**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：** | **林玮** |
| **学生学号：** | **201430620138** |
| **学生专业：** | **软件工程** |
| **开课学期：** | **2016-2017 第二学期** |

**软件学院**

**2016年5月**

**实验3-数字证书及其应用**

**（安全协议）**

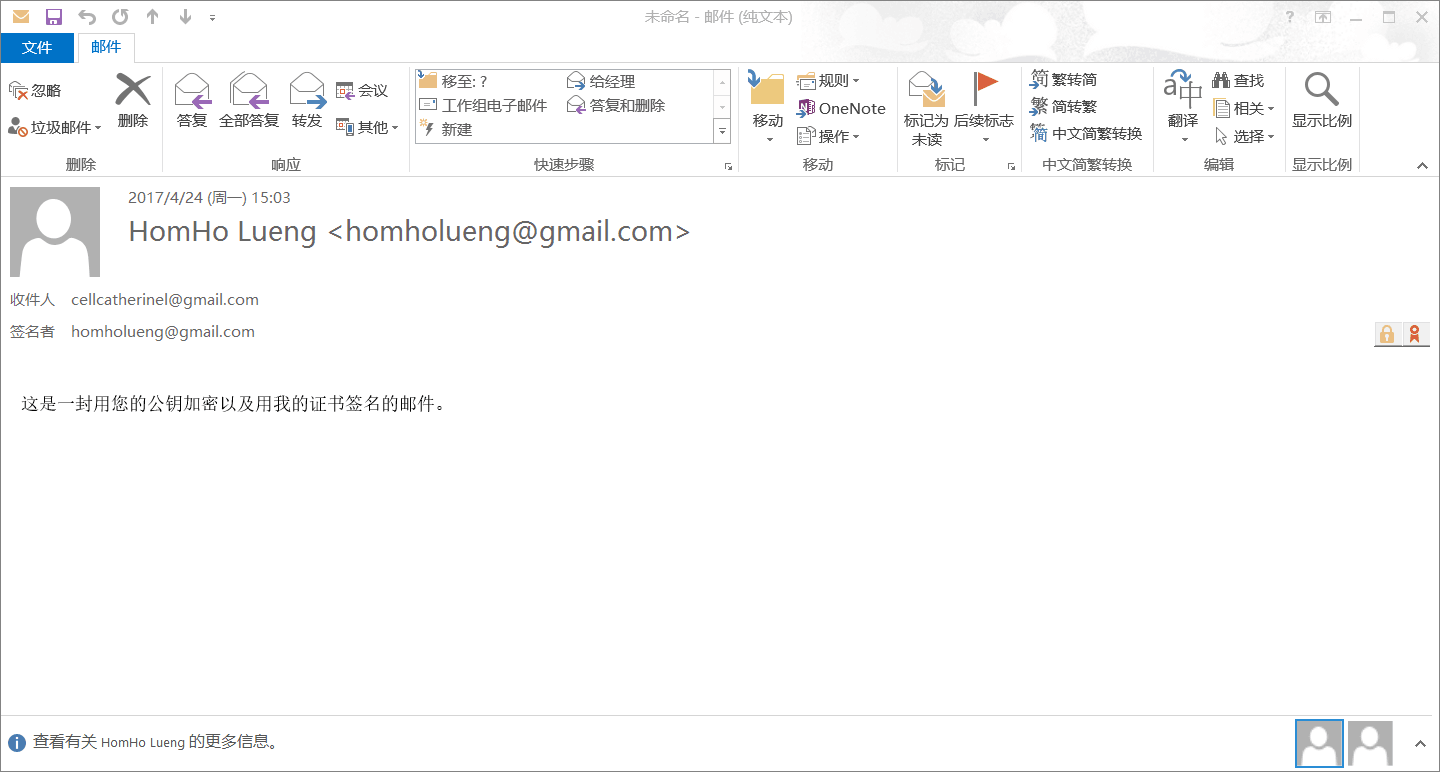
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **地 点：** | B7 楼 | 133 房； | **实验台号：** |  |
| **实验日期与时间：** | 2017年3月21号 | | **评 分：** |  |
| **预习检查纪录：** | 良好 | | **实验教师：** | 陈春华 |

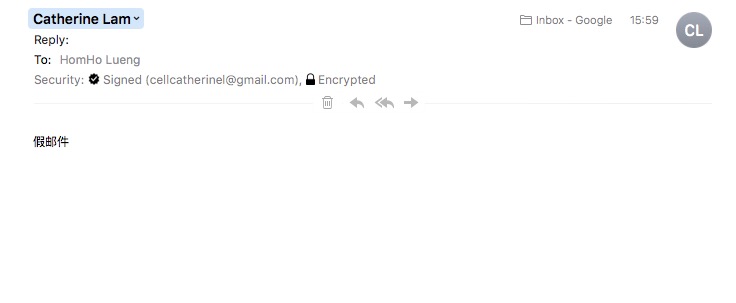
# 实验过程与结果

加密邮件的发送：

步骤：

1. 从<https://www.comodo.com/> 获取数字证书
2. 在Oulook的信任中心中添加证书
3. 获取对方的证书，发送邮件时选中加密和签署选项，就会用对方的公钥加密邮件，并用自己的证书对邮件进行数字签名
4. 接收邮件，截图如下



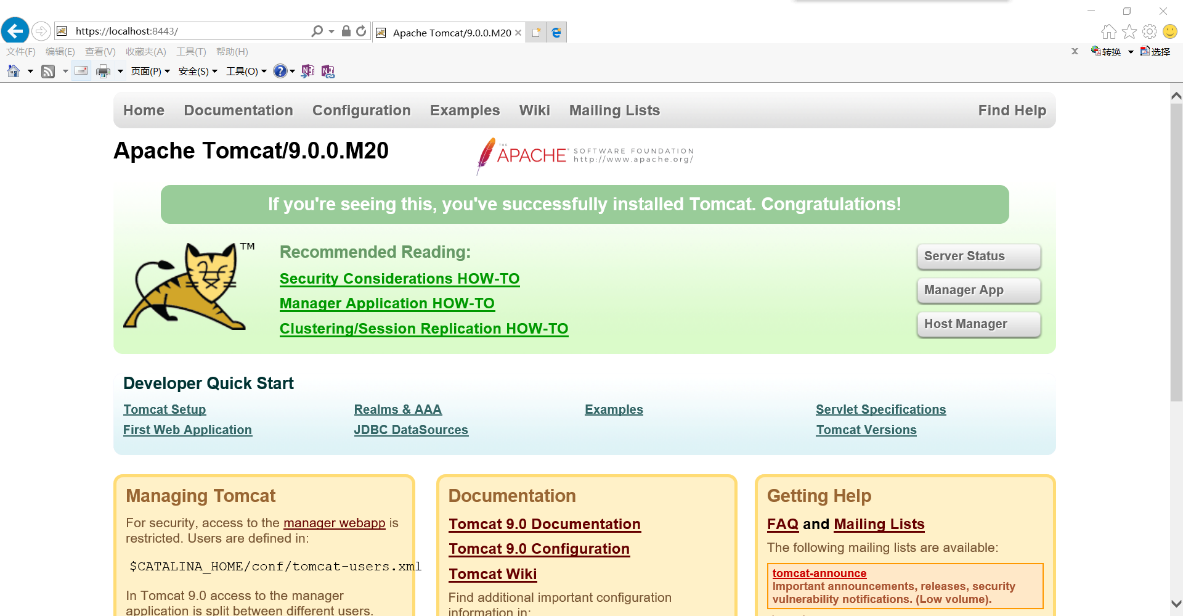


给tomcat中web应用配置使用SSL协议：

步骤：

1. 使用EasyRSA创建新的PKI和CA
2. 签发客户端证书和服务器证书
3. 让服务器信任客户端证书
4. 让客户端信任服务器证书
5. 打开<https://localhost:8443>

结果截图如下：



# 实验结论与思考题

1. 加密是为了防止信息被接收方以外的人获取

签名是为了确认该信息是由发送方发出，而不是由其他人发出

1. 根据中华人民共和国电子签名法规定，电子签名具有法律效力，民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。 当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。
2. 因为邮件加密需要用到接收方数字证书中的公钥。当发件人对邮件进行加密时，使用接收人的数字证书中的公钥对邮件进行加密。邮件的接收方接收到该邮件后，使用自己的私钥对邮件进行解密，可以得到邮件的明文。因为使用公钥加密的数据，只有对应的私钥才可以解密，而对一封加密邮件来说，只有接收人才具有对应的私钥，也就是只有接收人才可以对邮件解密得到邮件的明文。使用接收方的公钥直接对邮件的内容进行加密。
3. 不能，证书与邮箱地址绑定。