

[密码学商城开发技术文档]

(密码学原理与实践-实践部分)

[项目名称：支付安全的密码学电子商城]

[姓名： 严幸]

[学号： 1190200910]

目录

1. 背景与意义	1
1.1 项目开发意义	1
1.2 国内外现状及技术综述	1
2. 需求分析	3
2.1 总体需求	3
2.2 功能需求	3
2.3 性能需求	3
3. 概要设计	4
4. 详细设计	5
5. 实现与测试	9
6. 结束语	20
参考文献	21

1. 背景与意义

1.1 项目开发意义

21 世纪以来, 在因特网开放的网络环境下, 基于客户端/服务端应用方式, 买卖双方不谋面地进行各种商贸活动, 电子商务得到迅猛发展^[1]。人们的生活越来越离不开电子商城, 与之伴随而来的还有电子银行系统, 也得到了迅速发展^[2]。然而, 电子商城也给犯罪分子提供了可趁之机^[3]。如何在电子商务的支付过程中保护好用户的隐私与财产安全是一个必须解决的问题。如今的电子商城大多采用电商-网银-CA 三方结合的策略来保证通信安全, 甚至直接采用 https 协议来保证 Web 服务的加密通信, 可以有效的保证通信双发消息的机密性、不可篡改性、不可抵赖性。

在本项目当中, 完成了一个电子商城的设计, 可以保证用户在注册、登录、购物操作、支付操作中, 与电商和银行的服务器进行报文交换时达到机密性、不可篡改性、不可抵赖性。本项目完全基于 http, 这是一个不可靠的信道, 我们通过端到端的加密, 在上层应用中实现了消息的机密性、不可篡改与不可抵赖。与实现可靠数据传输的 TCP 协议类似, 这是一个典型的“将不可靠信道转化为可靠信道”的实例。

1.2 国内外现状及技术综述^[4]

根据多年来的使用经验, 国内外学者提出电子商务安全要求包括四个方面:

(1) 数据传输的安全性。对数据传输的安全性需求即是保证在公网上传送的数据不被第三方窃取。对数据的安全性保护是通过采用数据加密(包括秘密密钥加密和公开密钥加密)来实现的, 数字信封技术是结合秘密密钥加密和公开密钥加密技术实现的保证数据安全性的技术。

(2) 数据的完整性。对数据的完整性需求是指数据在传输过程中不被篡改。数据的完整性是通过采用安全的散列函数和数字签名技术来实现的。双重数字签名可以用于保证多方通信时数据的完整性。

(3) 身份验证。由于网上的通信双方互不见面, 必须在交易时(交换敏感信息时)确认对方等真实身份; 在涉及到支付时, 还需要确认对方的账户信息是否真实有效。身份认证是采用口令字技术、公开密钥技术或数字签名技术和数字证书技术来实现的。

(4) 交易的不可抵赖。网上交易的各方在进行数据传输时, 必须带有自身特有的、无法被别人复制的信息, 以保证交易发生纠纷时有所对证。这是通过数字签名技术和数字证书技术来实现的。

电子商务系统安全系统结构包括以下部分:

(1) 基本加密算法;

(2) 以基本加密算法为基础的 CA 体系以及数字信封、数字签名等基本安

全技术；

（3）以基本加密算法、安全技术、CA 体系为基础的各种安全应用协议。

以上部分构成了电子商务的安全体系，在此安全体系之上建立电子商务的支付体系和各种业务应用系统。有关基本加密算法、数字信封、数字签名以及各种安全协议的实现应符合相关标准的规定。

CA 认证体系通常以各种基本加密算法为基础，同时采用各种基本安全技术，为上层的安全应用协议提供证书认证功能。

通常，上述安全体系中最为重要的是下述两部分：

（1）符合 CA 证书标准、通常为各国自行开发并拥有版权的认证体系，该体系为用户发放 CA 证书，包括 SSL 证书。CA 证书以 X.509 为基础，并在此基础上进行扩展，兼容如 SSL 等多种协议的证书。

（2）SET CA，符合 SET 标准的 CA 认证体系，专为基于银行支付卡的电子商务服务提供者及用户发放 SET 证书。

2. 需求分析

2.1 总体需求

实现一个安全交易的电商网站，保证用户和商家能够安全的注册、登录、交易，避免信息的泄露或篡改，保护用户和商家的隐私数据安全和财产安全。

2.2 功能需求

电商的基本功能需求：

- 买家、卖家的登录与注册
- 卖家录入商品信息
- 卖家完成商品的上架/下架
- 展示商品信息列表
- 买家购物车
- 买家的商品结算与货款支付
- 买家、卖家的订单信息管理及操作(商品发货、确认收货)

2.3 性能需求

此项目的应用场景仅限于实验环境，因此对性能的需求较小。

采用的测试机参数列表如下

11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz

RAM 16.0 GB (15.8 GB 可用)

Windows 10 家庭中文版

网站的开发框架采用原生 Java Web，基于 Tomcat 服务器，开发环境为 **IntelliJ IDEA 2021.2.2**。

3. 概要设计

电商系统总体功能框架如下：

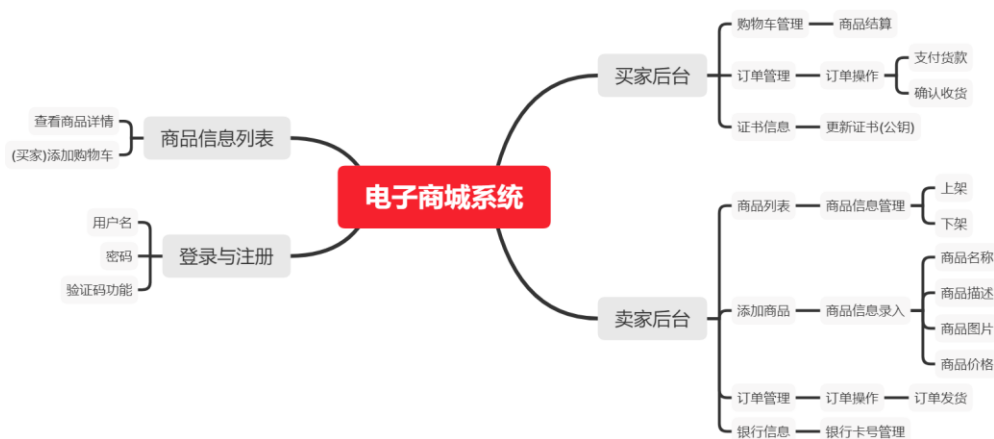


图 1 电商系统总体框架

总体包括两种角色：买家和卖家。

卖家可以在后台完成商品的录入，然后买家就可以在商品列表中浏览到卖家上架的商品，并添加商品到购物车、完成支付功能。其中，需要加密的通信过程有：

- 登录与注册
- 买家与卖家的订单操作
- 买家的订单支付过程

4. 详细设计

后端方面，设计了若干个 **Servlet** 用于请求的处理和转发。在前端方面，设计了若干个 **jsp** 页面用于显示数据。

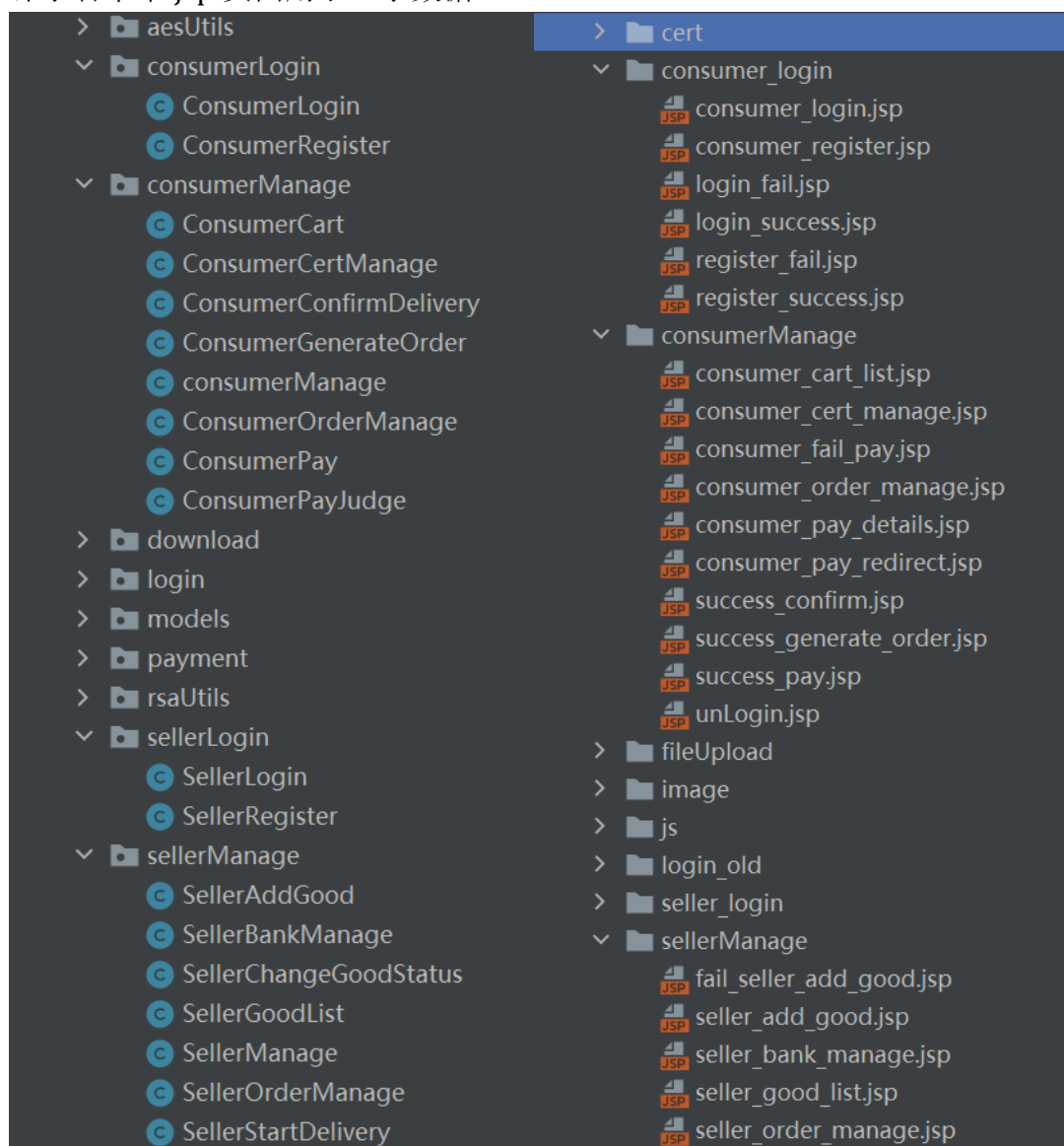


图 2 程序代码结构图

当用户访问某个 **URL** 时，请求会先转发到对应的 **Servlet** 中，在请求的 `req` 中包含了本次请求的各个参数，同时 **Tomcat** 服务器维护每个用户请求的 `session`，通过 `session` 可以在服务器端保存每个用户的状态信息。在 **Servlet** 中，服务器处理用户的请求，并将处理后的数据转发到对应的 **jsp** 页面中，然后再将页面显示给用户看到。

4.1 报文加解密

服务器给客户端发送的每个页面中都包含了电商的公钥。客户端如果需要向电商发送加密信息，则需要用电商的公钥对数据进行加密，这个加密是通过客户

端的 JavaScript 在浏览器中完成的，因此在公共信道上不会有明文传输，浏览器将消息加密后才会通过 POST 或 GET 请求发送出去。

在这里我们的所有加密都采用了电子信封技术，采用公私钥结合的方式完成消息的加密。具体方法是，当客户需要向电商发送敏感数据时，会先生成一个临时的对称密钥(AES 密钥)，使用对称密钥对明文进行 AES 加密得到密文，然后用电商的公钥对临时密钥进行加密，从而得到加密后的 AES 密钥，客户将加密后的 AES 密钥和密文发给服务器，服务器用私钥解密 AES 密钥，即可对明文进行解密。

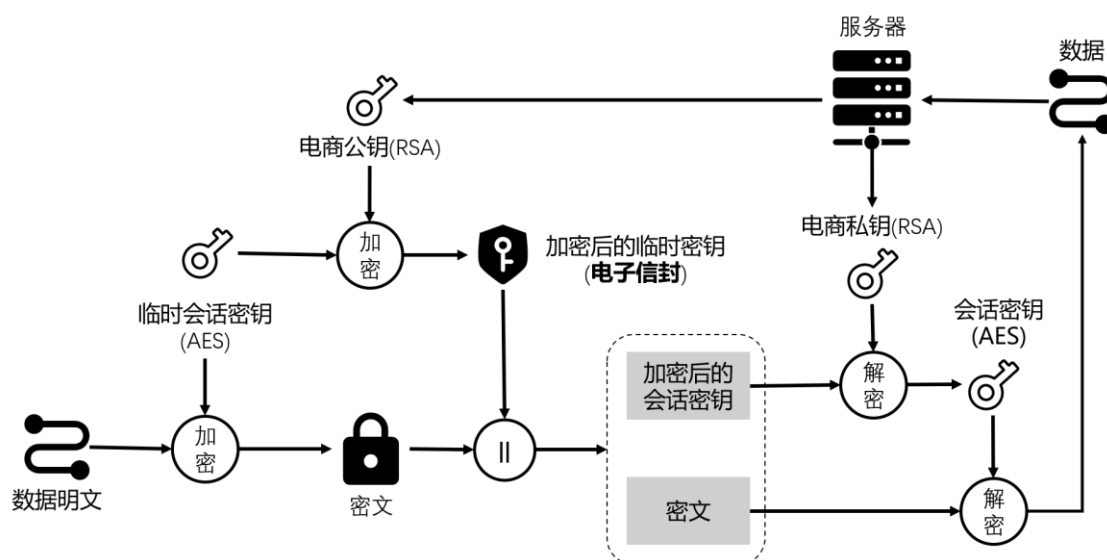


图 3 基于电子信封技术的报文加密方案

4.2 登录与注册

安全性说明：

系统中的两种角色(买家与卖家)均可注册登录。由于登录与注册操作的敏感性，在登录与注册过程中，客户端与服务器端的报文采用端到端的加密方案。当用户访问页面时，电商服务器会在返回的前端页面中包含自己的 RSA 公钥，以使用户将自己的数据用电子信封加密后发给服务器。服务器收到包含用户信息的电子信封后，用自己的 RSA 私钥解密信封后拿到用户输入的用户名与密码，从而在后端完成注册或登录操作。同时，在注册和登录页面提供电商的证书下载接口与 CA 提供的证书验证接口，以使用户验证电商公钥的合法性。

功能性说明：

卖家注册时须绑定自己的银行卡号，以使用户支付货款；买家注册时须绑定自己的 CA 证书(其中包含了买家的 RSA 公钥)，以便在结算时完成 SET 协议中的双签名。登录和注册均采用图形验证码验证，以防数据库被暴力破解。

4.3 卖家商品管理

添加商品：

卖家需要上架新的商品时，要在添加商品的页面中输入商品名称、商品描述、商品价格并上传商品图片，然后将商品信息通过 form 表单提交给电商后端，电

商后端完成图片的存储与商品信息的数据库录入。

在卖家后台，可以展示自己添加的所有商品信息，并进行商品信息的更新，同时完成商品的上架与下架，下架的商品将不在商品列表向买家展示。

4.4 商品展示

与淘宝/京东商城类似，本项目采用在首页展示商品缩略信息、点击后展示商品详情的方式向用户展示商品信息。

在商品列表页面，显示商品的缩略图、商品名称、商品价格、店铺名称等用户关注的首要信息；在商品详情页面，显示商品的详细信息，并提供“添加购物车”按钮给买家，从而实现购物车功能。

4.5 购物车

在数据库中用一张表来专门存储所有买家的购物车数据，其中包含了商品 id、买家名称。

买家登陆后，在商品详情页面可以完成添加购物车的操作。添加购物车之后，在买家后台页面可以进行购物车管理。买家如果想购买某个商品，必须先将商品添加至购物车，然后在买家后台的购物车中进行结算。

4.6 商品结算与支付

商品结算与支付的操作，必须进行加密与签名，从而保证机密性与不可篡改性。商品的支付采用 SET 协议，结合了双签名技术。

顾客想要购买商品时，在购物车中点击结算，电商后端生成一个订单保存在数据库中，订单中包含了买家卖家的用户名、商品 id、商品数量、订单时间以及支付状态、发货状态、收货状态。生成订单后，顾客可以进行订单的支付。在支付时采用 SET 协议与双签名，具体流程如下。

买家在客户端(浏览器中)生成 OI 和 PI，买家在加密时需要输入自己的 RSA 私钥(与注册时的证书对应)用于签名，同时需要输入自己的银行卡号，放到 PI 中加密后发给银行，用于支付。在我们的设计中，OI 包括 orderID, goodID, goodNum, consumerUsername, sellerUsername, orderTime；PI 包括 bankCardNum, orderID, money, sellerUsername。总体流程如下：

如下面的示意图所示，用户端(浏览器)利用订单相关信息生成 OI，利用顾客填写的支付信息生成 PI。用户生成两个 AES 对称密钥 SymKey1 和 SymKey2，利用 SymKey1 对 OI 加密得到 EncryptedOI，利用 SymKey2 对 PI 加密得到 EncryptedPI。然后用电商的公钥对 SymKey1 加密得到 EncryptedSymKey1，用银行的公钥对 SymKey2 加密得到 EncryptedSymKey2。电商和银行的公钥在浏览器中内置。在签名方面，用户分别对 OI 和 PI 进行哈希运算从而得到 OIMD 和 PIMD，然后用户将 PIMD 和 OIMD 连接后再次哈希，得到 POMD，然后顾客用自己的私钥对 POMD 签名从而得到 DS(dual signature, 双签名)。然后用户将 EncryptedOI、EncryptedPI、EncryptedSymKey1、EncryptedSymKey2、PIMD、OIMD、DS 发送给电商端，这些发送出去的报文将在公共信道上传输，但是它们都经过了这样或那样的加密处理，可以保证端到端的安全性。

SET协议——加密部分

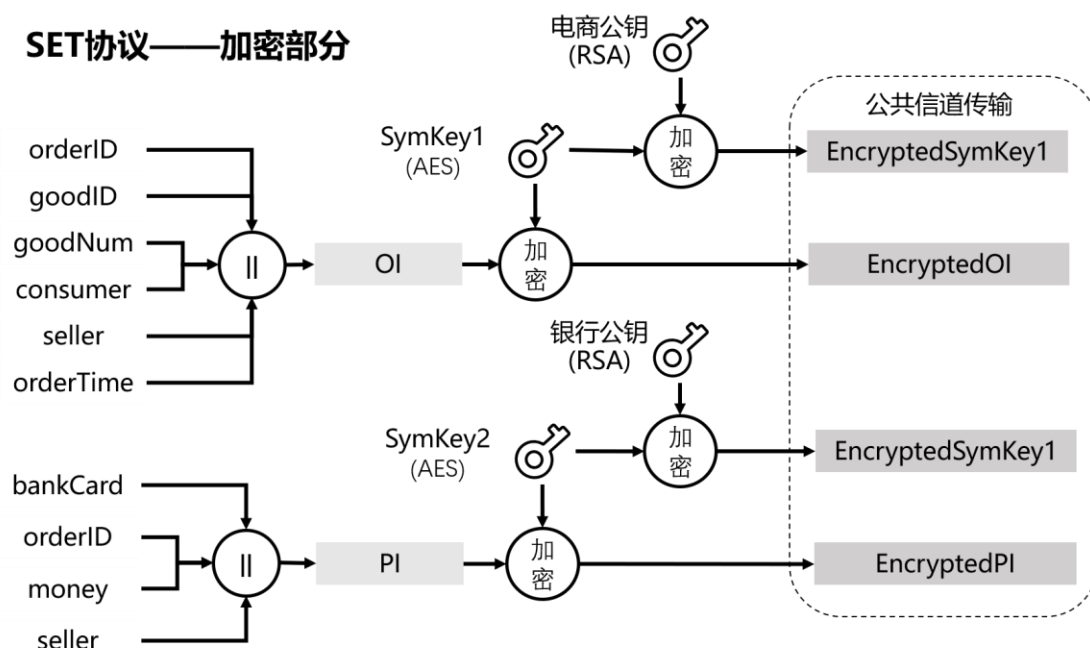


图 4 SET 协议的加密部分

SET协议——签名部分

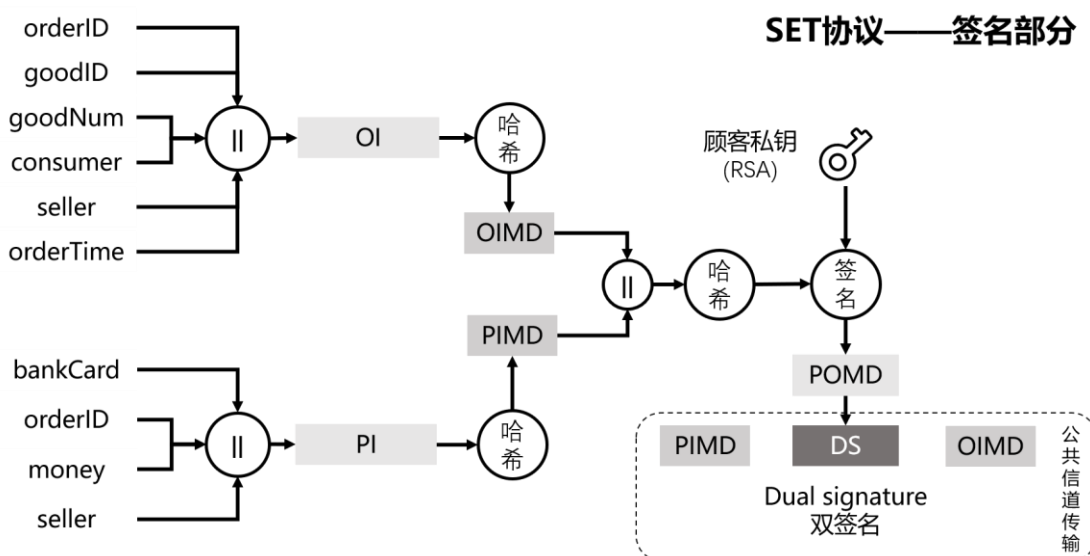


图 5 SET 协议的签名部分

4.7 其他

订单管理：买家的订单管理包括支付操作、确认收货操作；卖家的订单管理包括发货操作，这几样操作均采用加密传输通信保证数据安全。

买家证书：在买家注册时，要求买家填写自己的证书信息，以便电商在收到顾客发来的报文时验证真实性。同时客户可以随时修改自己的证书信息。

卖家银行：当顾客确认收货时需要将钱款自动打入卖家银行账户，因此需要卖家在注册时绑定银行账户信息。

电商证书：在主页面提供一个电商证书的下载链接，同时显示一个 CA 提供的证书验证接口链接，以便顾客验证电商证书(公钥)的真实性。

5. 实现与测试

项目包含若干个 servlet，每个 servlet 处理一个请求。

5.1 首页

商城的首页是导航页面，用于串联商城的各个子页面。首页采用一个静态的 index.jsp 页面来实现，其中包含了一些 HTML 文本及样式。

[Welcome!](#)

欢迎来到密码学商城!

请选择操作:

> [商品列表](#)

卖家操作:

> [卖家注册](#)

> [卖家登录](#)

> [卖家后台](#)

买家操作:

> [买家注册](#)

> [买家登录](#)

> [买家后台](#)

[下载电商证书](#)

[验证证书](#)

图 6 商城首页

5.2 登录与注册

这里以卖家登录与注册为例，在首页点击“卖家注册”即可进入注册页面。在实现上，“卖家注册”绑定了一个名为

`"${pageContext.request.contextPath}/sellerRegister"`

的超链接，这个超链接对应了电商服务器的一个名为 `sellerRegister` 的 servlet，当顾客点击超链接时，请求会被转发到 `sellerRegister` servlet 的 `doGet()` 方法当中，在 `sellerRegister` servlet 的 `doGet` 方法中，我们通过 `getRequestDispatcher` 方法获得到 `/seller_login/seller_register.jsp` 的转发器，然后通过 `forward` 方法将请求转发到这个页面中，于是便可向前端发送 `seller_register.jsp` 页面。

用户在主页点击“卖家注册”，页面跳转到注册页面：

图 7 卖家注册页面

在注册页面中我同样提供了电商证书与验证的超链接。

在卖家注册页面中，用户可以输入用户名、密码、卖家的银行卡号，以及验证码。

验证码的实现是通过一个名为 `checkCode` 的 `servlet` 完成的。在这个 `servlet` 中，我们调用了名为 `GraphicHelper` 的辅助类生成验证码图片，并返回验证码内容，然后将验证码图片的字节流输出到 `HttpServletResponse` 当中，于是便可完成验证码的传输。由于 HTTP 是一个无状态的协议，我们必须使用 `session` 在服务器端保存用户的状态。我们每生成一次验证码就将 `session` 中名为 `checkCode` 的属性当中，于是便可在服务器端实现验证码内容的“记忆”。

然后我们在注册页面的 `jsp` 中，通过下面的 HTML 静态标签完成验证码 `servlet` 的调用。

```
<tr>
  <td class="td_left">验证码</td>
  <td class="td_right"><input type="text" name="checkcode" id="checkcode" placeholder="请输入验证码">
    
  </td>
</tr>
```

图 8 验证码 `jsp` 代码

在用户输入了用户名、密码等信息，并点击“注册”按钮之后，浏览器前端不会立即发送数据(那样就是明文传输了!)，而是会执行一段 JavaScript 代码(这段代码由注册按钮的 `onclick` 事件绑定)。在执行 JavaScript 代码当中，除了完成一些常规检查(如两次密码是否相同)，同时会完成信息的加密。

```
console.log("提交的用户名:", username);
console.log("提交的密码:", password);
var symmetricKey = AESGenerateKey(32);
console.log("对称密钥:", symmetricKey);
var encryptedUsername = AESEncrypt(symmetricKey,
var encryptedPassword = AESEncrypt(symmetricKey,
var encryptedBigIntegerSymKey = RSAEncrypt(rsaPub
console.log("加密的对称密钥:", encryptedBigInteger
console.log('加密的用户名:', encryptedUsername);
console.log('加密的密码:', encryptedPassword);
```

图 9 加密 `js` 代码

上面的这段 JavaScript 就完成了用户名和密码的电子信封加密，加密后通过模拟表单的方式向服务器后端发送一个 POST 请求。这时在公共信道上传输的是经过加密的用户名和密码报文，即使存在窃听者，也无法解密。

服务器后端拿到用户的 POST 请求后，在 doPost 方法中完成中，从 req 解析出加密的各个请求参数，通过自己的私钥解密出电子信封，然后获得用户输入的用户名、密码等信息，并对验证码进行检查。其余的 doPost 方法内容就是完成相关的数据库操作，最后返回是否注册成功的消息给前端。于是注册界面的功能使用完成。

登录页面与注册页面类似，输入信息后，“登录” button 的 onclick 事件同样绑定到一个 JavaScript 函数中，在函数中完成用户数据的加密后再提交 POST 请求。登录的 servlet 后端收到登录请求后，采取与注册同样的方式完成电子信封的解密，获取到用户输入的用户名和密码后，进行数据库查询，并对验证码进行校验。



图 10 登陆页面

登录后端 servlet 对用户名和密码到数据库中进行验证，如果验证失败则向前端返回一个登陆失败的提示；如果验证通过则在 session 中写入登录的用户名 username 和用户类型 userType(seller/consumer, 卖家/买家)，并向前端返回登录成功的消息。下面是一次登录成功的示例图：

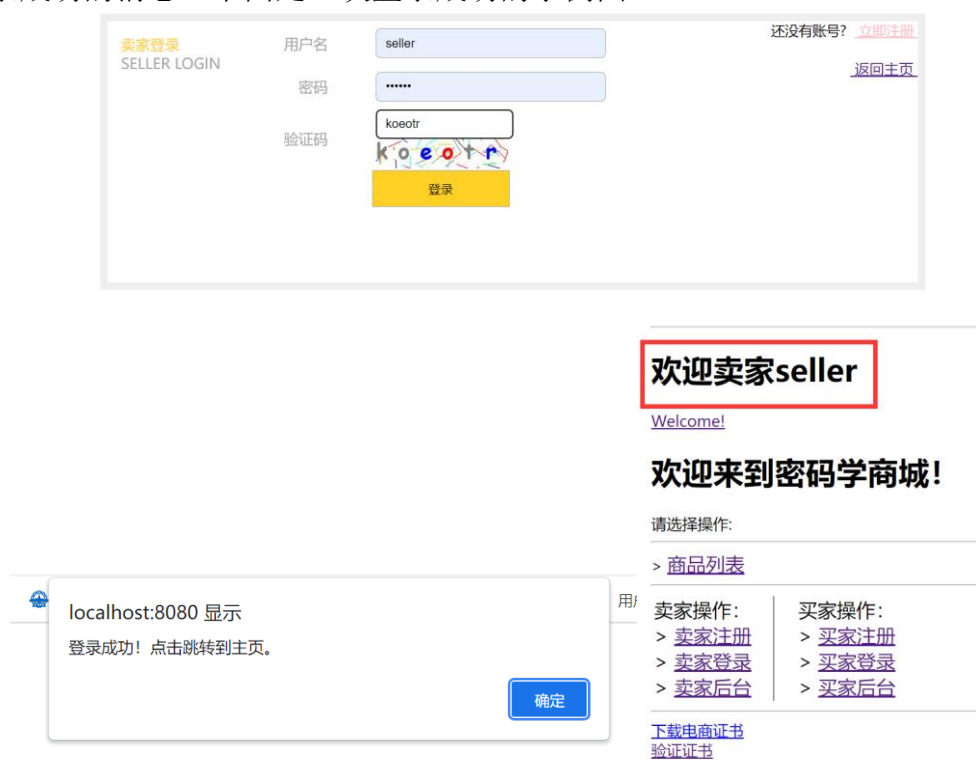


图 11 登录成功

登陆成功后会在 **session** 中保存登录状态，由于 **session** 中的数据保存在服务器端，因此可以保证登陆状态的安全性。

至此，安全的登录与注册已经完成。

5.3 卖家商品管理

在卖家没有登录时，如果尝试点击“卖家后台”则会被提示登陆后再进入：



图 12 非法操作提示

登录的状态通过 **session** 来验证。卖家登陆后点击“卖家后台”则可进入卖家后台的管理页面。在卖家后台，卖家可以进行商品的管理：

卖家后台-欢迎您, seller! 返回主页 退出登录

商品列表
添加商品
订单管理
银行信息

添加商品

商品名称	
商品描述	
商品图片	<input type="button" value="选择文件"/> 未选择任何文件
商品价格	<input type="text" value="100.00"/>
是否上架	<input type="checkbox"/> 上架

图 13 添加商品页面

相关功能包括添加商品、修改商品状态、订单管理、银行信息。在“添加商品”页面中(“添加商品”是一个 **servlet**)，卖家用户可以输入需要新增的商品信息及相关描述，并上传商品图片，设置商品价格，从而完成商品信息的录入。这里的商品信息通过 **meta-data** 类型的 **form** 表单提交到后端服务器，后端服务器通过 **DiskFileItemFactory** 完成 **form** 表单的解析，并从中提取出图片文件及其他参数。将图片文件用随机文件名保存在服务器端，从而完成商品信息的录入。下面进行一个测试商品的录入：

卖家后台-欢迎您, seller! 返回主页 退出登录

商品列表
添加商品
订单管理
银行信息

添加商品

商品名称	计算机视觉——算法与应用
商品描述	作为人,我们可以轻松感知周围的三维世界。相比之下,不管计算机视觉在近年来已经取得多么令人瞩目的成果,但要让计算机能像两岁小孩那样解释和理解图像,却仍然是一个遥不可及的梦想。为什么计算机视觉会成为如此富有挑战性的难题?它当前发展到了哪个阶段?围绕这些问题,《计算机视觉——算法与应用》探索了用于分析和解释图像的各种常用方法,描述了42个成功的视觉应用实例,既有医学成像之类的专业应用,又有图像编辑和拼接之类有趣的大众应用。这种精心的编排和设计有利于学生将这些看似高深的技术应用于自己的照片和视频,从而在趣味
商品图片	<input type="button" value="选择文件"/> QQ截图20211216194400.png
商品价格	<input type="text" value="100.00"/>
是否上架	<input checked="" type="checkbox"/> 上架

图 14 录入商品信息

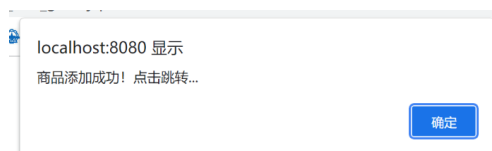


图 15 录入商品成功

添加成功后在商品列表中即可查看到各个添加的商品:

卖家后台-欢迎您, seller! 返回主页 退出登录

商品名称	商品图片	商品描述	商品价格	状态	操作
测试商品		测试商品测试商品测试商品测试商品测试商品测试商品测试商品测试商品测试商品测试商品	¥ 100.0	上架	<input type="button" value="下架"/>
测试商品2		测试商品2测试商品2测试商品2测试商品2测试商品2测试商品2测试商品2	¥ 200.0	上架	<input type="button" value="下架"/>
计算机视觉算法与应用		作为人,我们可以轻松感知周围的三维世界。相比之下,不管计算机视觉在近年来已经取得多么令人瞩目的成果,但要让计算机能像两岁小孩那样解释和理解图像,却仍然是一个遥不可及的梦想。为什么计算机视觉会成为如此富有挑战性的难题?它当前发展到了哪个阶段?围绕这些问题,《计算机视觉——算法与应用》探索了用于分析和解释图像的各种常用方法,描述了42个成功的视觉应用实例,既有医学成像之类的专业应用,又有图像编辑和拼接之类有趣的大众应用。这种精心的编排和设计有利于学生将这些看似高深的技术应用于自己的照片和视频,从而在趣味横生的动手实践中获得成就感。本书主题和特色:编排结构有利于活跃课堂气氛,适合面向项目的课程,针对各种特定课程提供了本书使用提示每章末尾的习题着重强调对算法的测试,重点包含大量针对小型期中课题的建议,附录中提供额外的补充材料和更详细的数学知识介绍,包括线性代数、数值方法和贝叶斯估计理论完整的参考文献和每章的补充阅读,覆盖各个子领域新的研究进展和成果	¥ 100.0	上架	<input type="button" value="下架"/>

图 16 卖家后台-商品列表页面

“商品列表”是一个名为 sellerGoodList 的 servlet, 在它的 doGet 方法中, 进行数据库查询, 从数据库中查询到当前登录的卖家发布的所有商品, 并把它们发送到前端 jsp 页面中显示给用户。在商品列表中, 可以对商品的状态进行修改, 如上架和下架, 这里的操作中, 浏览器和服务器之间是电子信封加密传输的, 防止黑客对操作的商品 id 进行篡改。

5.4 商品列表与商品详情

卖家上架商品后, 买家就可以在商城的商品列表中看到商品的信息。我们用一个买家账号登录, 然后进入商品列表界面:



图 17 商品列表页面

商品列表是一个 `Servlet`，在这个 `Servlet` 的 `doGet` 方法中，会查询数据库中所有上架的商品并显示到页面前端。在商品列表界面，点击商品的描述或图片，即可进入商品的详情：

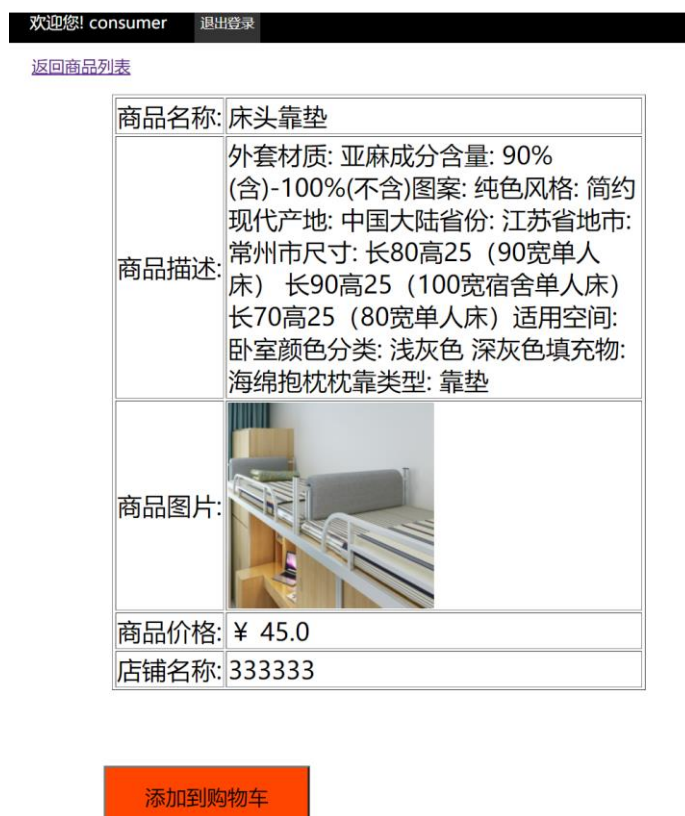


图 18 商品详情页面

商品详情也是一个 `Servlet`，它会根据请求参数中的商品 ID 查询数据库，并把商品的详细信息输出到页面前端显示给用户。在商品详情页面，用户可以点击“添加到购物车”从而实现商品添加到购物车。

5.5 购物车

在商品详情页面点击“添加购物车”按钮即可将商品添加到买家的购物车。购物车的数据库存在于服务器端。购物车页面也是通过一个 `Servlet+JSP` 来实现的，在 `Servlet` 的 `doGet` 方法中，服务器到购物车数据库中查询该买家用户的用户名对应的所有商品，并把商品信息输出到 `JSP` 页面中显示给用户前端，从而实现了购物车的显示。

在购物车中，可以对商品进行结算，点击“结算”按钮后，会立即生成一个该商品的订单，用户在订单管理中可以支付订单，用户需要在 30 分钟内支付订单，否则订单会被撤销。




买家后台-欢迎您, qq! 返回主页 退出登录					
购物车	商品名称	商品图片	商品描述	商品价格	操作
订单管理	陶瓷碗		日式陶瓷碗家用吃饭餐具米饭碗小汤碗手绘高脚碗创意斗笠碗喇叭碗 材质: 瓷图案: 其他/other风格: 日式产地: 中国大陆流行元素: 手绘插画碗口直径: 5英寸颜色分类: 四色线条 (单个) 网格梅花 (单个) 蓝色线条 (单个) 塘草 (单个) 毛重: 250g价格区间: 10元-19.9元货号: 日式喇叭碗主图来源: 自主实拍图个数: 1个茶餐具工艺: 釉下彩适用人群: 大众	¥13.6	结算
证书信息	计算机视觉算法与应用		作为人，我们可以轻松感知周围的三维世界，相比之下，不管计算机视觉在近年来已经取得多么令人瞩目的成果，但要让计算机能像两岁小孩那样解释和理解图像，却仍然是一个遥不可及的梦想。为什么计算机视觉会成为如此富有挑战性的难题？它当前发展到了哪个阶段？围绕着这些问题，《计算机视觉——算法与应用》探索了用于分析和解释图像的各种常用方法，描述了42个成功的视觉应用实例，既有医学成像之类的专业应用，又有图像编辑和拼接之类有趣的大众应用.....	¥100.0	结算
	炒锅		不锈钢防油锅盖手柄29CM防油网罩防油网罩防油网罩炒菜防油挡板32CM	¥11.9	结算

图 19 购物车页面

5.6 商品结算与支付

商品结算时，用户在购物车内点击结算，会生成一个订单，然后在订单管理中可以查看到订单信息。

买家后台-欢迎您, consumer! 返回主页 退出登录										
购物车	订单管理									
订单管理	订单编号	商品名称	单价	数量	订单金额	卖家ID	支付状态	发货状态	订单完成	订单时间
证书信息	9	测试商品测试商品	¥100.0	1	¥100.0	seller	已支付	已发货	已完成	2021-12-13 10:50:10
	11	测试商品测试商品	¥100.0	1	¥100.0	seller	已支付	未发货	未完成	2021-12-15 10:29:53
	12	测试商品测试商品	¥100.0	1	¥100.0	seller	已支付	已发货	未完成	2021-12-17 20:43:21
	13	商品12-18	¥100.0	1	¥100.0	seller	已支付	已发货	已完成	2021-12-18 14:30:49
	14	测试15-56	¥100.0	1	¥100.0	seller	未支付	未发货	未完成	2021-12-18 15:28:42

图 20 订单管理页面

然后我们点击“开始支付”即可进入支付页面。

支付订单

订单编号	14
商品ID	16
商品数量	1
买家名称	consumer
卖家名称	seller
购买时间	2021-12-18 15:28:42 (毫秒值1639812522000)
支付银行卡号	
您的mod	2886788989219977234381
您的公钥exp	65537
您的私钥exp(用于签名, 不会上传)	2303722540491704065766

开始支付

图 21 订单支付页面

在订单支付页面，顾客需要输入自己的银行卡号以及私钥，浏览器会在前端执行一段 JavaScript 代码，用顾客的私钥完成订单信息的双签名，同时对 PI 和 OI 分别用银行和电商的密钥加密后，再发送到后端，从而完成信息的保密性。

在电商的后端会根据 SET 协议的规则对顾客的双签名进行验证，同时对 OI 进行解密，从而获得订单信息，再查找数据库，找到卖家的银行卡号，把请求转发给电子银行系统。

顾客点击“开始支付”button 之后，电商后端对顾客的双签名验证通过，然后将请求转发至银行系统，顾客的页面被重定向到银行系统当中。

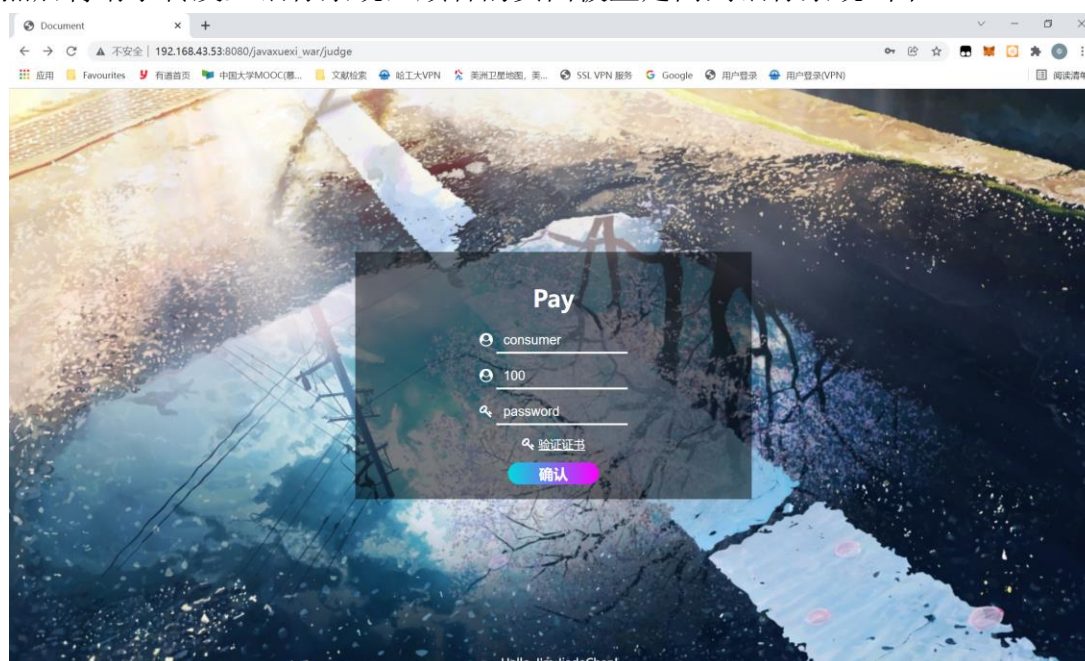


图 22 银行支付页面

用户在银行系统输入自己的银行卡支付密码，从而完成支付。完成支付之后，

银行会对支付成功的消息用自己的私钥进行签名，将消息转发给电商，电商收到消息后验证该消息的真实性与有效性，如果验证通过则说明支付成功，电商在数据库中完成订单状态的修改，最后重定向到支付成功的页面展示给用户。



图 23 银行支付成功

最后完成了支付之后，用户在订单管理的页面当中可以看到订单的状态已经变成“已支付”。

买家后台-欢迎您, consumer! 返回主页 退出登录

购物车

订单管理

证书信息

订单管理

订单编号	商品名称	单价	数量	订单金额	卖家ID	支付状态	发货状态	订单完成	订单时间	操作
9	测试商品测试商品	¥ 100.0	1	¥ 100.0	seller	已支付	已发货	已完成	2021-12-13 10:50:10	订单已完成
11	测试商品测试商品	¥ 100.0	1	¥ 100.0	seller	已支付	未发货	未完成	2021-12-15 10:29:53	确认收货
12	测试商品测试商品	¥ 100.0	1	¥ 100.0	seller	已支付	已发货	未完成	2021-12-17 20:43:21	确认收货
13	商品12-18	¥ 100.0	1	¥ 100.0	seller	已支付	已发货	已完成	2021-12-18 14:30:49	订单已完成
14	测试15-56	¥ 100.0	1	¥ 100.0	seller	已支付	未发货	未完成	2021-12-18 15:28:42	确认收货

图 24 支付成功-订单信息

整体的支付流程示意图如下：



图 25 订单支付流程示意图

5.7 订单管理

一条订单包括三个状态变量：支付状态、发货状态、收货状态。在买家后台，

可以对订单进行支付，从而修改订单的支付状态，买家后台也可以对已发货的订单进行确认收货，从而让货款顺利进入卖家的银行卡当中；卖家后台可以对已支付的订单进行发货操作。对于已确认收货的订单，状态被标记位“已完成”。对于订单状态的修改操作均采用电子信封加密，以防黑客篡改消息。

买家后台-欢迎您, qq! 返回主页 退出登录										
购物车 订单管理 证书信息	订单管理									
	订单编号	商品名称	单价	数量	订单金额	卖家ID	支付状态	发货状态	货款到账	订单时间
	4	苹果笔记本	¥ 3899.0	1	¥ 3899.0	111111	已支付	未发货	已到账	2021-11-27 22:30:56
	5	测试商品1	¥ 100.0	1	¥ 100.0	333333	已支付	已发货	已到账	2021-11-27 22:48:34
	6	苹果笔记本	¥ 3899.0	1	¥ 3899.0	111111	已支付	未发货	未到账	2021-12-10 14:12:46
	7	床头靠垫	¥ 45.0	1	¥ 45.0	333333	已支付	已发货	已到账	2021-12-10 14:14:55
	8	书包	¥ 289.0	1	¥ 289.0	333333	已支付	未发货	未到账	2021-12-13 08:39:44
	10	抱枕	¥ 25.8	1	¥ 25.8	333333	未支付	未发货	未到账	2021-12-13 22:21:57

图 26 订单管理页面(支付、收货、完成)

5.8 证书管理

买家的证书用于 SET 协议中的双签名报文在验签时使用，因此电商服务器需要维护买家的证书信息。买家可以在后台的“证书信息”中随时更改自己的证书信息，然后在每次需要支付时采用最新的私钥进行签名即可。证书信息的格式采用 CA 规定的格式化字符串。

买家后台-欢迎您, qq! 返回主页 退出登录	
购物车 订单管理 证书信息	证书信息
	Serial Number: B5E1D8FF0381A0FF4F80511C08EA39EC8362C1D5162FAEBC9980E810CB70A12E Yangwh CA: www.yangwhCA.com Sign Algorithm: sha256RSA Valid Time From: 20211213152327 Valid Time To: 20221213152327 User: consumer Public Key: 19461448773002628854891711061929754374314173674143803650636633488438656675663841911337019463292962129422736278629772214396 1772790710579948518036211955823911364434907997723466114358804144368943750598411857875691546236111133428923898931044134631 3549679748620619700224657881052762764851338145425911439907981487757432568032683362794801568408130732592384372754912240381 0184023942335739067971997488010670384976286148243107959029127445715418660568697631546435933049052471129915185129121901519 7343788465524279197145225692885173890510460444037974659306626395399156294117301666765293459767175216158502846640789416766 1108284451 Sign: 5bc54d90f419166dd64e56320c4d770f5439ea8c70abb20b11a3ad80f0d1a98806e1c6749812976a771ffidca359570862d64097eab690087638537309 df11373cee09c92b120af5102f5b28ea47af92218b6f8c6685e9f8c999d88e434db82a9888ccabe1a5ab51569c4ddb587b1f43b6756439e0a2fd7ac6d2 9e73a38cc2702f8ad7f5d0b2637c2607400416d28b946097113eb4077b805121ccadd85ac939934480174e99e225185949873b3f8022829044b80e1eb7c fcf10e2219f0eac97af4f2f08099d07b3d74efe8ba7af50d8153743afa1856ce3dfff8dc5dcad86f92e7b3d6c5859924127eddb9bbe77d3ffe2ef7408c149f4f 70ad0c1fd8d5a3e2b7
	更新证书

图 27 证书管理页

5.9 证书验证

在商城首页可以进行证书验证操作，点击进入证书验证页面：

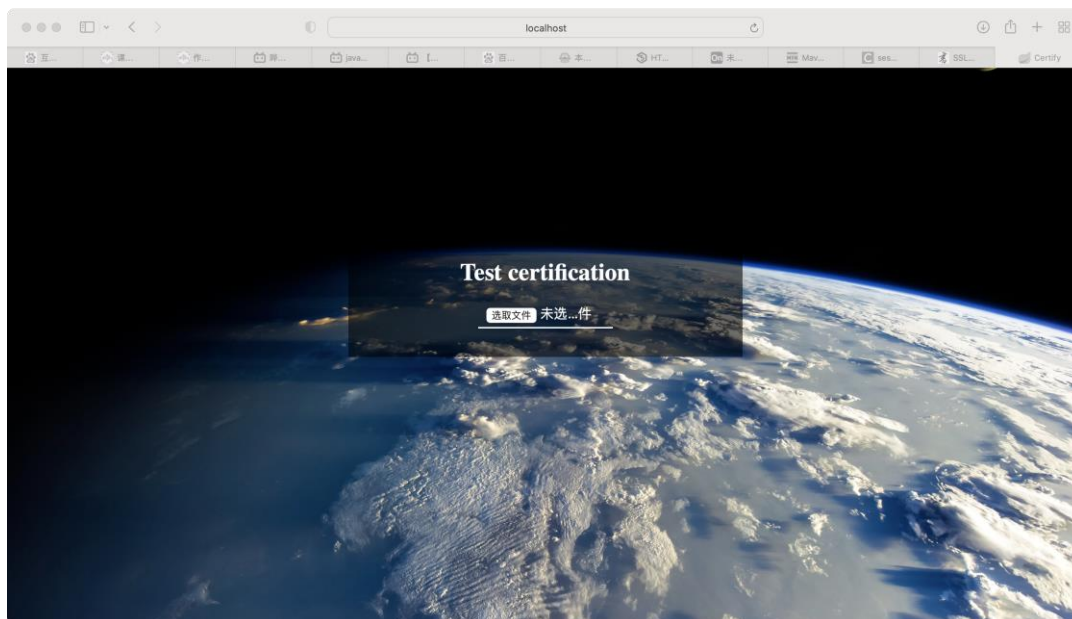


图 28 证书验证页

然后上传证书文件，可以看到证书验证通过的消息：

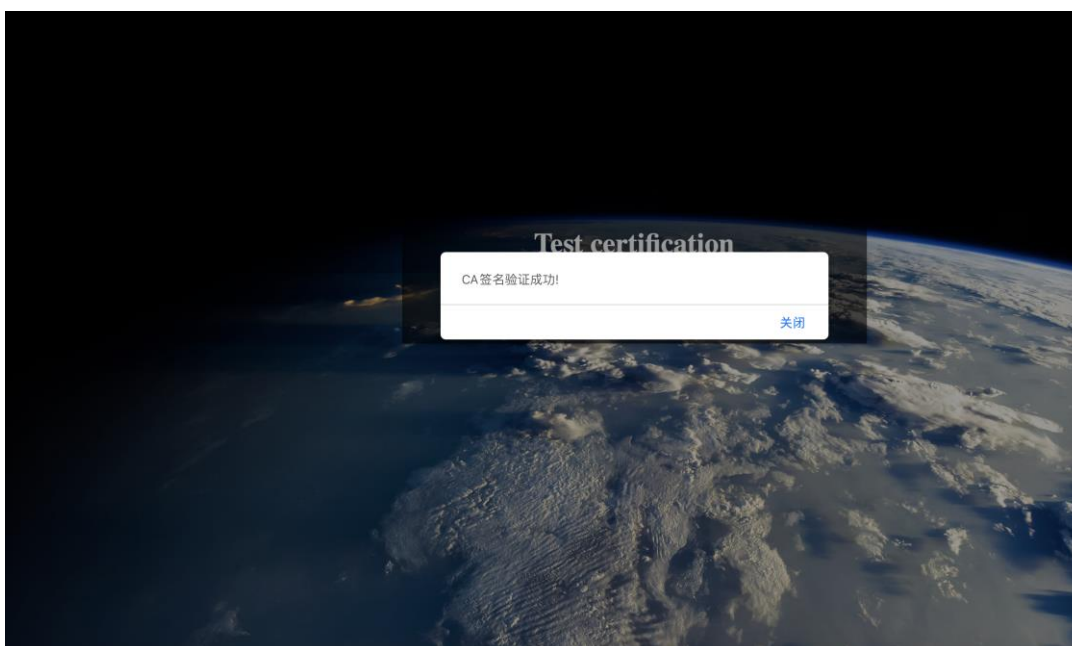


图 29 证书验证通过

6. 结束语

电子商务交易系统一般包括三个实体，买方，销售方及银行系统。电子商务系统需要数字签名和认证技术，都是借助于密码技术来实现。身份认证是通信和数据系统正确识别通信用户或终端个人身份的重要途径。身份认证的主要途径有：口令技术：散列函数生成保文摘要；与密钥配合使用；时间戳技术：电子商务中，时间是防止文件被伪造和篡改的关键性内容。DTS（DTS: digital time stamp service）是对电子文件发布时间的安全保护。

在本次密码学实验中，开发了一个完整的基于 http 协议的电商交易平台，它在 http 明文传输的基础上，通过端到端的加密方式，在一个不安全的传输信道上实现了传输报文的机密性、完整性、可用性保护，将一个不安全信道变成了一个安全的传输信道，实现了用户隐私信息的保护，深入理解了公私钥加密、数字签名、证书的使用方式。同时，熟悉了网站开发的完整流程，完成了从前端设计到后端开发的各项任务。

在本实验中，电商要负责将银行、CA 整合到自己的系统当中，其中涉及到许多接口的统一与协调，在整个项目过程中，我与组员很好的合作，设计了大量交互接口，整体合作流程十分顺利，很好的锻炼了合作开发能力。

整个开发过程中，遇到的困难主要有以下几个：

- 加密方式的同一性：对于同一个加密算法(如 sha256/AES)，由于实现细节的差异，前端(JavaScript)与后端(Java)很难找到同一套配套的算法。
- 前端设计的美观性：由于项目的性能需求不是很高，后端开发并不存在较大困难，但是由于我对 html、css 代码仍不是很熟悉，在前端方面很难设计出美观的界面。
- 项目结构的复杂性：本项目使用原生 JavaWeb 框架开发，整个项目结构比较杂乱，例如 html 引用 image 时，时常出现找不到图片的情况。
- 通信流程的有序性：SET 协议对支付报文(PI 与 OI)的内容做了规定，按照 SET 的规定进行交互可保证信息的完整性，但是其实现细节上仍有许多问题，在项目中耗费了较多时间进行报文结构以及交互信息时序的设计。

至此，密码学实验项目完成，感谢开发过程中李开元、杨文昊两位队友的鼎力相助，同时也感谢翟老师给予的指导。

参考文献

- [1]曹冬. 电子商务模式研究[D].对外经济贸易大学,2002.
- [2] 黄海龙. 基于以电商平台为核心的互联网金融研究[J]. 上海金融,2013(08):18-23+116.
- [3] 杨雅芬,施佳. 电商法实施对我国跨境电商平台的影响及策略[J]. 杭州电子科技大学学报(社会科学版),2021,17(05):28-33.DOI:10.13954/j.cnki.hduss.2021.05.005.
- [4] 霍要峰,张啸雄. 电子商务 O2O 中的安全体系分析[J]. 信息安全与通信保密,2012(11):121-123.