**实 验 报 告**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |
| --- | --- |
| **课程名称：** | **信息系统安全** |
| **学生姓名：** |  |
| **学生学号：** |  |
| **学生专业：** | **软件工程** |
| **开课学期：** | **2016-2017 第二学期** |

**XXXX单位**

**2016年5月**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **地 点：** | B7 楼 | 133 房； | **实验台号：** |  |
| **实验日期与时间：** | 2017年3月21号 | | **评 分：** |  |
| **预习检查纪录：** | 良好 | | **实验教师：** | 陈春华 |

# 实验过程与结果

# 加密邮件

# 实验结论与思考题

1. **加密邮件与签名邮件有什么区别？**

加密邮件 = 内容加密过的邮件 .

签名邮件 = 邮件 + 数字签名

加密为邮件提供了不可读性, 保证了内容不会被除目标接受者之外的人读取.

数字签名保证了信息的完整性,以及对发送者的身份认证,防止交易中的抵赖发生

2**、随着中华人民共和国电子签名法的颁布实施，你认为签名电子邮件具有法律效力吗？**

反向思考一下, 如果没有法律效力, 那电子签名法的实施有什么用? 法律效力肯定是有.

电子签名法中,签名证书的签发机构, 签名的拥有者,以及签名的使用者环节中的一部分, 按照正规途径办理及使用的签名电子邮件,具有法律效力.

还有某律师的看法: <https://zhuanlan.zhihu.com/p/21871436>

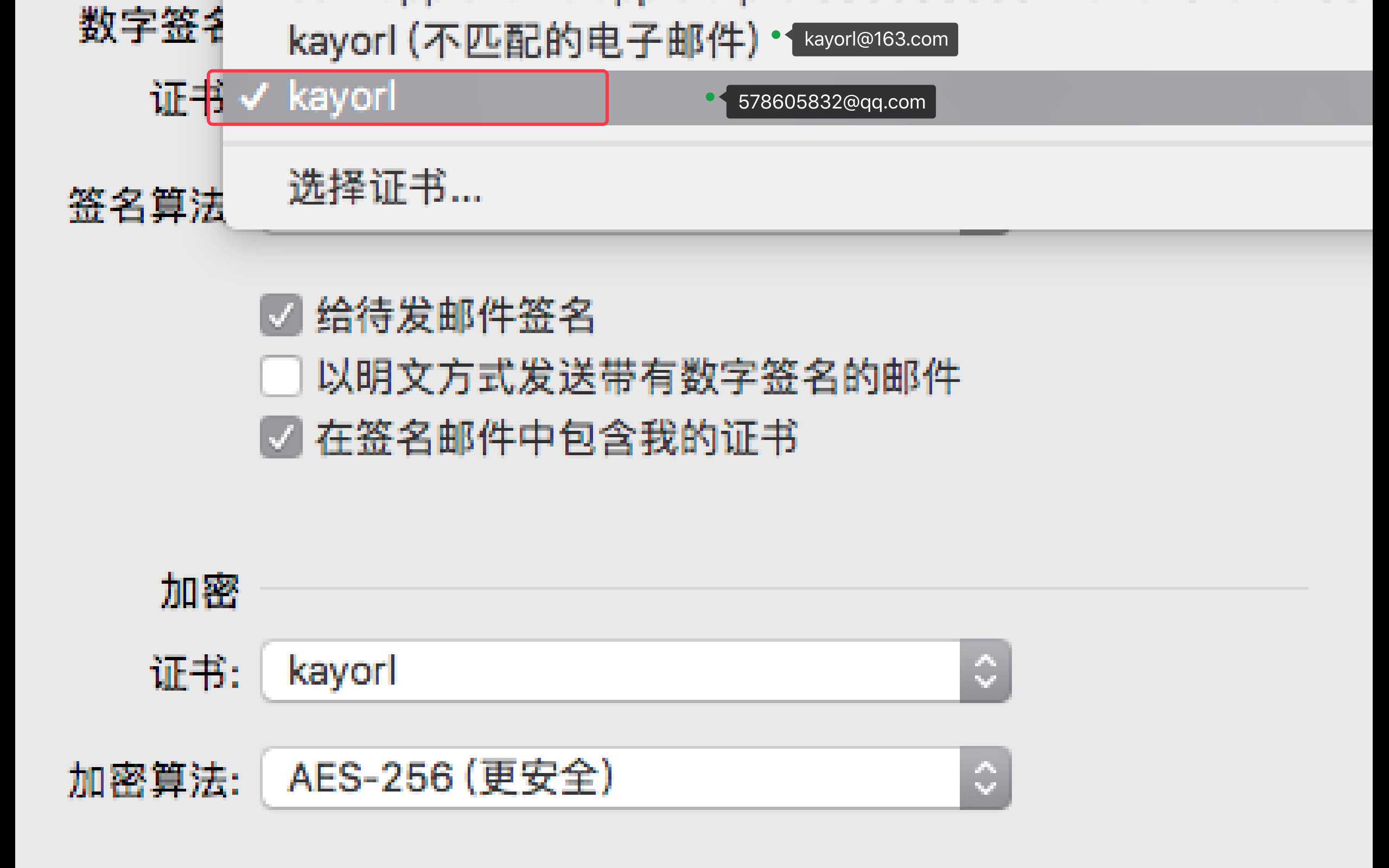
**3、为什么发送加密邮件需要对方的数字证书？其加密原理是什么？真的是使用接收方的公钥直接对邮件的内容进行加密吗？**

a. 加密证书中包含有对方的的公钥, 利用对方的公钥可以加密

b. 加密原理: 不对称加密系统中拥有私钥的乙方才能解开用公钥加密过的邮件

c. 不, 如果发送方选择发送数字签名, 加密内容会将发送方的数字签名随同邮件内容一起加密

**4、能用他人的证书发送签名邮件吗？为什么？**



事实证明不可以, 因为证书中包含了邮箱信息,邮箱信息如果不匹配的话，不允许选择及发送

