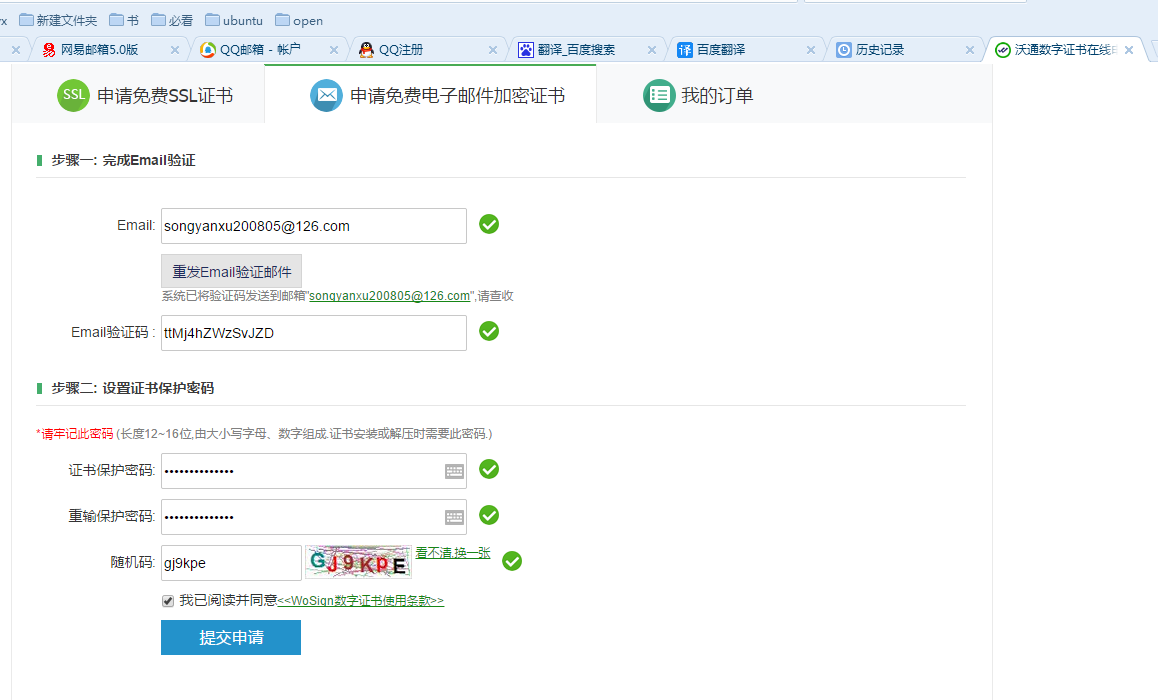
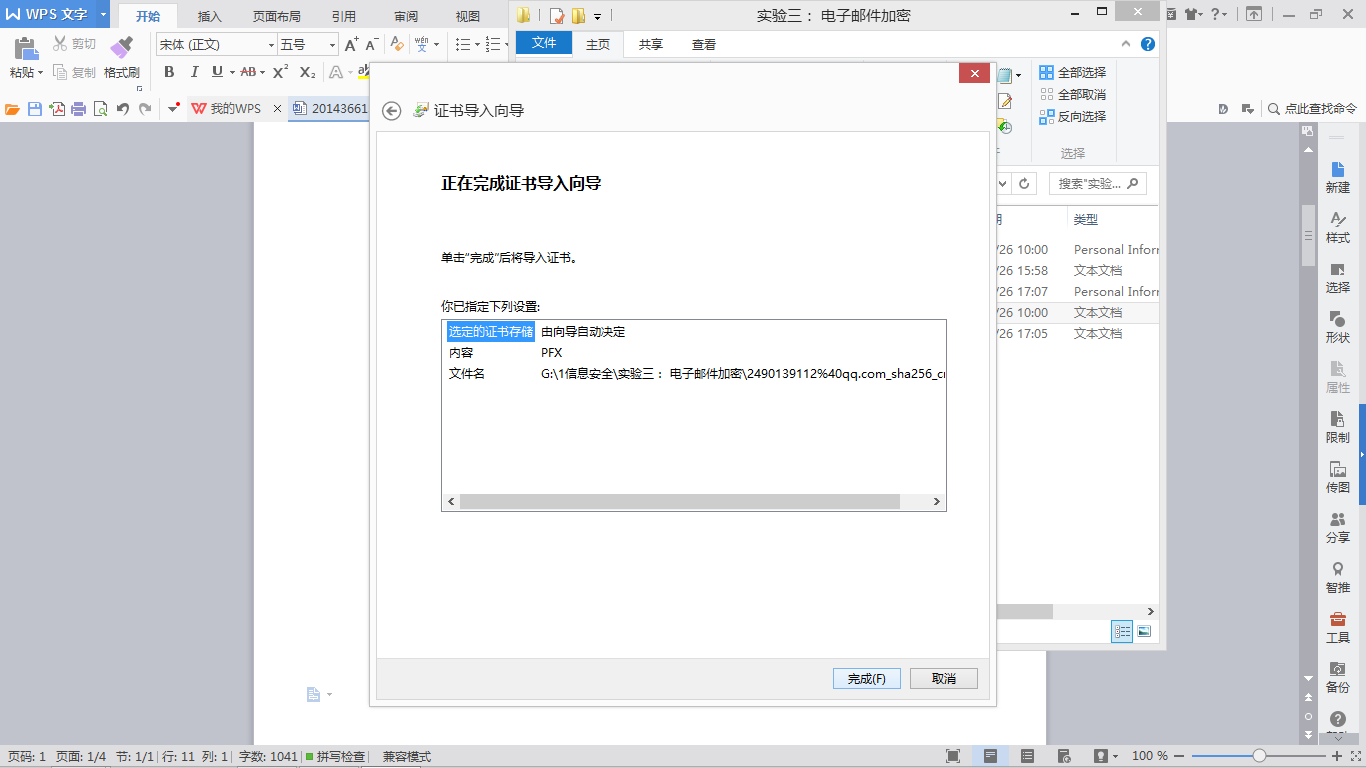
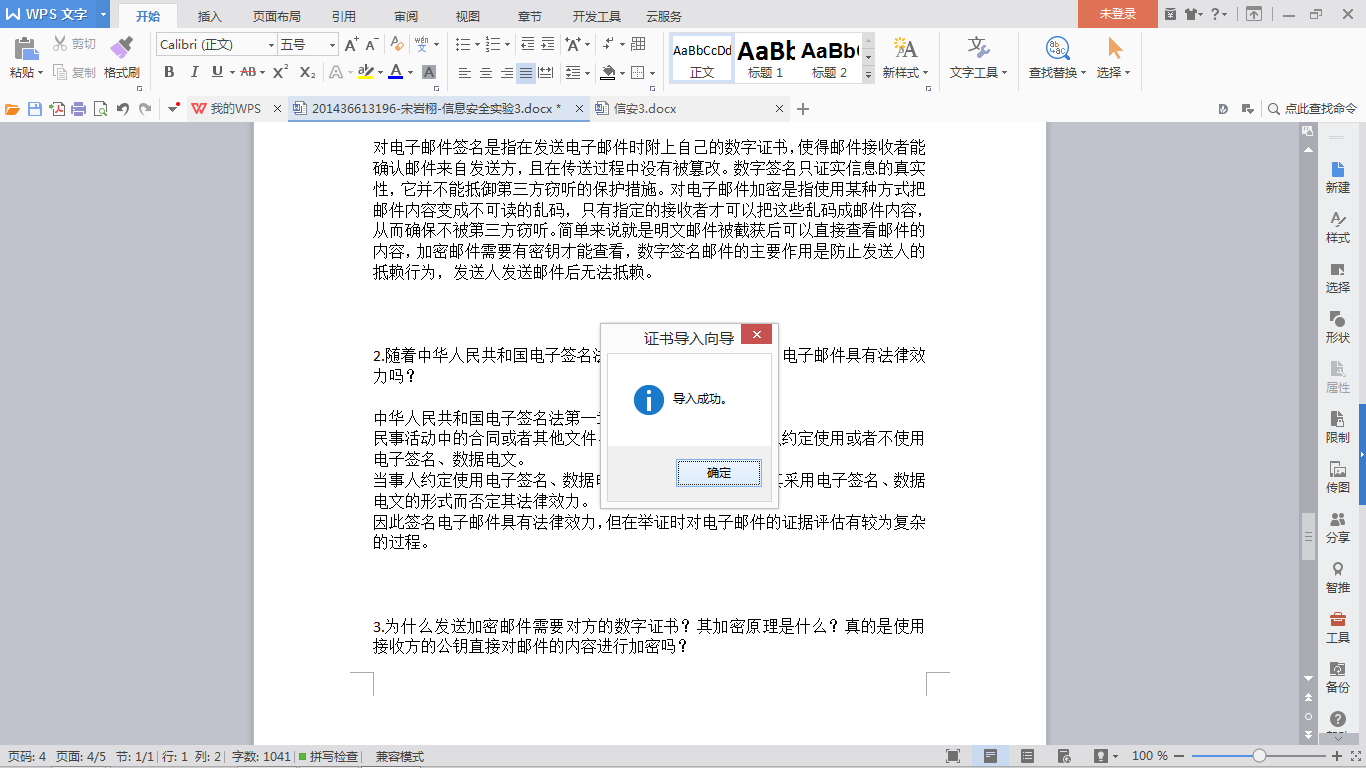
由于中国认证网的免费证书申请不到，所以使用了沃通的数字证书，

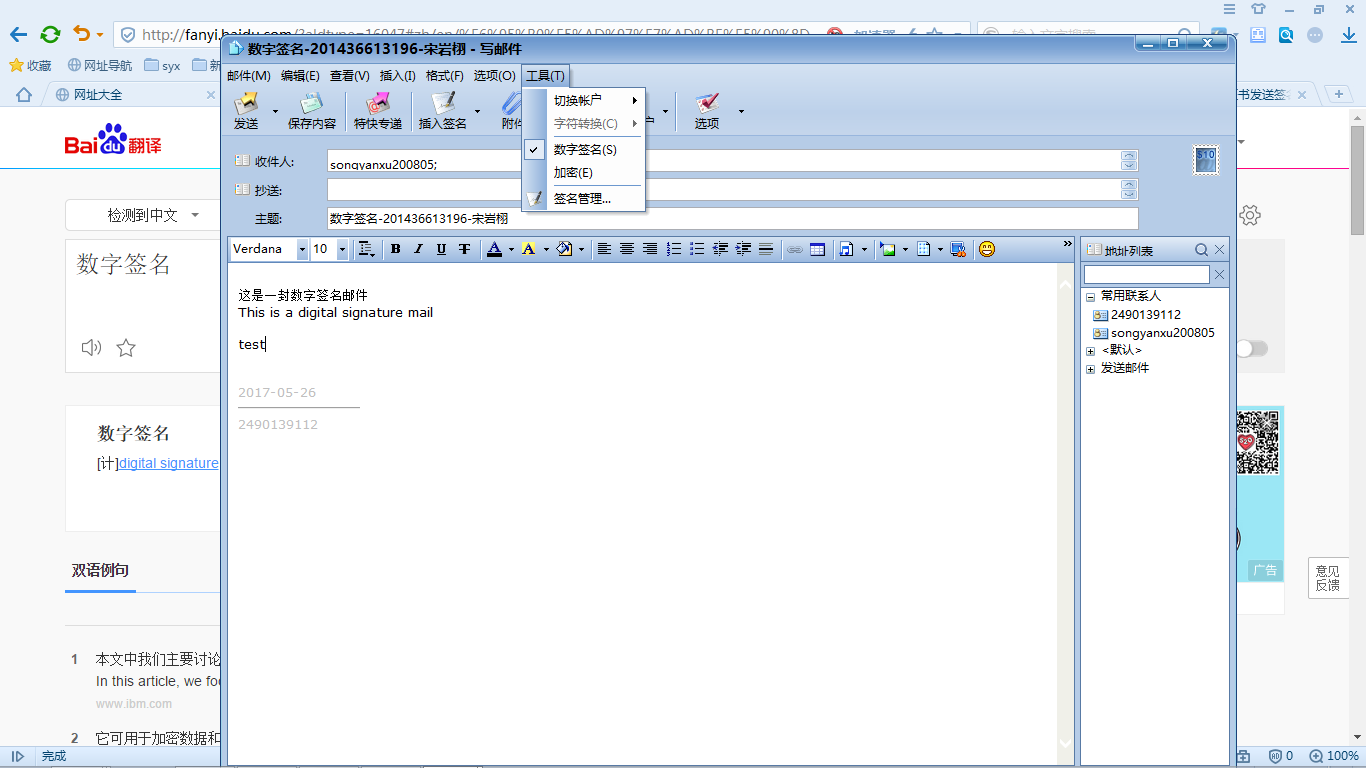


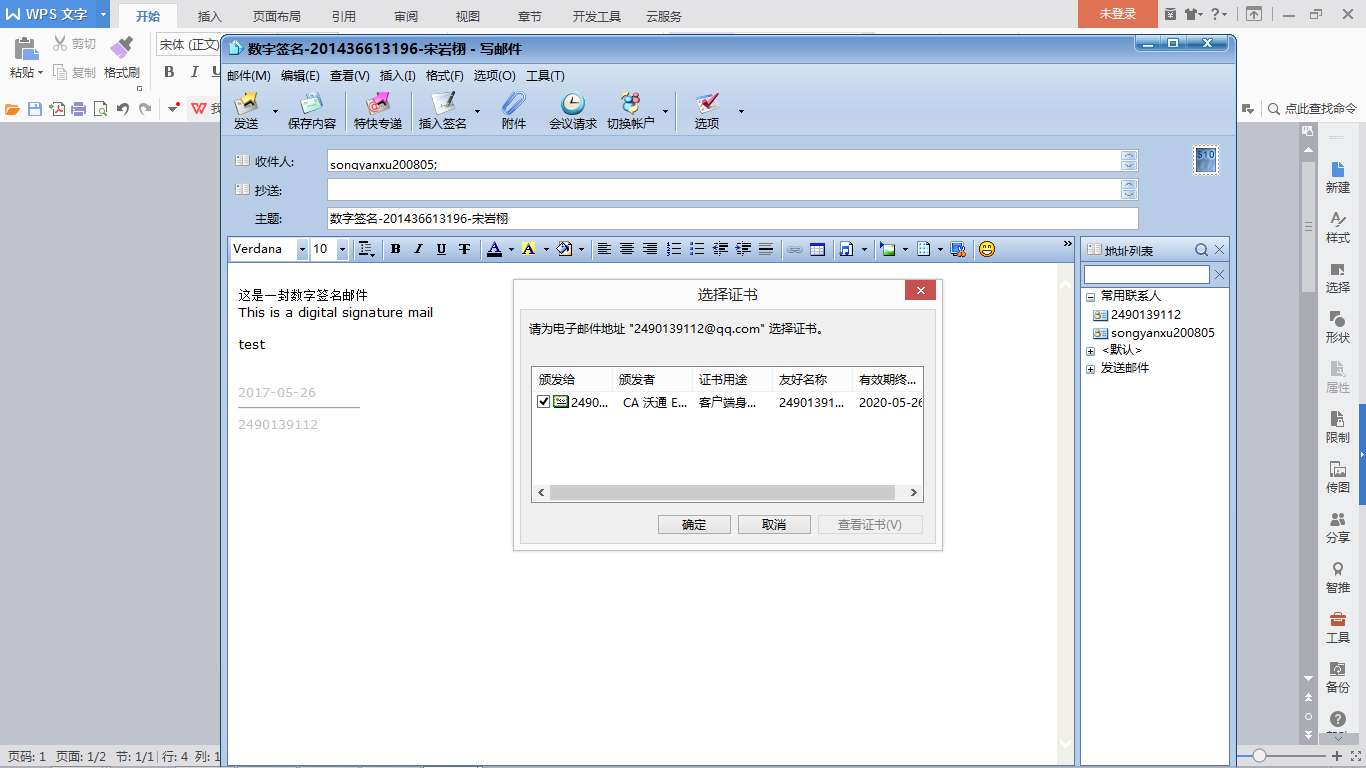
然后导入证书：



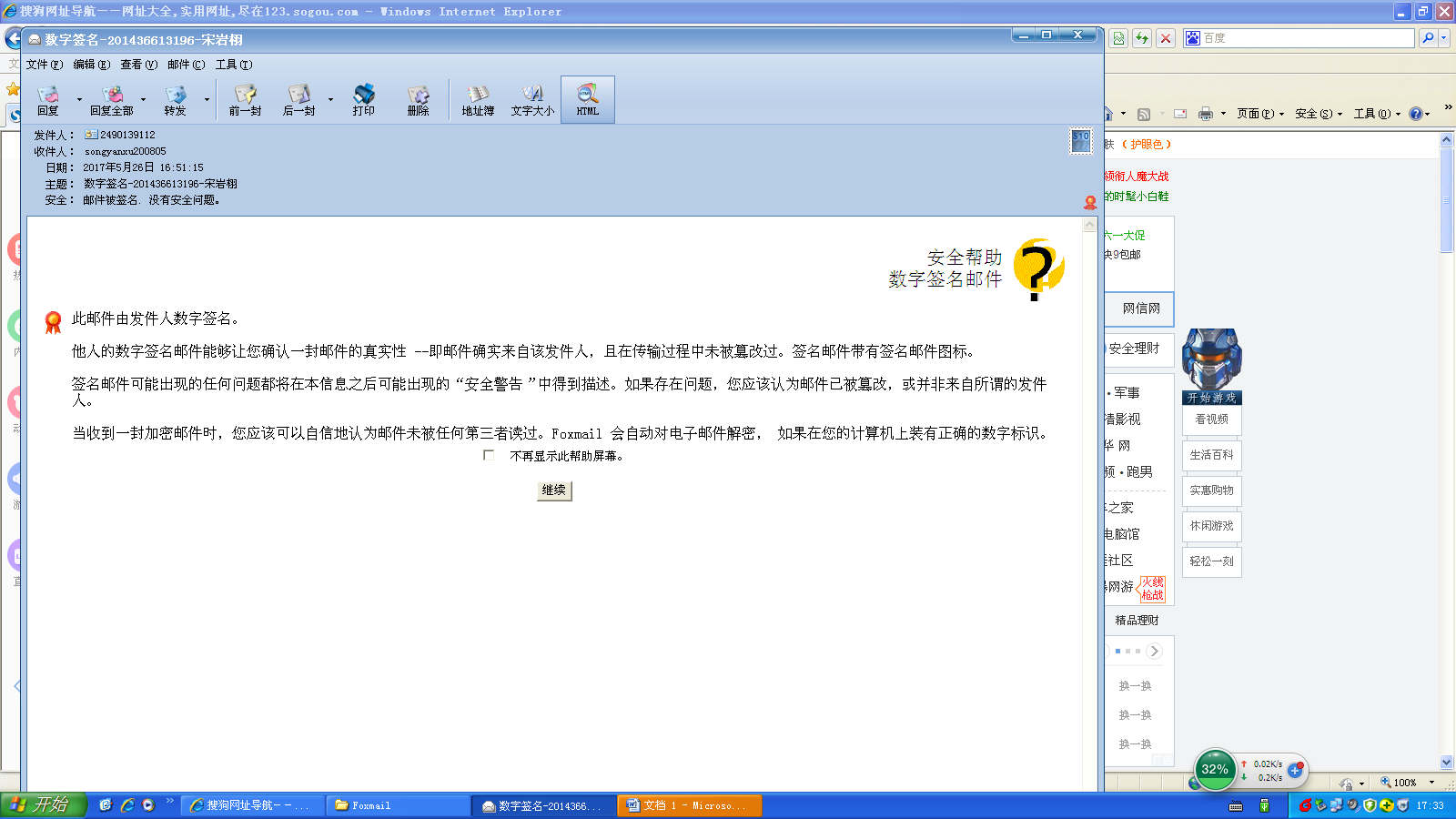


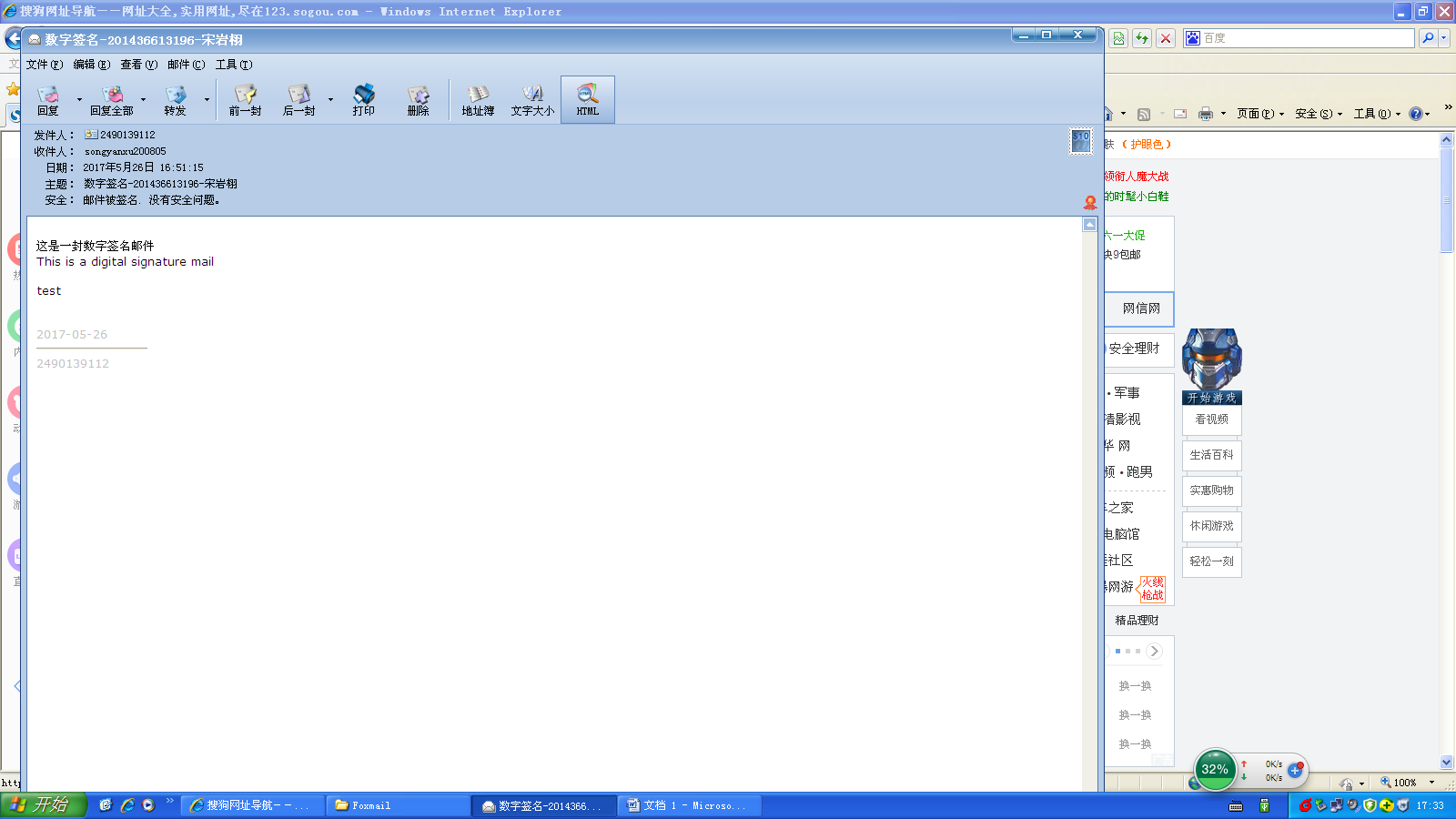
向b发送带数字签名的邮件：



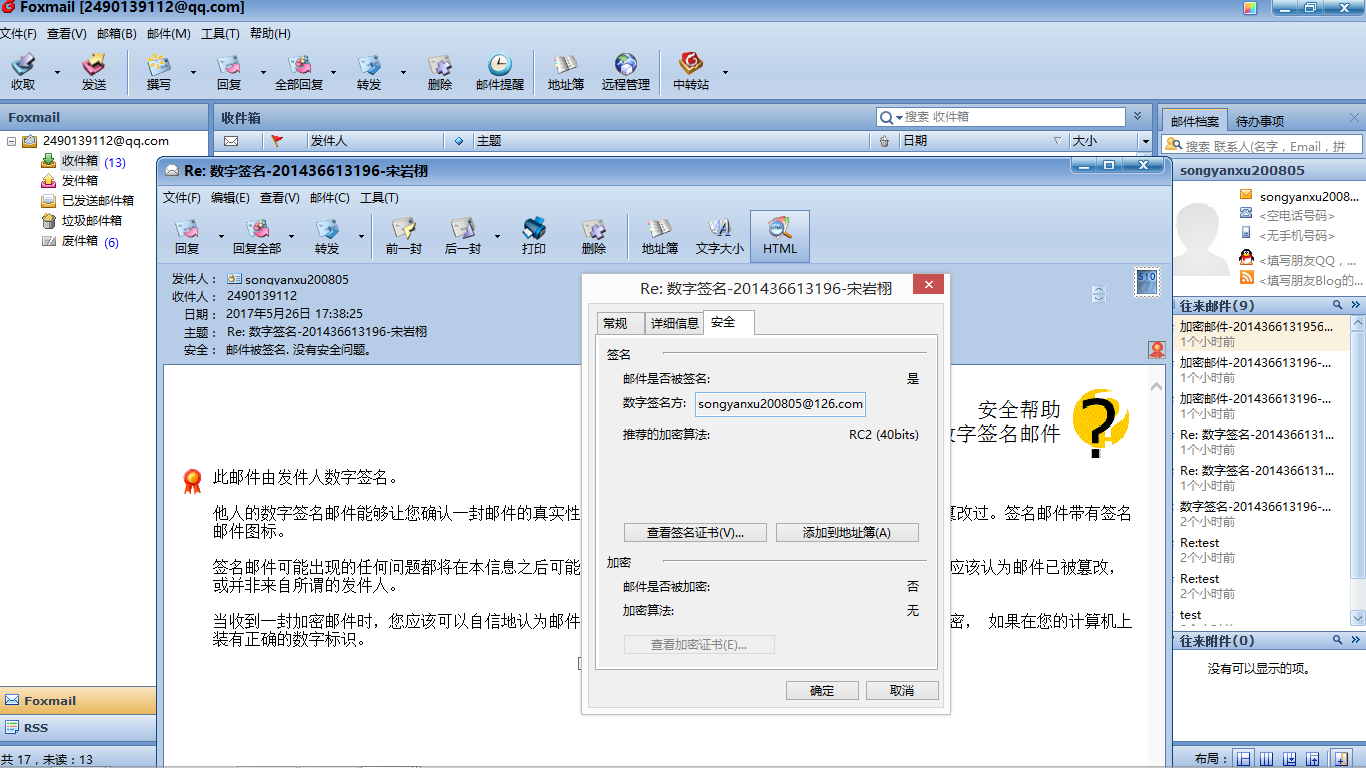


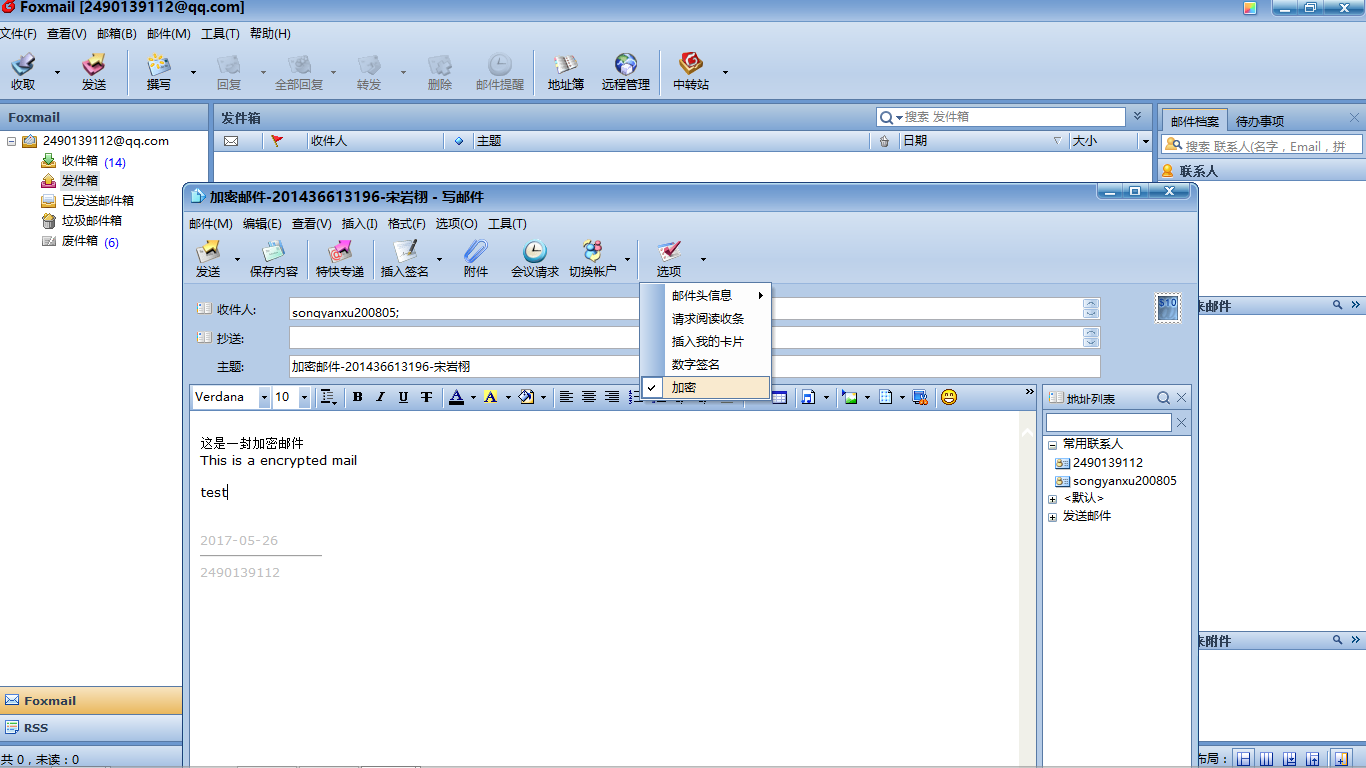
b收到来自a的邮件：

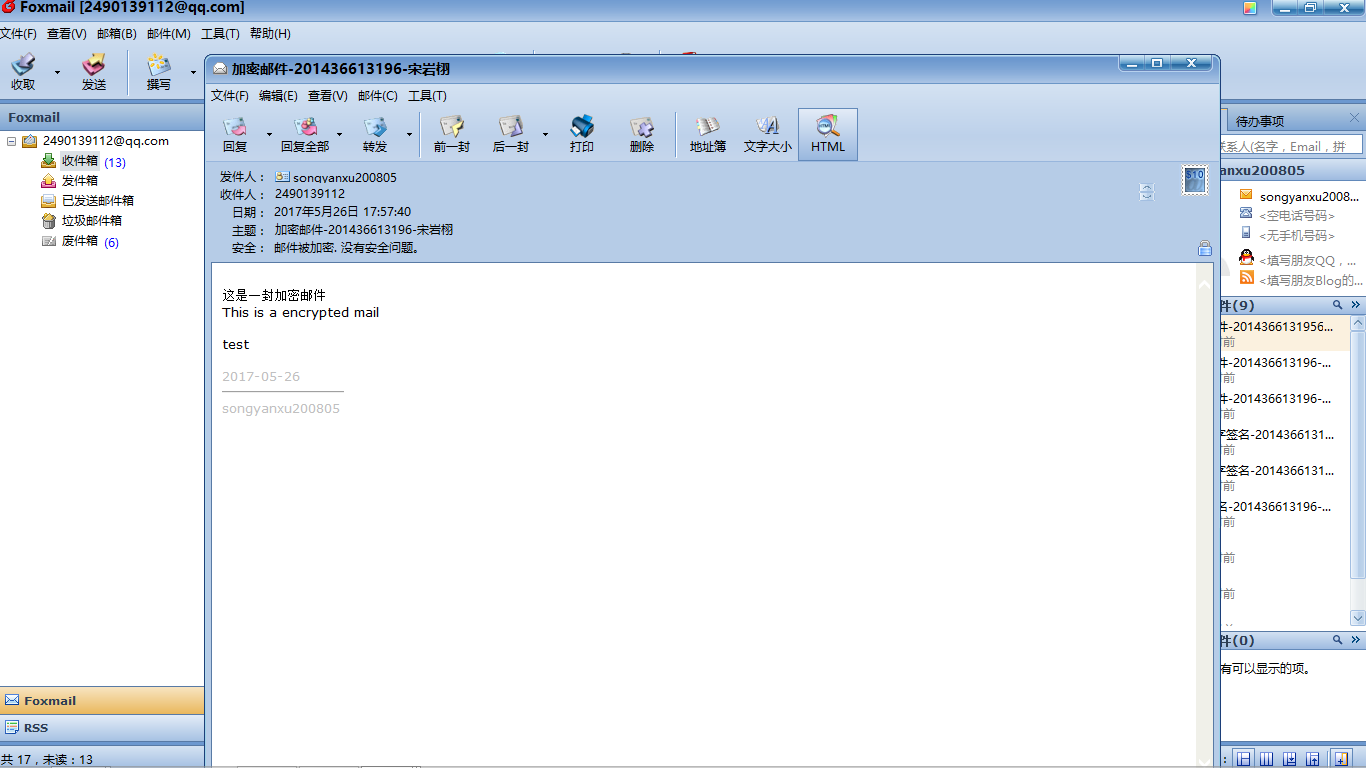




a收到来自b的带数字签名的回复后将b的签名添加到通讯簿中，这样就可以向b发送加密邮件了







b收到来自a的加密邮件



1.加密邮件和签名邮件有什么区别？

对电子邮件签名是指在发送电子邮件时附上自己的数字证书，使得邮件接收者能确认邮件来自发送方，且在传送过程中没有被篡改。数字签名只证实信息的真实性，它并不能抵御第三方窃听的保护措施。对电子邮件加密是指使用某种方式把邮件内容变成不可读的乱码，只有指定的接收者才可以把这些乱码成邮件内容，从而确保不被第三方窃听。简单来说就是明文邮件被截获后可以直接查看邮件的内容，加密邮件需要有密钥才能查看，数字签名邮件的主要作用是防止发送人的抵赖行为，发送人发送邮件后无法抵赖。

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？

中华人民共和国电子签名法第一章第三条：

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。

因此签名电子邮件具有法律效力，但在举证时对电子邮件的证据评估有较为复杂的过程。

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？

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。

数字证书必须具有唯一性和可靠性。为了达到这一目的，需要采用很多技术来实现。通常，数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所有的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地。

1. 能用他人的证书发送签名邮件吗？为什么？

能，因为要发送加密电子邮件，你需要有收件人的数字证书。获得收件人数字证书的方法可以是让对方给你发送带有其数字签名的邮件。有了对方的数字证书，你就可以向对方发送加密邮件了。发送加密邮件，也可以同时使用发件人的数字签名。