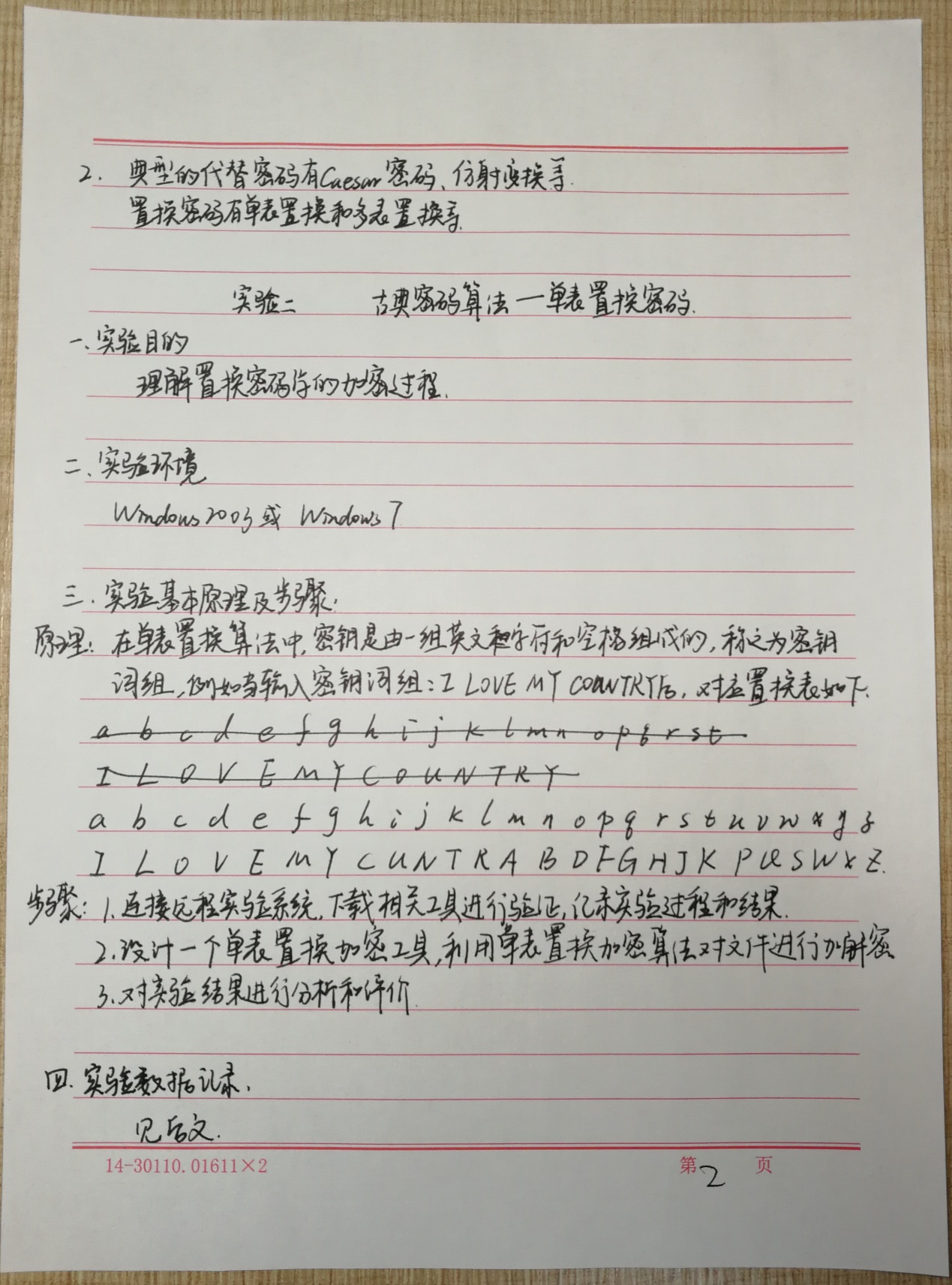
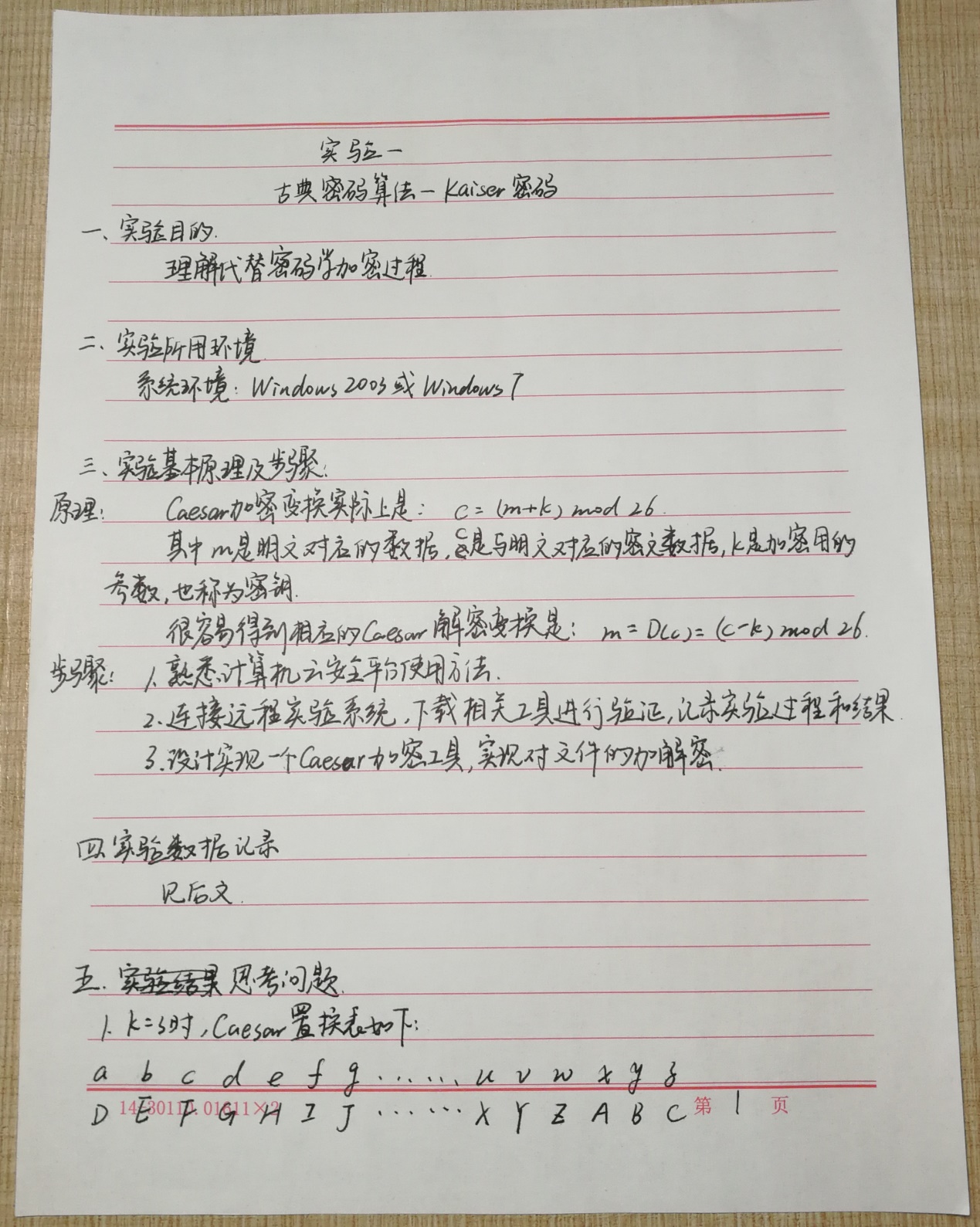
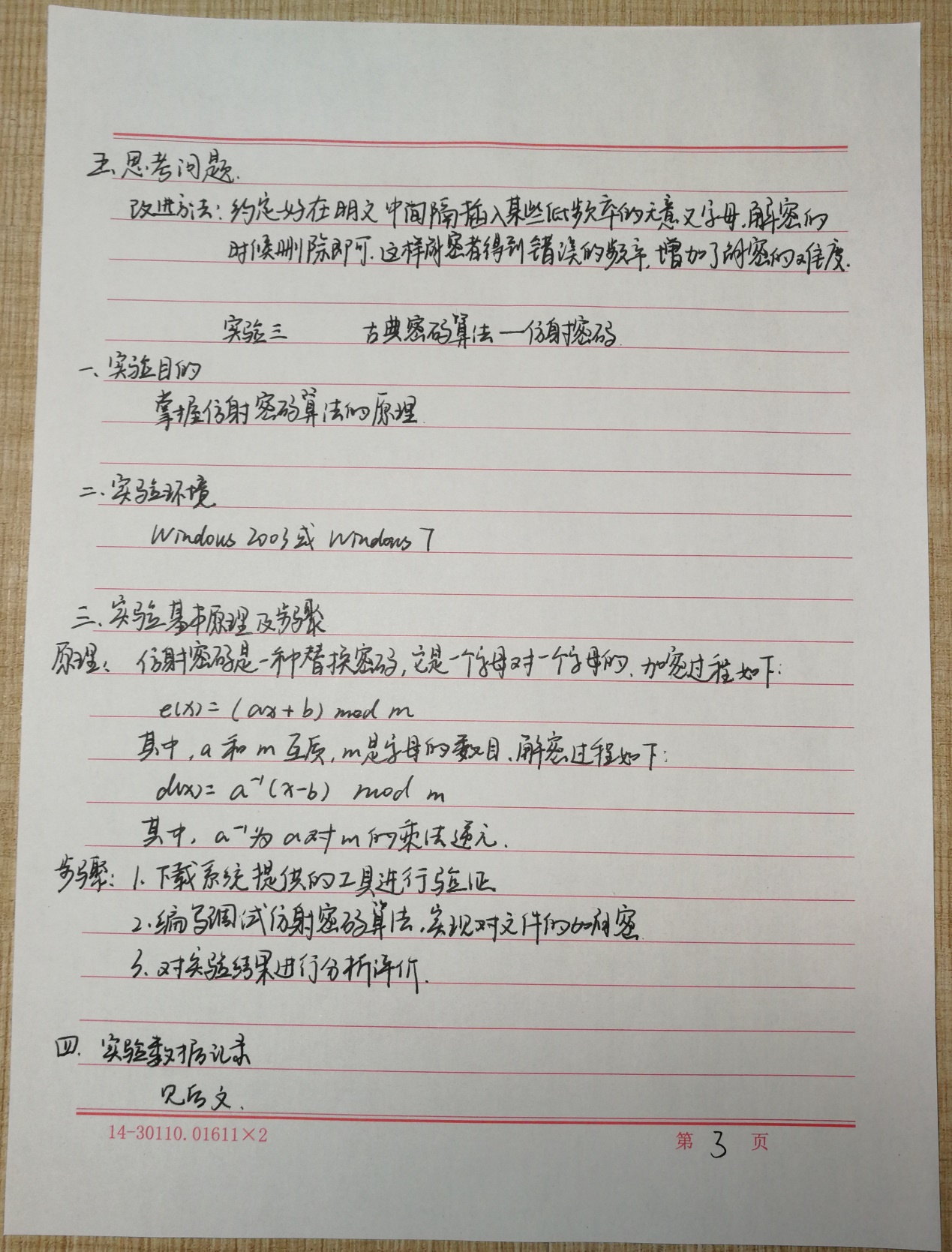
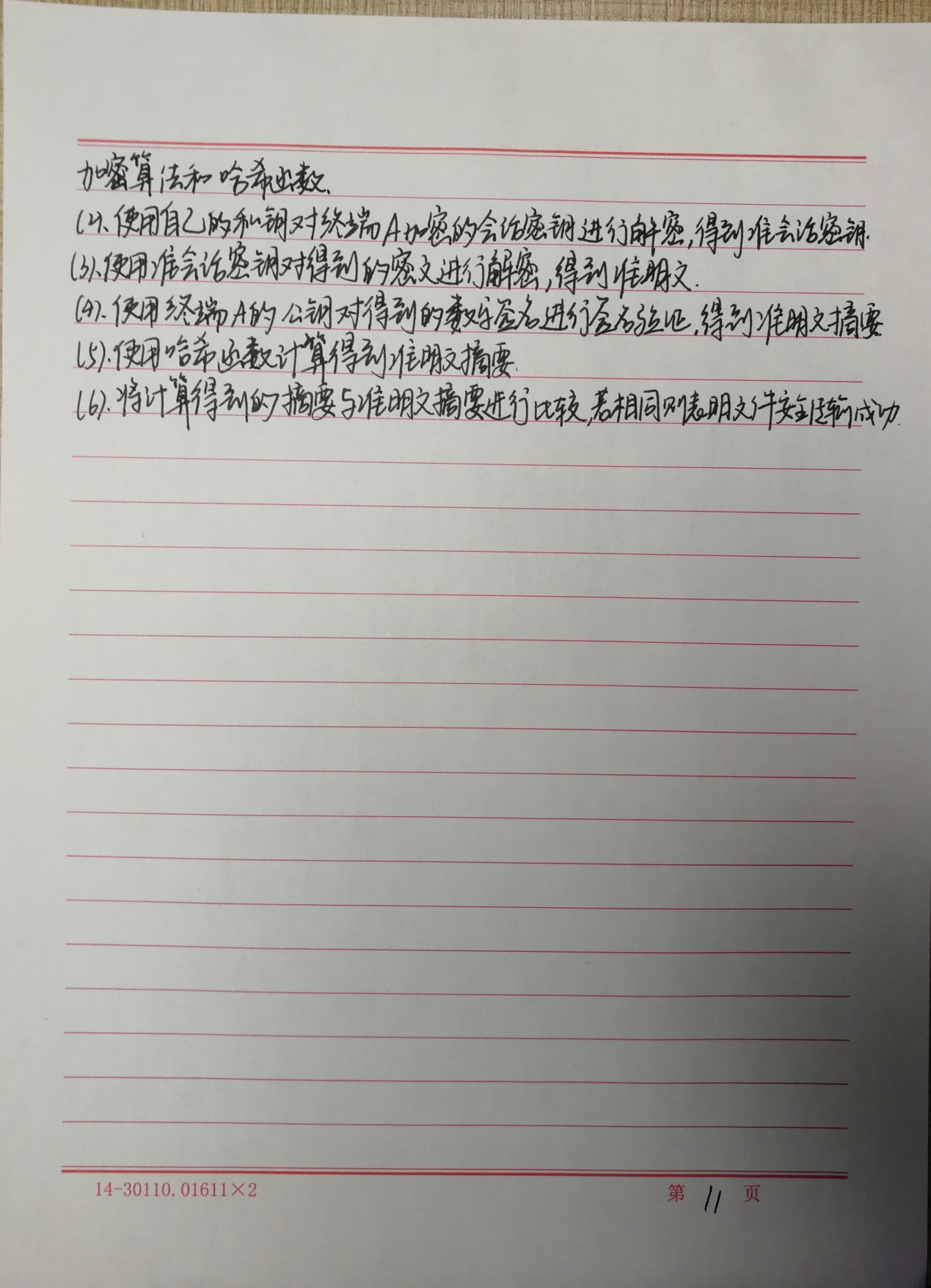
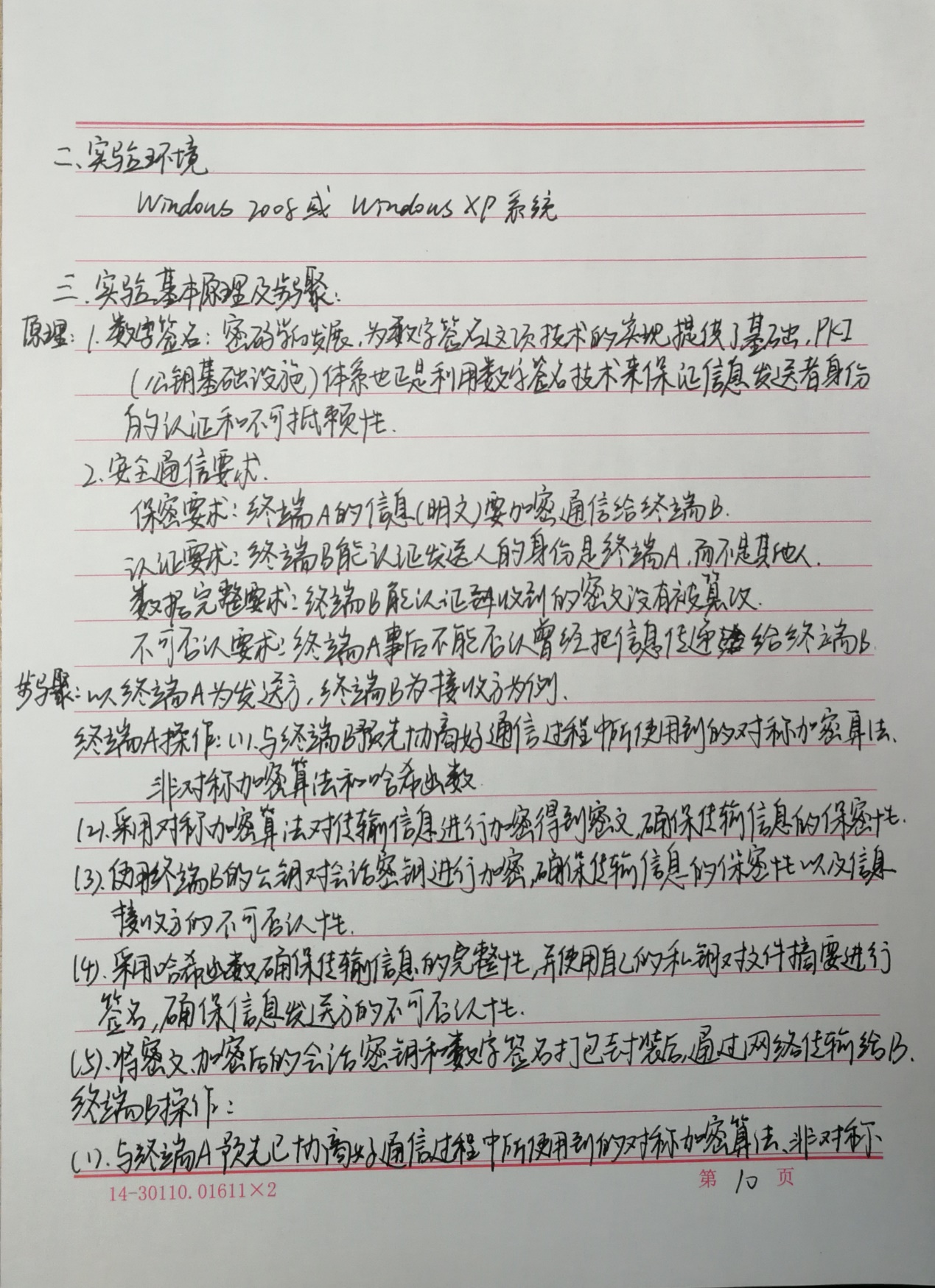
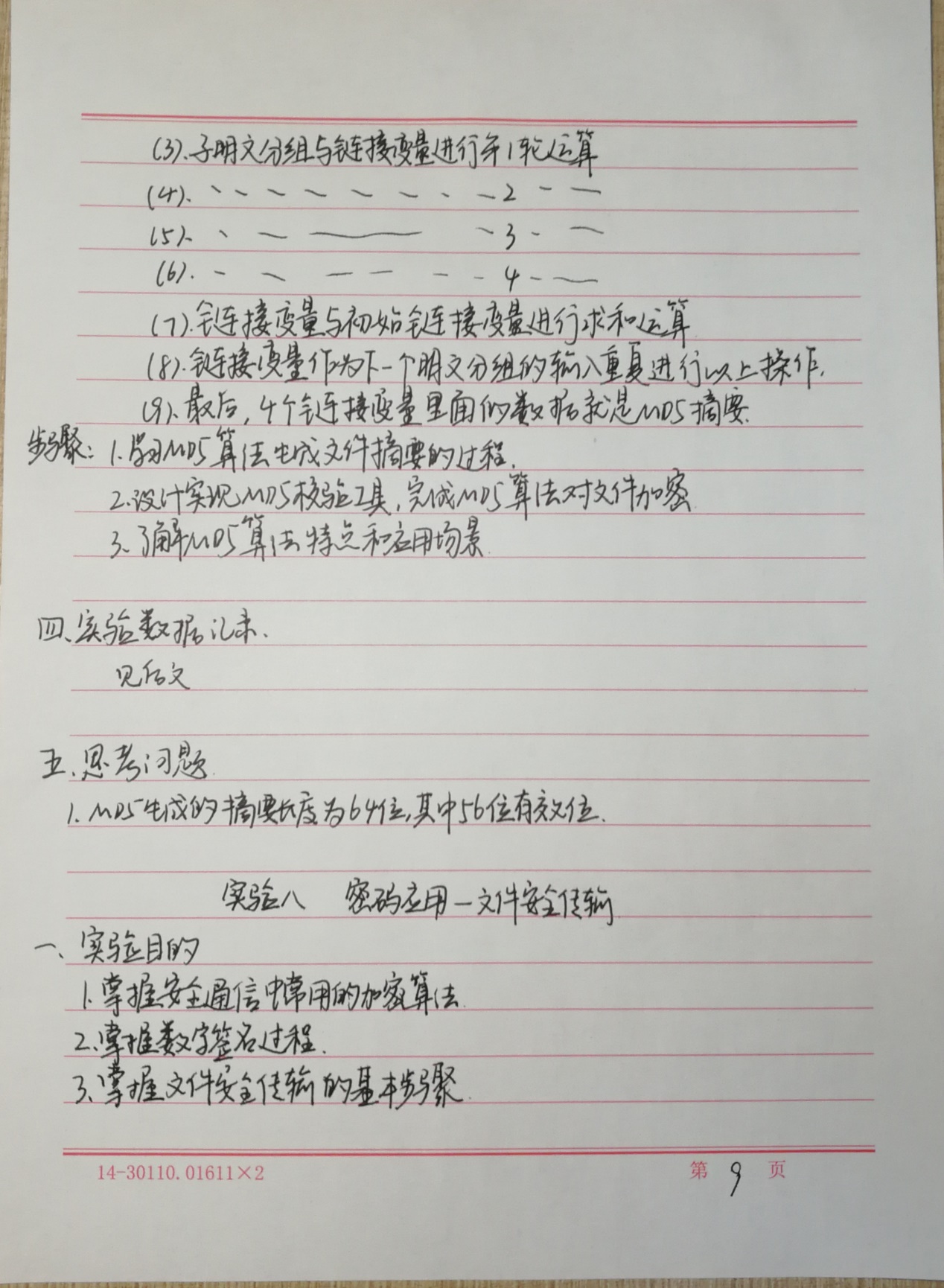
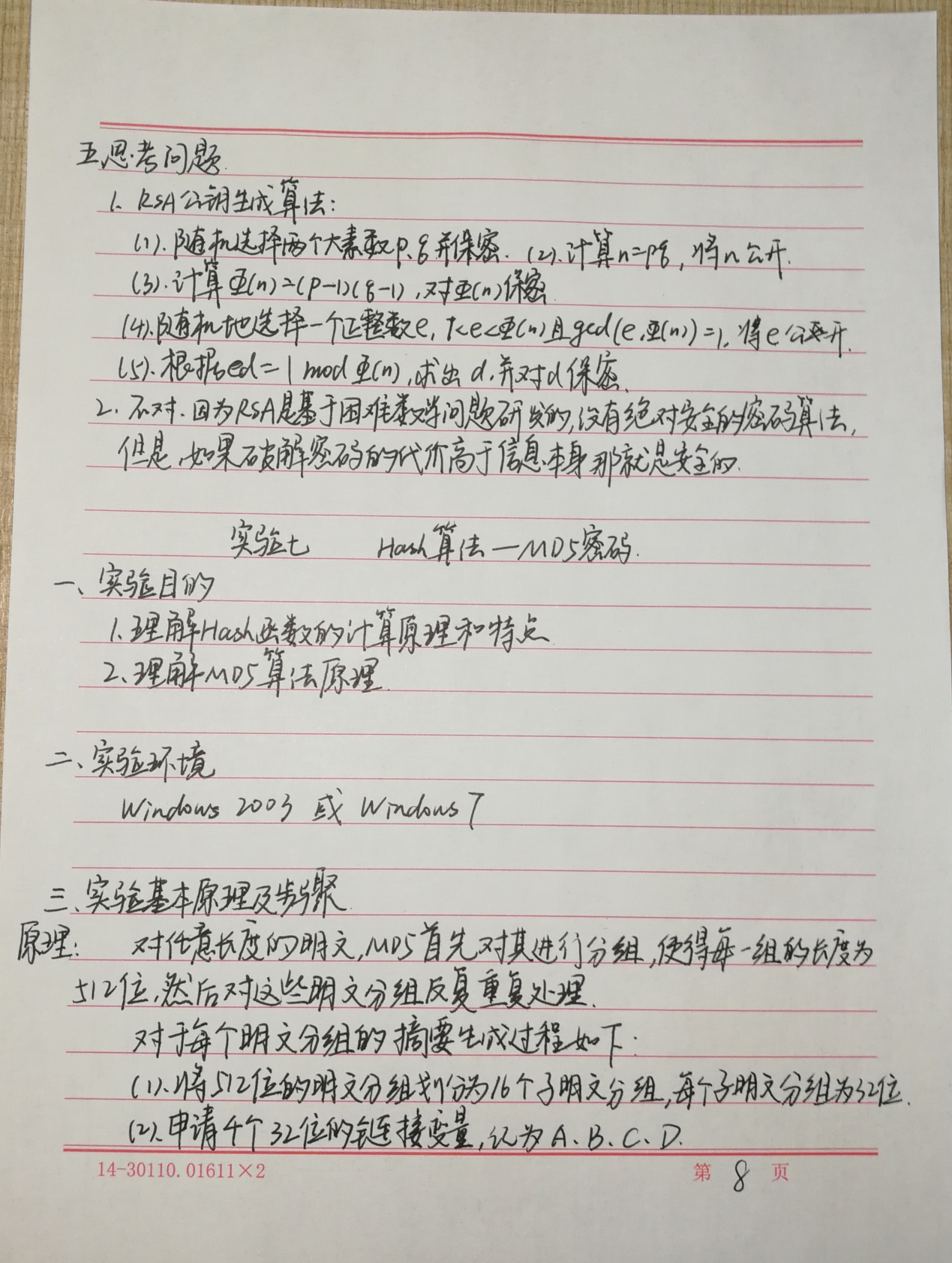
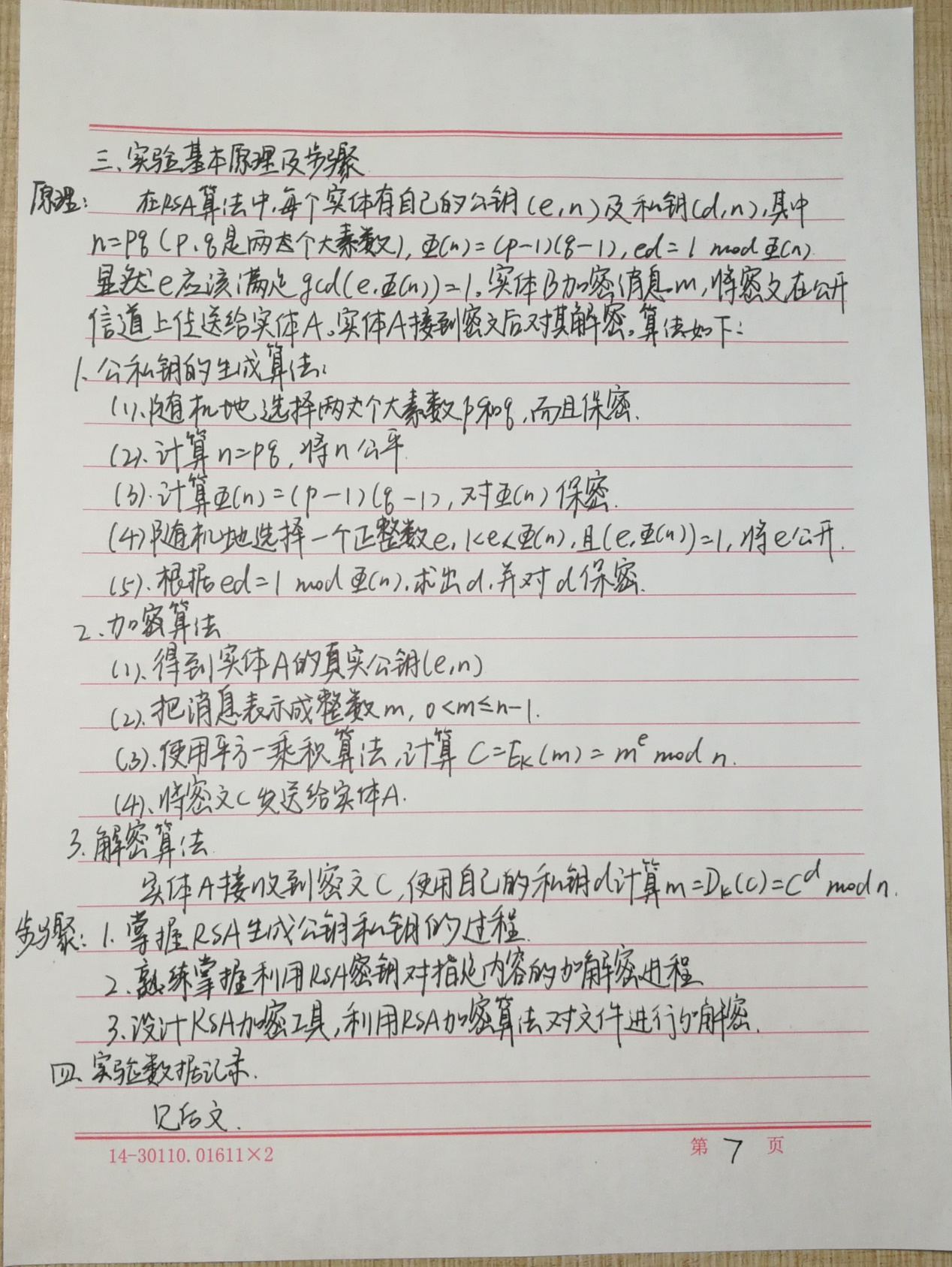
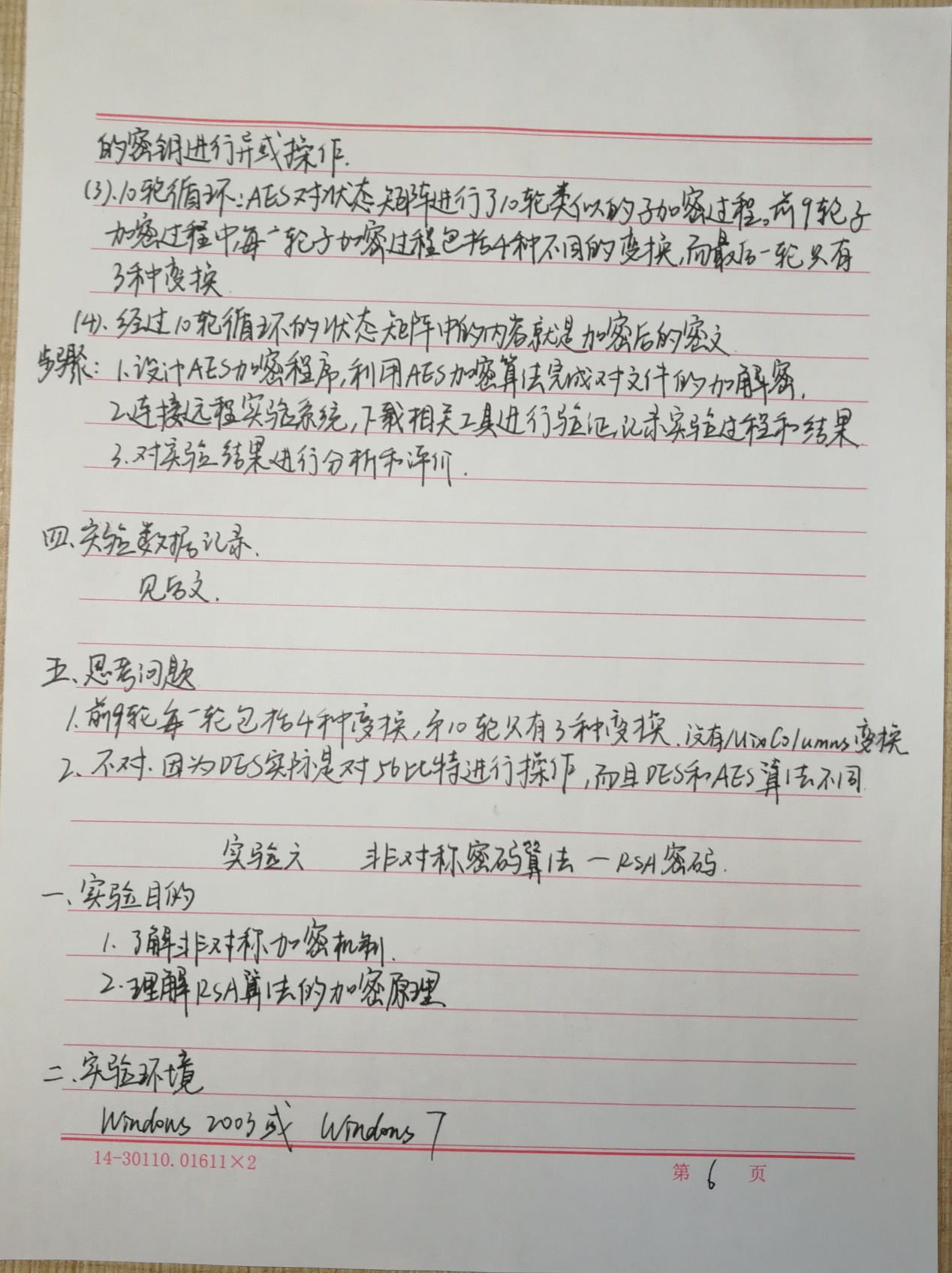
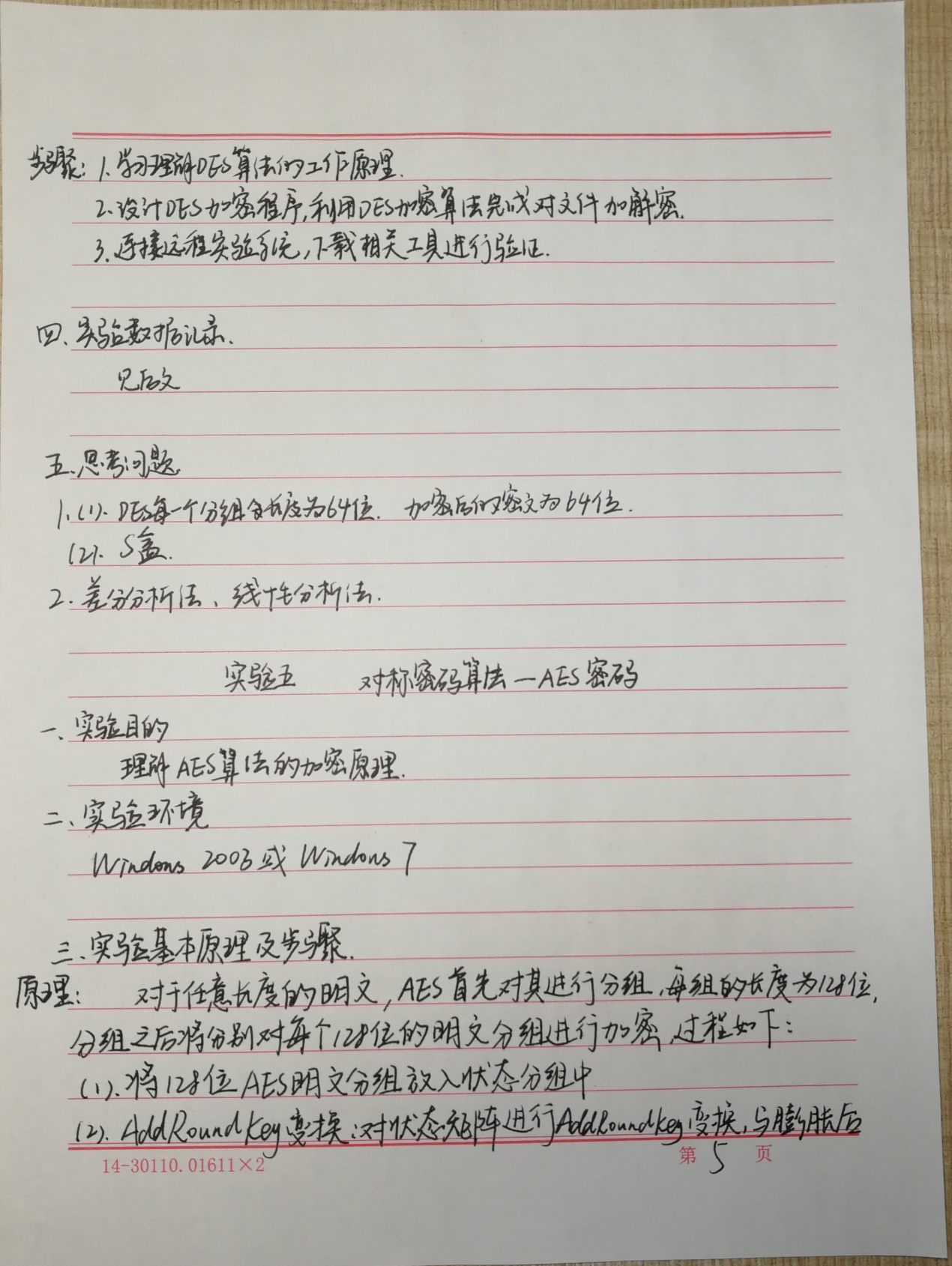
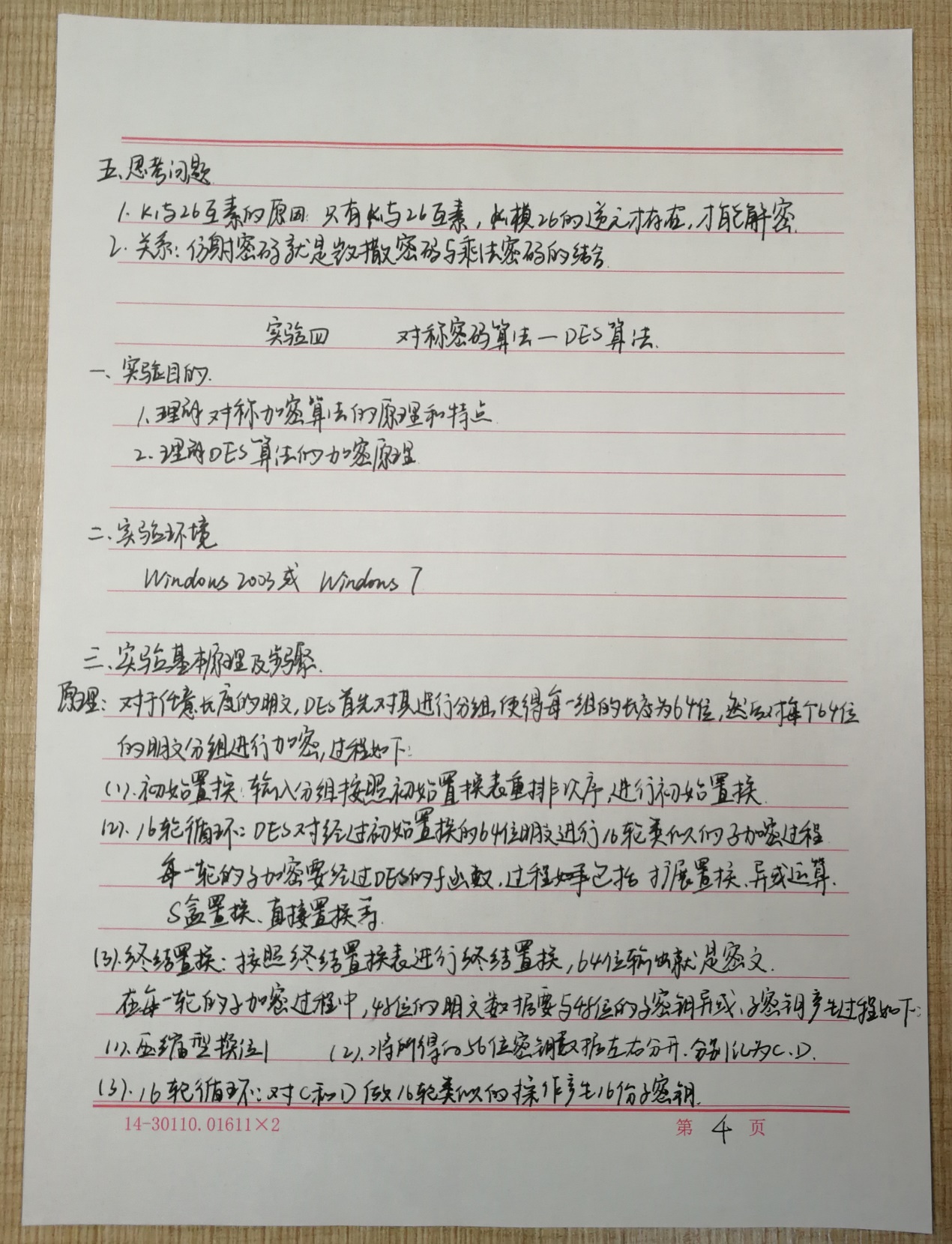
同作者

实验日期 2020 年 8 月 28 日

实验地点 EII-505

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# 一、实验报告

********

# 二、实验过程及实验结果截图

1. **凯撒密码：**

明文内容存放于文件plaintext.txt中，运行程序，选择密钥k=5，对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，密钥同上，对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



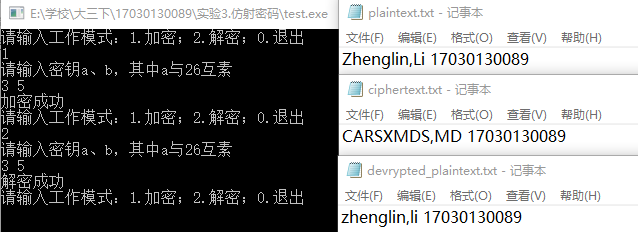
1. **单表置换密码：**

明文内容存放于文件plaintext.txt中，运行程序，选择密钥为“I love my country”，对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，密钥同上，对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



1. **仿射密码：**

明文内容存放于文件plaintext.txt中，运行程序，选择密钥a=3，b=5，对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，密钥同上，对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



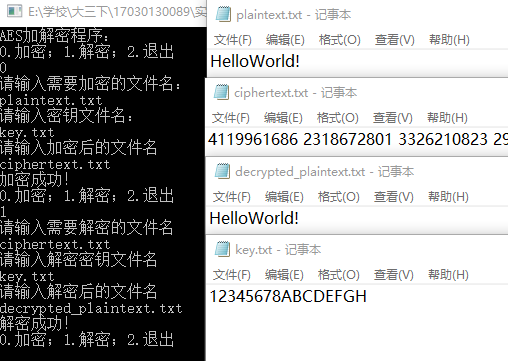
1. **DES算法：**

明文内容存放于文件plaintext.txt中，密钥内容存放与文件key.txt中，密钥为12345678。运行程序，对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，密钥同上，对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



1. **AES：**

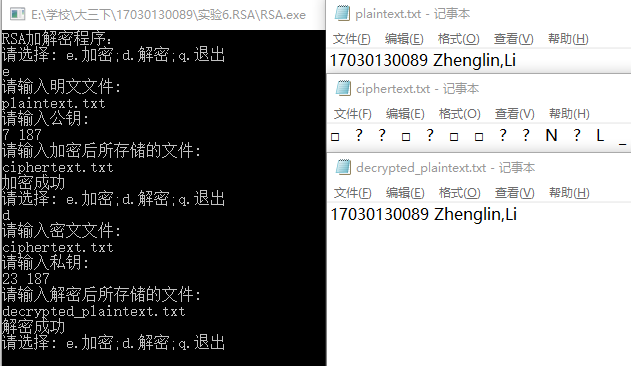
明文内容存放于文件plaintext.txt中，密钥内容存放与文件key.txt中，密钥为12345678ABCDEFGH。运行程序，对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，密钥同上，对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



1. **RSA：**

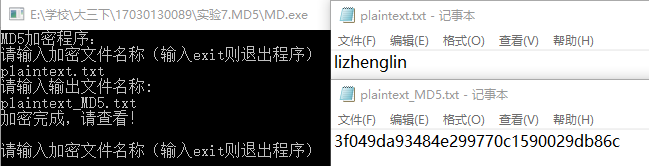
首先生成公私钥，选择p=11，q=17，e=7，则n=187，φ(n)=160，d≡e-1 (mod 160)，得d=23.则公钥为（7,187），私钥为（23,187）。

明文内容存放于文件plaintext.txt中。运行程序，使用公钥（7,187）对明文加密后，密文内容存放于文件ciphertext.txt中。然后进行解密，私钥为（23,187），对密文解密后的文件存放于文件decrypted\_plaintext.txt中，二者对比，内容一致。



1. **MD5：**

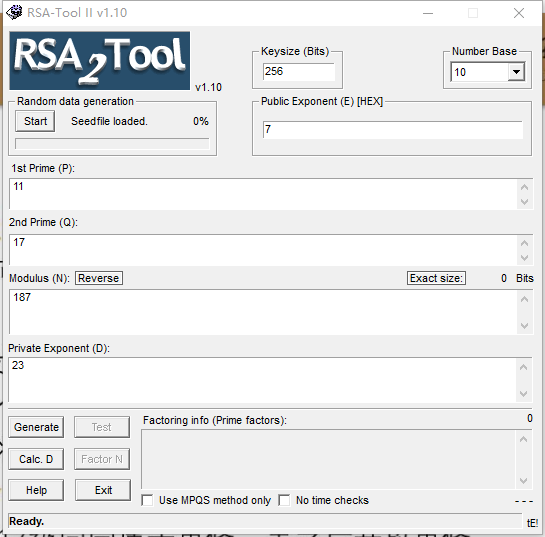
明文内容存放于文件plaintext.txt中。运行程序，对明文进行加密后，哈希值存放于文件plaintext\_MD5.txt中。结果如下。



1. **文件传输：**
2. A、B生成RSA的公钥和私钥：

A：选择p=11，q=17，e=7

得到公钥（e，n）=（7,187），私钥（d，n）=（23,187）



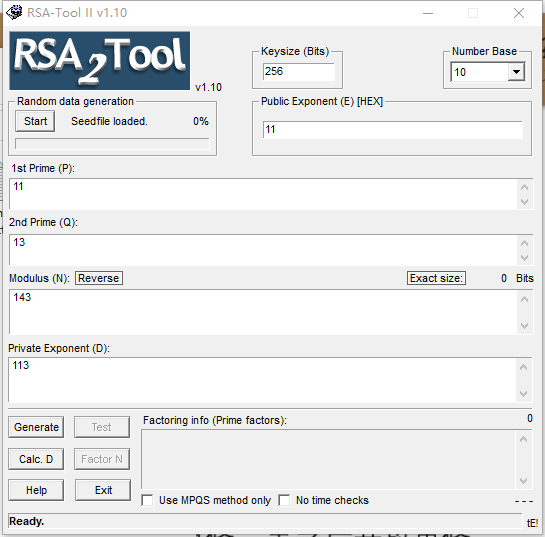


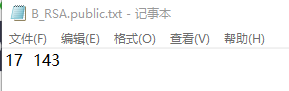


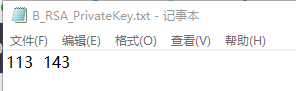
B：选择p=11，q=13，e=17

得到公钥（e，n）=（17，143）

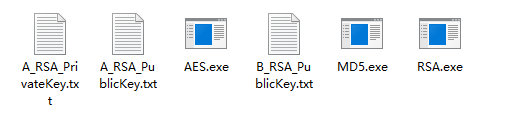
私钥（d，n）=（113，143）







1. **终端A的操作：**
2. 三个加解密程序，以及A的公私钥，和从B得到的B的公钥放在一起，如下：

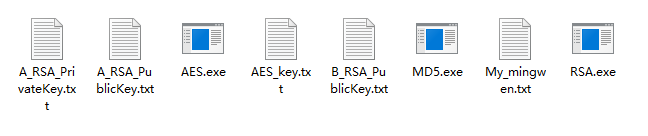


1. ①建立需要加密的文件My\_mingwen.txt：

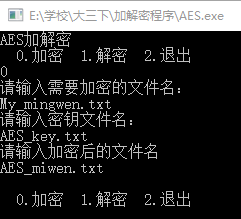


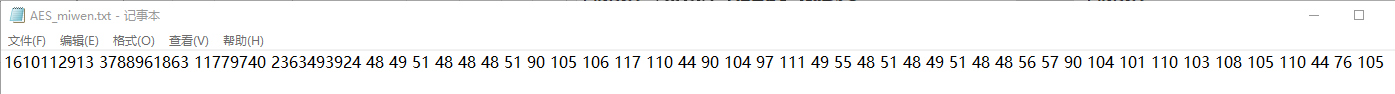
②建立AES加密的密钥文件AES\_key.txt：

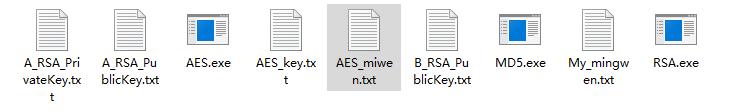




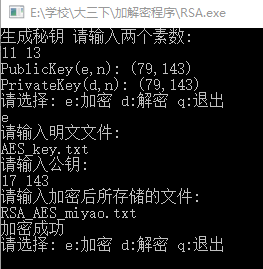
1. 对明文My\_mingwen.txt进行AES加密，生成AES\_miwen.txt。

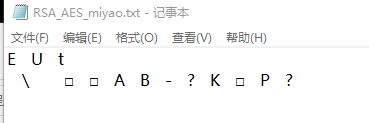


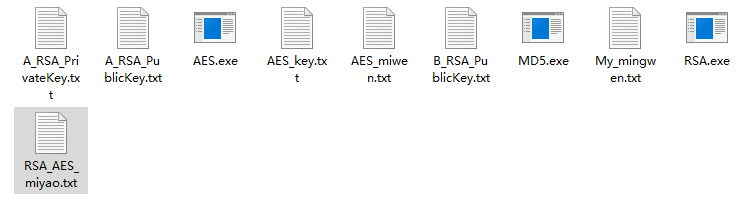




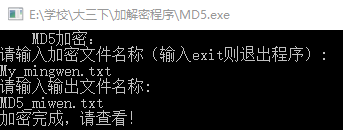
1. 用终端B的公钥对AES使用的密钥进行RSA加密，得到RSA\_AES\_miyao.txt：

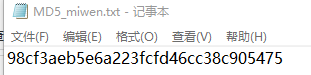


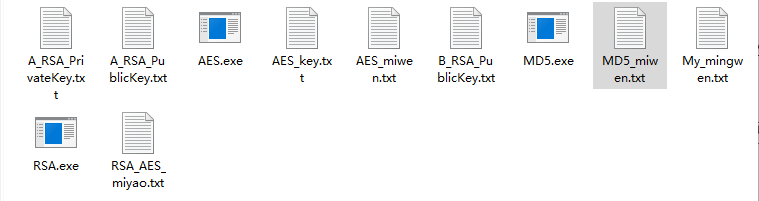




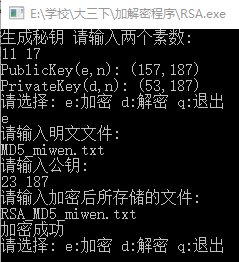
1. 用MD5算法对文件My\_mingwen.txt进行加密生成明文摘要，得到：MD5\_miwen.txt：

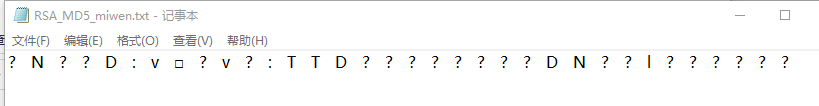


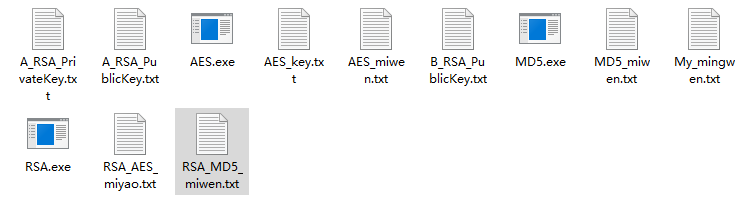




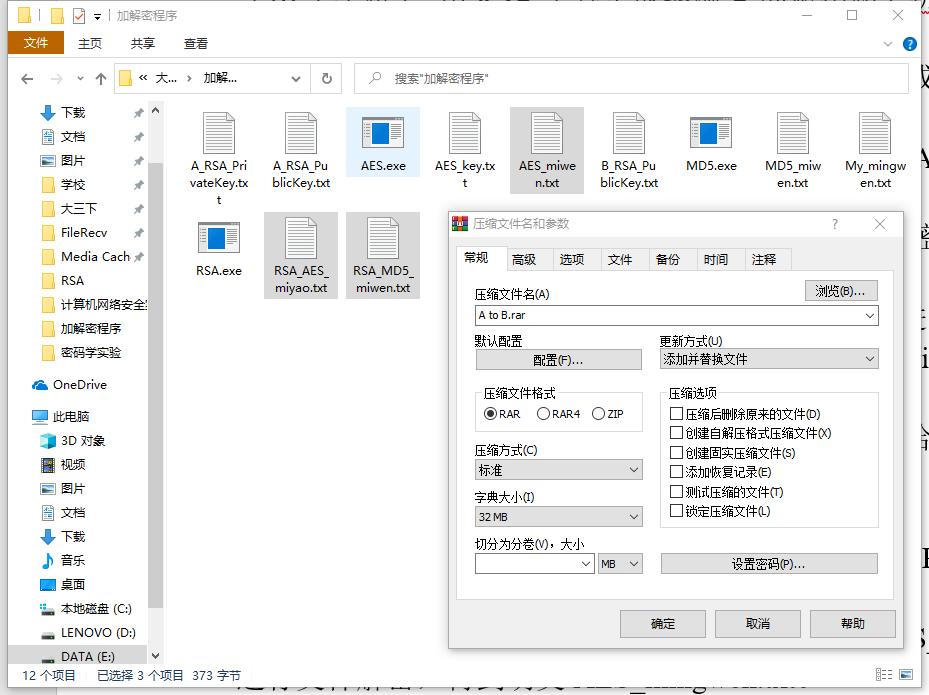
1. 用终端A的私钥对MD5\_miwen.txt文件内容进行加密（签名），得到带有数字签名的加密文件： RSA\_MD5\_miwen.txt



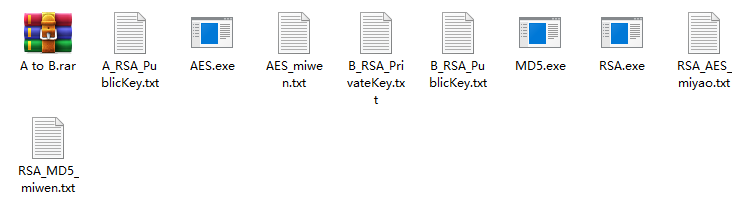




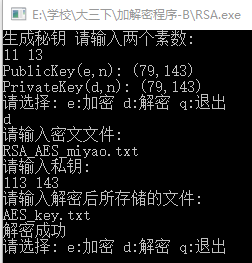
1. 最后把加密生成的文件AES\_miwen.txt、RSA\_AES\_miyao.txt、RSA\_MD5\_miwen.txt 打包发给终端B。

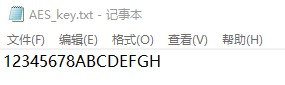


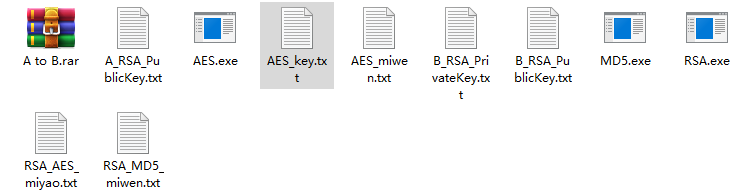
1. **终端B的操作：**
2. 接受A发送过来的压缩包，并取得A的公钥，此时有如下文件和加解密程序：



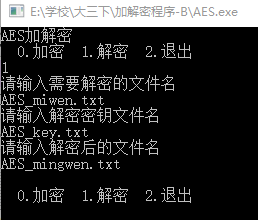
1. 用终端B的私钥对RSA\_AES\_miyao.txt 进行RSA解密。得到:AES\_Key：



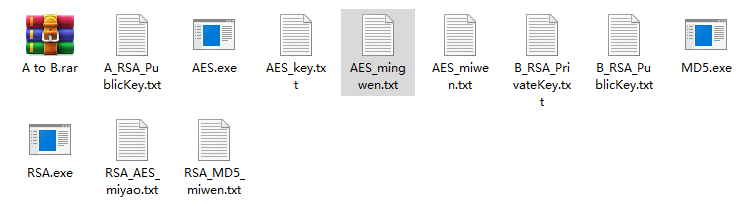




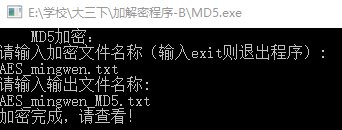
1. 用AES算法（密钥用AES\_key的内容），对AES\_miwen.txt进行文件解密，得到明文AES\_mingwen.txt

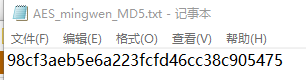


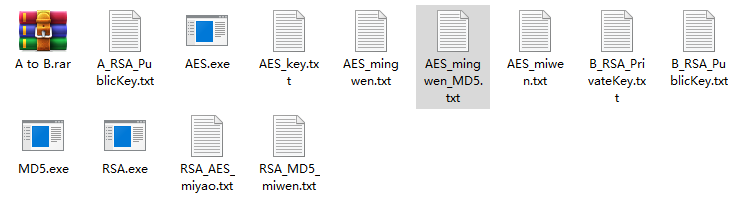




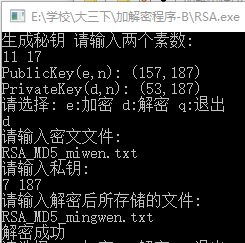
1. 用MD5算法对所得明文AES\_mingwen.txt进行加密生成解密后的明文摘要。得到： AES\_mingwen\_MD5.txt



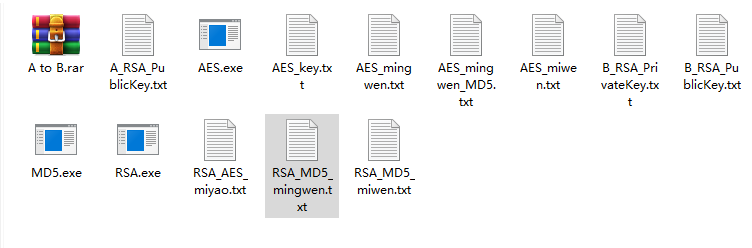




1. RSA算法用终端A 的公钥对RSA\_MD5\_miwen.txt 进行解密，得到: RSA\_MD5\_mingwen.txt







1. 比较RSA\_MD5\_mingwen.txt和AES\_mingwen\_MD5.txt有什么不同。



经比较，二者相同，实验成功。

# 三、实验收获

通过此次实验，加深了我对古典加密算法、对称加密算法和非对称加密算法的理解，尤其是自己动手编程之后，对其中的有了更深入的理解。而文件传输的实验，则将理论与实践结合，通过一系列加解密及签名等操作，完成了文件的安全传输。实验中也遇到了一系列问题，通过网上查阅资料、向老师同学请教，最终解决了相关问题。总的来说，收获很多。