**实验三、MD5哈希算法碰撞及其在司法领域的应用**

**一、实验目的**

理解哈希算法原理以及对验证电子数据完整性的重要性

掌握“非对称密码”加密原理与MD5算法的碰撞构造以及在司法领域对电子证据效力的影响

**二、实验内容**

通过GPG4Win实现数字签名

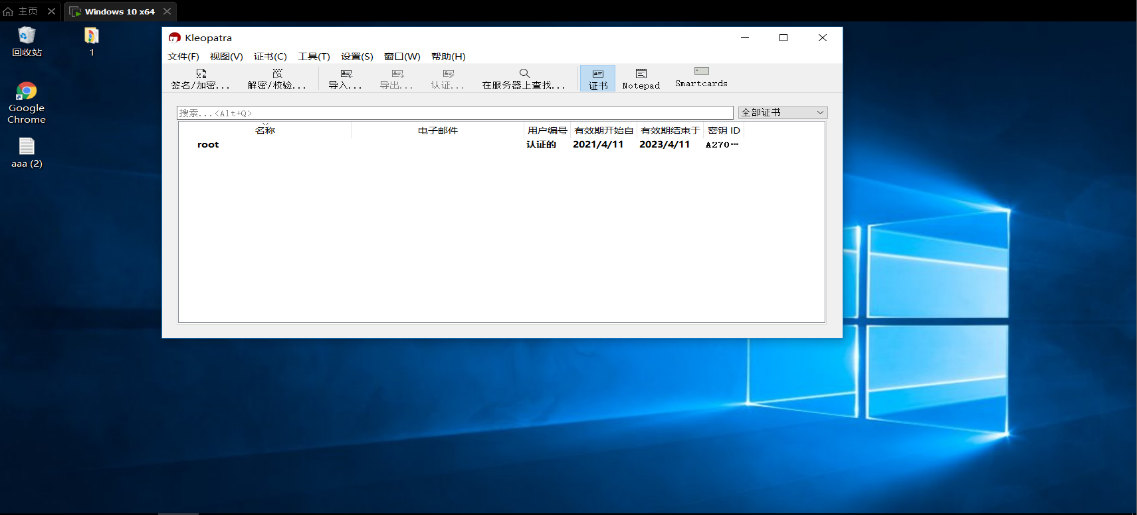
对office文档进行MD5碰撞构造实验

对可执行程序进行MD5碰撞构造实验

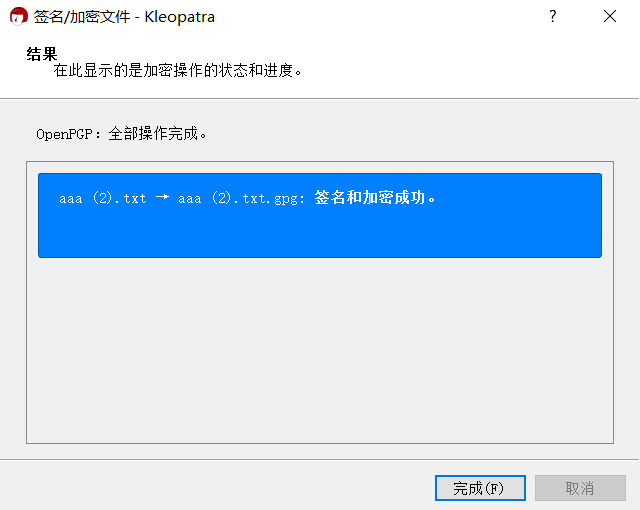
**三、实验步骤**

**1.通过GPG4Win实现数字签名**

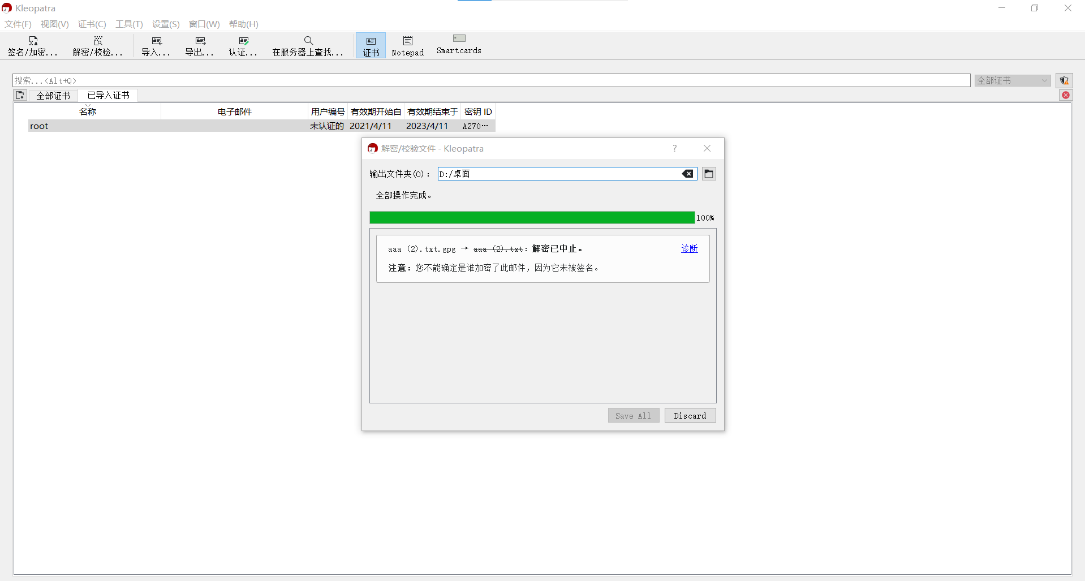
(1).创建密钥对并发送公钥



(2).使用公钥加密存有python程序代码的.txt文档

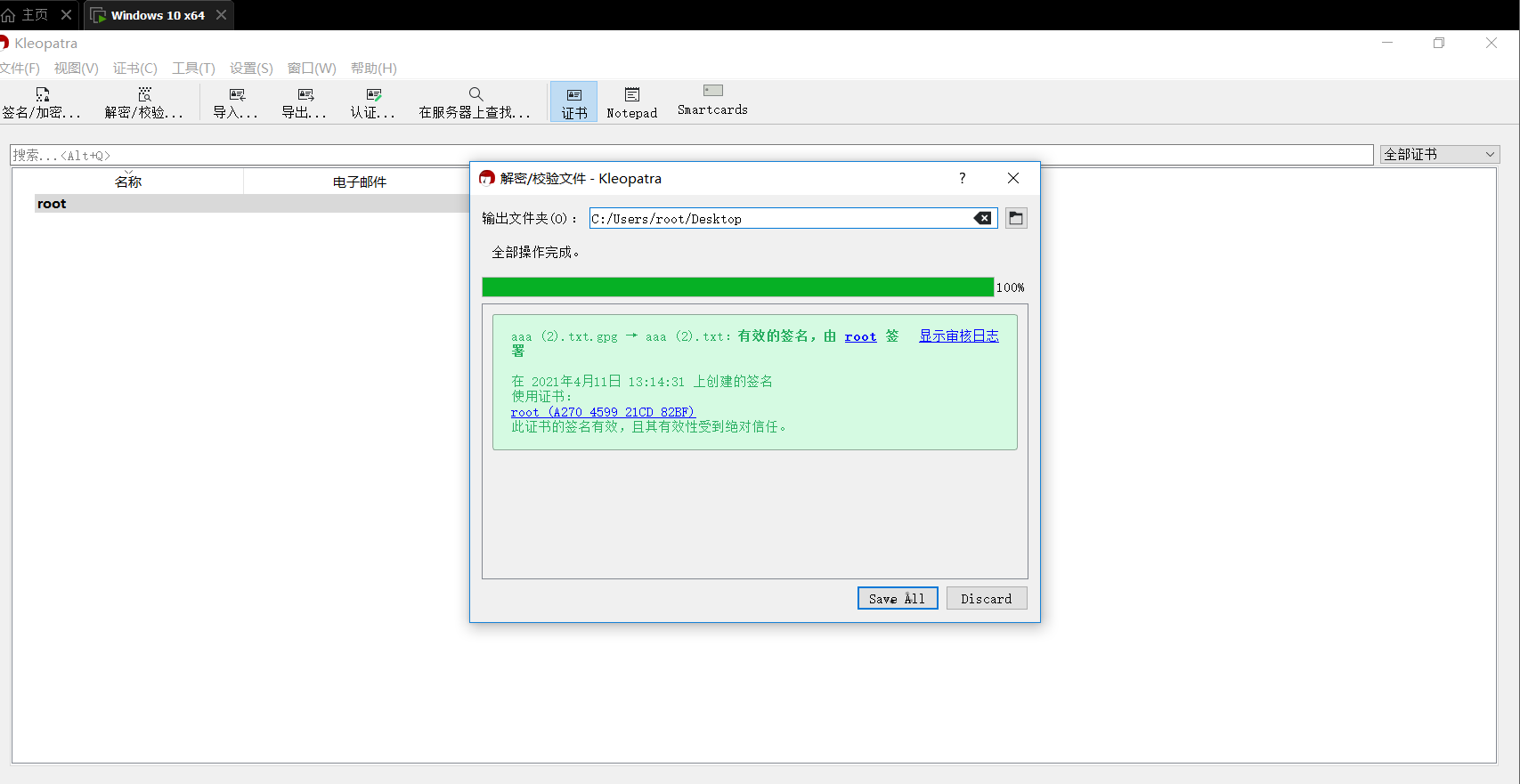


(3).使用不拥有私钥的用户尝试解密



结果:解密失败,无法查看内容

(4).使用拥有私钥用户解密



结果:解密成功,内容完整,准确



**2. 对office文档进行MD5碰撞构造实验**

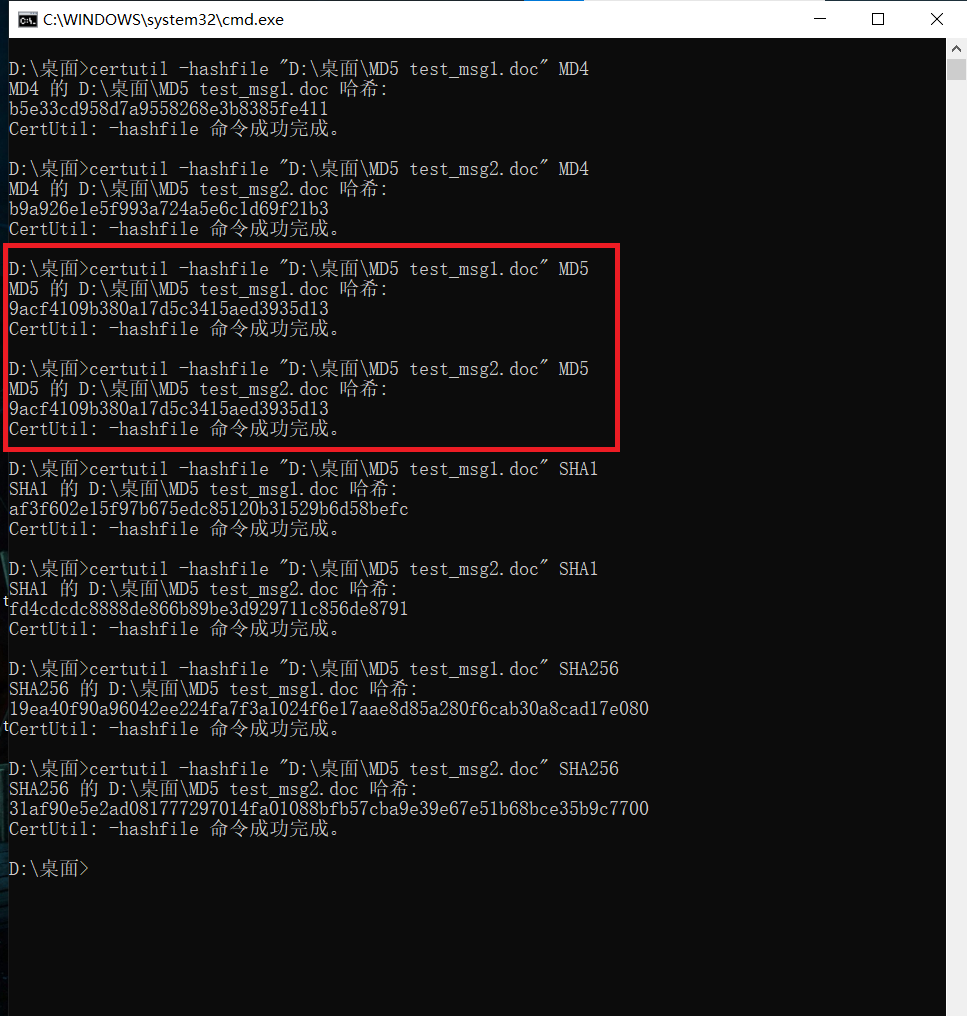
(1).使用fastcoll 对已存在的MD5 test.doc文档进行MD5碰撞构造实验

产生MD5 test\_msg1.doc , MD5 test\_msg2.doc 两文档





(2).查看两文档各自MD5 及SHA1 (仅对MD5进行了碰撞)



两文档MD5相同,而SHA1不同,不是同一文件

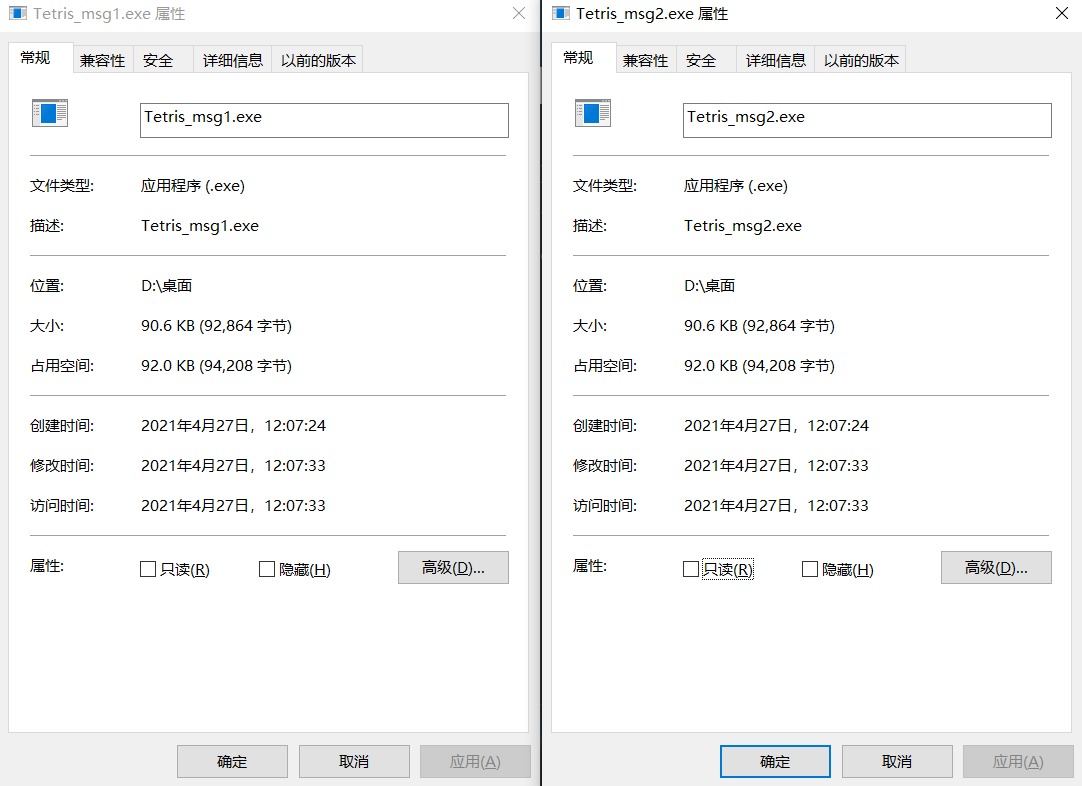
对office文档进行MD5碰撞构造成功

**3. 对可执行程序进行MD5碰撞构造实验**

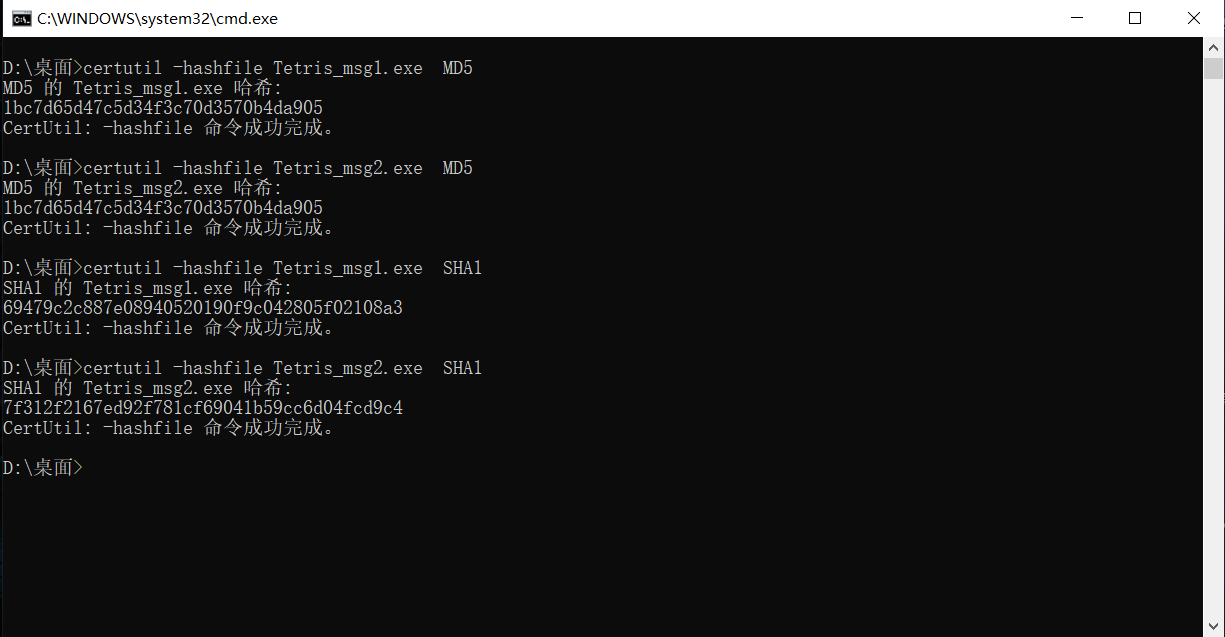
(1).使用fastcoll 对已存在Tetris.exe文件的进行MD5碰撞构造实验

产生Tetris\_msg1.exe, Tetris\_msg1.exe 两文件





(2).查看两文件MD5 及SHA1 (仅对MD5进行了碰撞)



两文件MD5相同而SHA1 不同,不是同一.exe文件

对可执行程序进行MD5碰撞构造成功

**四、实验结果**

1.成功使用GPG4Win产生的公钥加密,并验证仅有私钥可解密,实现数字签名

2.成功对office文档进行MD5碰撞构造实验,产生MD5 相同而SHA1不同的两doc文档,二者非同一文档(仅对MD5进行了碰撞)

3.成功对可执行程序进行MD5碰撞构造实验, 产生MD5 相同而SHA1不同的两.exe可执行程序,二者非同一可执行程序(仅对MD5进行了碰撞)

**五、写出本次实验的实验心得**

1.了解了哈希算法及相关知识

哈希算法: 将任意长度的二进制值串映射为固定长度的二进制值串。

哈希值: 通过原始数据映射之后得到的二进制值串。

构成哈希算法的条件：

从哈希值不能反向推导出原始数据（所以哈希算法也叫单向哈希算法）

对输入数据非常敏感，即使原始数据仅修改了1 Bit，最后得到的哈希值也大不相同；

散列冲突的概率要很小，对于不同的原始数据，哈希值相同的概率非常小；

哈希算法的执行效率要尽量高效，针对较长的文本，也能快速地计算出哈希值。

2. 了解了哈希算法对验证电子数据完整性的重要性

“完整性校验”即检查文件是否完整,出现文件不完整的情况包括感染病毒,植入木马/后门/人为篡改,传输故障等。

哈希算法具有不可逆性,确定性,无法通过散列值逆推原始数据,当两份原始数据计算出来的散列值不同时,这两段数据肯定是不同的,以此可用于检验电子数据的完整性。

3. “非对称密码”加密原理

非对称加密算法是一种密钥的保密方法。需要两个密钥：共有密匙和私有密钥。公钥与私钥是一对，用公钥对数据进行加密，只有用对应的私钥才能解密。加密信息交换过程：A生成一对密钥并将公钥公开，B使用A的公钥对信息加密后发送给A；A用自己私钥对加密后的信息进行解密。A回复B时，使用B的公钥进行加密, B使用自己的私钥进行解密。

A可以使用自己的私钥对信息进行签名后再发送给B；B再用甲方的公钥对A发送回来的信息进行验签。A只能用其私钥解密由其公钥加密后的任何信息。

4. MD5算法的碰撞构造在司法领域对电子证据效力造成了影响

认定电子证据效力应综合考量合法性、真实性与证明力, 电子证据的合法性主要包括证据形式的合法性及取证手段的合法性两大方面。 MD5算法的碰撞构造对大大降低了与MD5相关电子证据效力的合法性、真实性与证明力,也影响到了其他方面电子证据在司法领域的效力。 5. 在计算机取证过程中需要保证数据的完整性, 这要求在学习过程中需要扎实基础,有大胆的思维和质疑精神。