

电子商务与安全

实验指导书

班级：1504201

姓名：殷悦

实验报告的内容

1. 题目

描述每个实验的内容是什么。

2. 需求分析、程序数据流与功能图

用 E-R 图描述数据库的模式设计及每个关系模式的建立；描述数据字典及程序数据流与功能图；每个事件、函数或过程的头和规格说明；列出每个过程或函数所调用和被调用的过程或函数，也可以通过调用关系图表示。主要算法的框架。

3. 调试报告

调试过程中遇到的主要问题是如何解决的；对设计和编码的回顾讨论和分析；改进设想；经验和体会等。

4. 源程序清单和结果

源程序要加注释，要有测试数据及结果。

实验 1： 学习 Vbscript 语言 和 ASP 的 ADO 接口访问 SQL SERVER2000 的数据库（4 学时）

本次实验的主要目的和内容：

1. 熟悉 VBScript 在 HTML 中的应用
2. 掌握 ASP 的 ADO 接口访问 SQL SERVER2000 数据库连接
3. 应用 ASP 开发基于 SQL SERVER 数据库的开发一个小型商务网站注册、登录及商品显示过程

实 验 报 告 1

一、 需求分析、程序数据流与功能图

需求分析

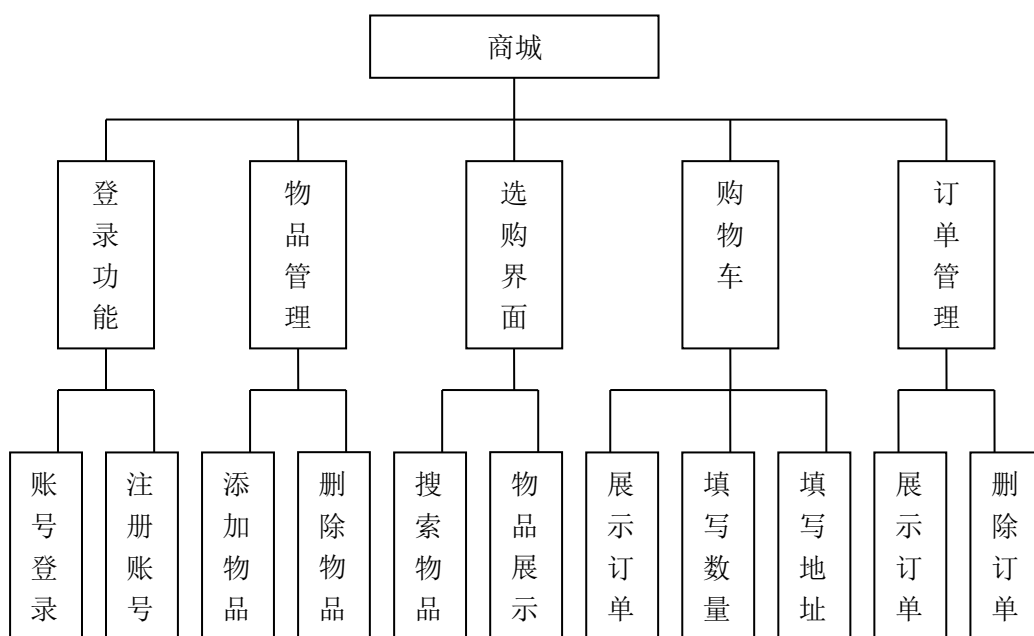


图 1 需求分析

注册账号流程图

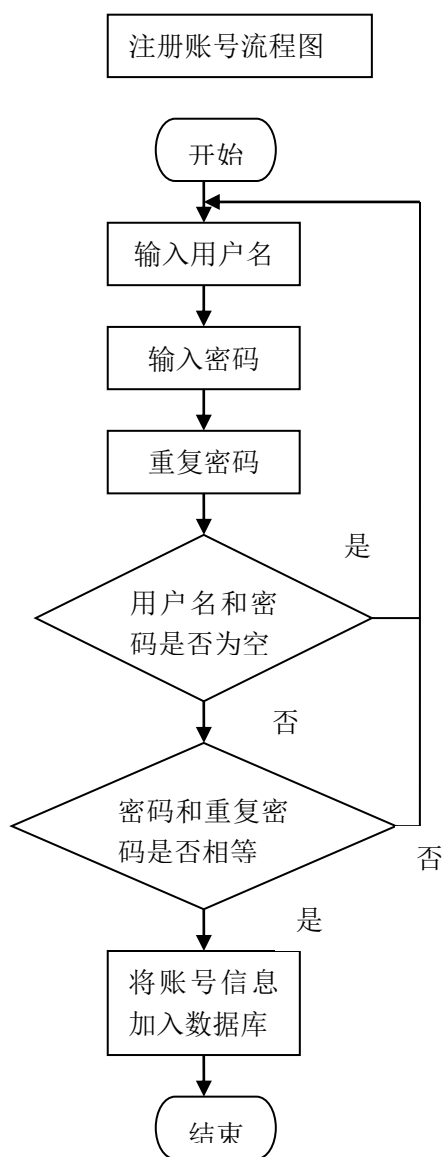


图 2 注册账号流程图

登录流程图

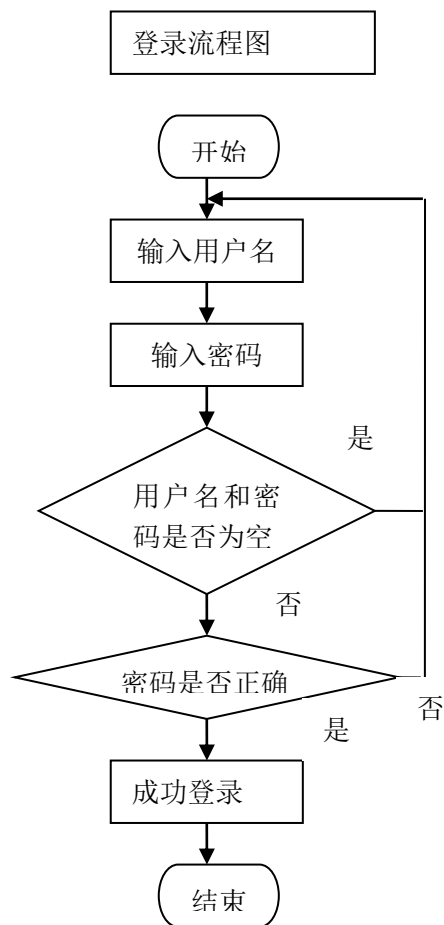


图 3 登录流程图

二. 程序源代码及结果

创建数据库: create.sql

--账号数据库, 第一个实验用

CREATE TABLE account

```
(  
    username varchar(20) NOT NULL ,  
    password varchar(20) NOT NULL  
);
```

--购买数据库, 第二个实验用

CREATE TABLE buy

```
(  
    ONum int NOT NULL ,  
    BCount int NULL ,  
    BName varchar(20) NOT NULL  
);
```

--货物数据库, 第二个实验用

CREATE TABLE goods

```
(  
    GName varchar(20) NOT NULL ,  
    GPrice float NULL ,  
    GCount int NULL  
);
```

--订单数据库, 第二个实验用

CREATE TABLE orders

```
(  
    ONum int NOT NULL ,  
    OTime datetime NULL ,  
    username varchar(20) NOT NULL ,  
    consignee varchar(20) NULL ,
```

```

location varchar(50) NULL ,
zipcode varchar(20) NULL ,
tel varchar(20) NULL ,
cfm int NOT NULL
);

```

数据库连接：conn.asp 数据库连接界面



<%

```
Set conn=Server.createobject("adodb.connection")
```

'conn.Open "test"'之前在自己 Windows 虚拟机，装上 ODBC 的 mysql 驱动，用 ODBC 连接上我的 mysql 服务器 ODBC 直接写名为 test 数据库
'注册的万网虚拟主机 asp 环境，并带 sql server 数据库，可以远程连接数据库，数据库登录地址 <https://dms-net.aliyun.com/>

```

StrConn="driver={SQL
Server};server=qds167524598.my3w.com;uid=qds167524598;pwd=yinyue12
3;database=qds167524598_db"

```

```
Conn.open StrConn
```

```
If conn.State <> 1 Then
```

```
    Response.write "Failed to connect Sql!"
```

```
    Response.End
```

```
End If
```

%>

```
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
```

登录页面：login/index.htm 登录静态界面

预览地址 <http://shop.wifewifi.com/login/>



```
<html>
```

```
  <head>
```

```
    <title>Login</title>
```

```
  </head>
```

```
  <body>
```

```
    <form method="GET" action="login.asp">
```

```
      <p align="center"><font face="隶书" size="5">Login</font></p>
```

```
      <p align="center">Username:<input type="text" name="username" size="20"></p>
```

```
      <p align="center">Password:<input type="password" name="password" size="20"></p>
```

```
      <p align="center">
```

```
        <input type="submit" value="Login" name="submit">
```

```
        <input type="reset" value="Reset" name="reset">
```

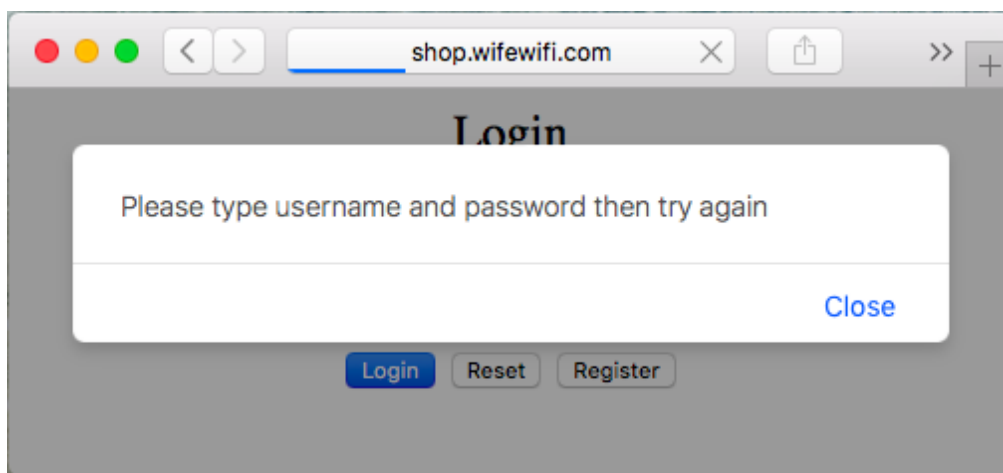


```

        <input type="button"
onclick="javascript:top.location='reg.htm';" value="Register">
    </p>
</form>
</body>
</html>

```

login/login.asp 登录验证



```
<!--#include file="../conn.asp"-->
```

<%’上面包含，连接数据库

```
Dim username,password
```

```
Dim conn,rs
```

```
username=Trim(Request("username"))
```

```
password=Trim(Request("password"))
```

```
If username <> "" and password <> "" Then
```

```
    strSql="select * from account where username='"&username&"' and
password='"&password&"'
```

```
    Set rs=server.CreateObject("adodb.recordset")
```

```
    rs.open strSql,conn,1,1
```

‘查数据库，如果没找到，就说明账号或密码不正确

```

    If rs.eof Or rs.bof Then
        Response.write "<script
LANGUAGE='javascript'>alert('Username      or      password
wrong!');history.go(-1)</script>"
        Response.end
    End If
    rs.close
    '将用户名保存到 session 中，并跳转页面
    Session("username")=username
    Response.Redirect("../index.asp")
    Response.End
Else'如果没输入用户名和密码，就弹出来输入用户名密码的错误提示
    Response.write "<script LANGUAGE='javascript'>alert('Please type
username and password then try again');history.go(-1)</script>"
    End If
%>

```

注册页面：login/res.htm 静态页面

预览地址 <http://shop.wifewifi.com/login/reg.htm>



The screenshot shows a web browser window with the address bar displaying 'shop.wifewifi.com'. The page content is a registration form titled 'Register'. It includes three text input fields labeled 'Username:', 'Password:', and 'Confirm :'. At the bottom of the form, there are three buttons: 'Display a menu', 'Register', and 'Reset'.

<html>

```

<head>
    <title>Register</title>
</head>
<body>
    <form method="GET" action="reg.asp">
        <p align="center"><font fane="隶书"
size="5">Register</font></p>
        <p align="center">Username:<input type="text"
name="username" size="20"></p>
        <p align="center">Password:<input type="password"
name="password" size="20"></p>
        <p align="center">Confirm :<input type="password"
name="confirm" size="20"></p>
        <p align="center">
            <input type="submit" value="Register" name="submit">
            <input type="reset" value="Reset" name="reset">
        </p>
    </form>
</body>
</html>

```

login/res.asp 注册模块

```
<!--#include file="../conn.asp"-->
```

```
<%
```

```
    Dim username,password
```

```
    Dim conn,rs
```

```
    username=Trim(Request("username"))
```

```
    password=Trim(Request("password"))
```

```
    confirm=Trim(Request("confirm"))
```

‘判断账号和密码是否为空，如果不为空判断密码和重复密码是否相等，
不相等就输出错误

```
If username <> "" and password <> "" Then
    If password <> confirm Then
        Response.write "<script
LANGUAGE='javascript'>alert('Password or confirm must be the
same!');history.go(-1)</script>"
    End if
    strSql="select * from account where username='"&username&'"
    Set rs=server.CreateObject("adodb.recordset")
    rs.open strSql,conn,1,1
    If rs.eof Or rs.bof Then
        strSql="insert Into account(username,password) Values
('"&username&"','"&password&"')
        'Set rs=server.CreateObject("adodb.recordset")
        'rs.open strSql,conn,1,1
        Set rs=conn.execute(strSql)
        Response.write "<script
LANGUAGE='javascript'>alert('Register success.Please
login!');history.go(-2)</script>"
        Response.End
    Else
        Response.write "<script
LANGUAGE='javascript'>alert('Username exist!');history.go(-1)</script>"
        Response.End
    End If
    Response.End
    rs.close
Else
    Response.write "<script LANGUAGE='javascript'>alert('Please type
username and password then try again');history.go(-1)</script>"
End If
```

%>

login/goods.asp 货物添加管理页面

Username:yinyue [Logout](#)

Goods information

Add goods

Goods name:	<input type="text"/>
Price:	<input type="text"/>
Count:	<input type="text"/>
	Add Reset

Goods list

Name	Price	Count	Operate
89K	12800	998	Buy Delete
9A91	18000	3000	Buy Delete
AA12	30000	1998	Buy Delete
Flashbang	5000	50000	Buy Delete
Smoking grenade	4000	10000	Buy Delete
Display a menu	1.5	999	Buy Delete

```
<!--#include file="../conn.asp"-->
```

```
<html>
```

```
<head>
```

```
    <title>Goods information</title>
```

```
</head>
```

```
<body>
```

```
<p>Username:<%Response.write Session("username")%>
<input          type="button"          onclick="javascript:history.go(-1);"
value="Logout"></p>
<h1 align="center">Goods information</h1>
<hr>
<h3>Add goods</h3>
<form method="GET" action="opr.asp">
  <table border="2" width="80%">
    <tr>
      <th>Goods name:</th>
      <th><input type="text" name="GName" size=20></th>
    </tr>
    <tr>
      <th>Price:</th>
      <th><input type="text" name="GPrice" size=20></th>
    </tr>
    <tr>
      <th>Count:</th>
      <th><input type="text" name="GCount" size=20></th>
    </tr>
    <tr>
      <th>&nbsp;</th>
      <th>
        <input type="submit" value="Add" name="submit">
        <input type="reset" value="Reset" name="reset">
      </th>
    </tr>
  </table>
</form>
<h3>Goods list</h3>
```

```
<table border="4" width="80%">
  <tr>
    <th>Name</th>
    <th>Price</th>
    <th>Count</th>
    <th>Operate</th>
  </tr>
<%
  strSql="select GName,GPrice,GCount from goods"
  Set rs=server.CreateObject("adodb.recordset")
  rs.open strSql,conn,1,1
  If Not rs.eof And Not rs.bof Then
    Do While Not rs.eof
%>
  <tr>
    <th><%=rs("GName")%></th>
    <th><%=rs("GPrice")%></th>
    <th><%=rs("GCount")%></th>
    <th>
      <a
href="opr.asp?submit=Buy&GName=<%=rs("GName")%>">Buy</a>
      <a
href="opr.asp?submit=Delete&GName=<%=rs("GName")%>">Delete</a>
    </th>
  </tr>
<%
  rs.movenext
  Loop
End If
rs.close
```

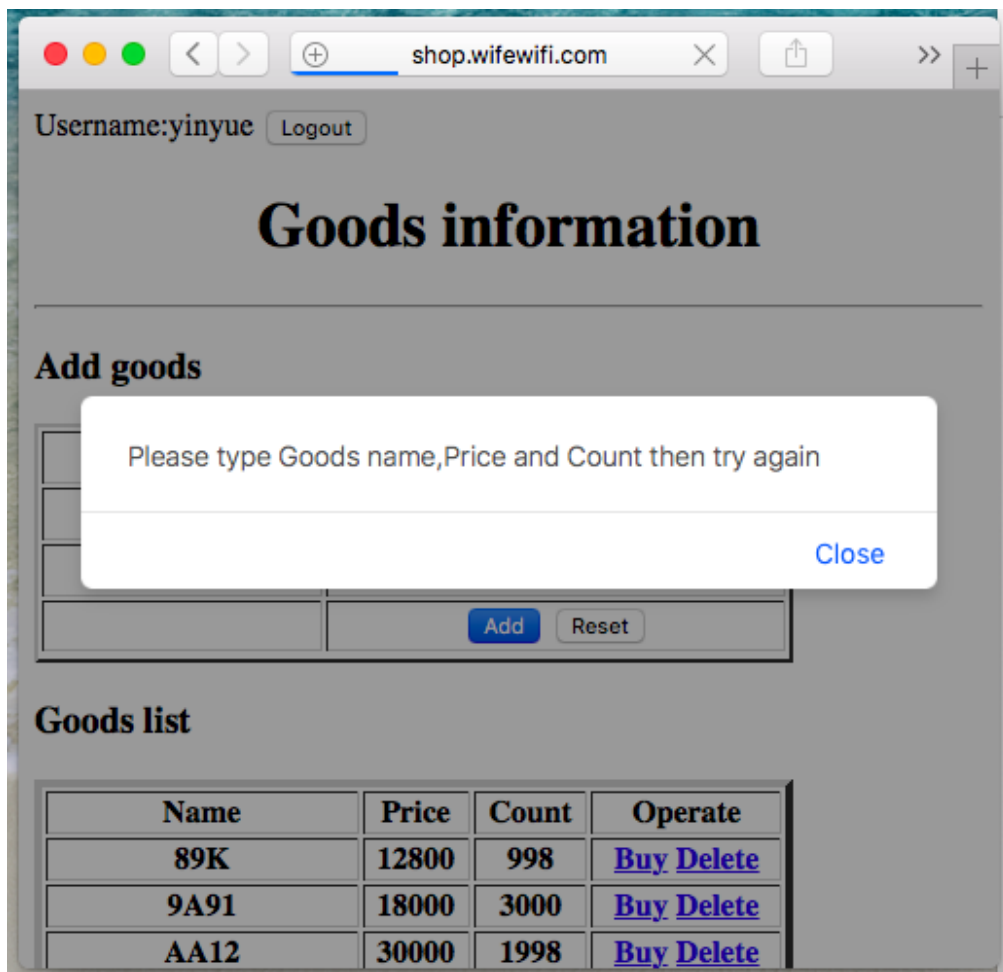
```
%>
```

```
</table>
```

```
</body>
```

```
</html>
```

货物管理功能模块：login/opr.asp



```
<!--#include file="../conn.asp"-->
```

```
<%
```

```
Dim Name,GPrice,GCount,submit
```

```
submit=Trim(Request("submit"))
```

```
If submit="Add" Then
```



```
GName=Trim(Request("GName"))
GPrice=Trim(Request("GPrice"))
GCount=Trim(Request("GCount"))
Response.write GName&GPrice&GCount
If GName <> "" and GPrice <> "" and GCount <> "" Then
    strSql="select * from goods where GName='"&GName&"'"
    Set rs=server.CreateObject("adodb.recordset")
    rs.open strSql,conn,1,1
    If rs.eof Or rs.bof Then
        strSql="insert Into goods(GName,GPrice,GCount) Values
('"&GName&"','"&GPrice&"','"&GCount&"')
        Set rs=server.CreateObject("adodb.recordset")
        rs.open strSql,conn,1,1
        Response.write "<script
LANGUAGE=javascript>alert('Add
successfully!');history.go(-1);window.location.reload()</script>"
        Response.End
    Else
        Response.write "<script
LANGUAGE=javascript>alert('Goods name exists!');history.go(-1)</script>"
        Response.End
    End If
    Response.End
Else
    Response.write "<script LANGUAGE=javascript>alert('Please
type Goods name,Price and Count then try again');history.go(-1)</script>"
    End If
ElseIf submit="Buy" Then
    GName=Trim(Request("GName"))
    strSql="update goods set GCount=GCount-1 where
```

```
GName=""&GName&""
    Set rs=server.CreateObject("adodb.recordset")
    rs.open strSql,conn,1,1
    Response.write "<script LANGUAGE='javascript'>alert('Buy
successfully!');history.go(-1);window.location.reload()</script>"
    ElseIf submit="Delete" Then
        GName=Trim(Request("GName"))
        strSql="delete from goods where GName=""&GName&""
        Set rs=server.CreateObject("adodb.recordset")
        rs.open strSql,conn,1,1
        Response.write "<script LANGUAGE='javascript'>alert('Delete
successfully!');history.go(-1);window.location.reload()</script>"
    End If
%>
```

实验 2： 学习电子商务安全实验（4 学时）

本次实验的主要目的和内容：

1. 掌握电子商务数据加密与数字签名技术，掌握上网下载 PGP 电子邮件软件加密技术思想，写出工作流程。
2. 自己设计一种加密算法完成文本或图像数据的加、解密实验。

实 验 报 告 2

一、需求分析、程序数据流与功能图

PGP 加密流程：

1. 数字签名：

发送者生成签名：

- （1）发送者形成一个消息
- （2）pgp 采用 mds 算法派生消息的 128bit 三列码；
- （3）发送者规定此次操作所采用的秘密密钥，且提供一密语，以此启动 pgp 解密发送者的秘密密钥；
- （4）pgp 用发送者的秘密密钥采用 rsa 算法加密散列码，将结果附到该消息。对应发送者的公钥的密钥 id 附到签名后。

接受者认证签名：

- （1） pgp 取附到签名后的密钥 id，以此从公开密钥环上提取正确的公开密钥
- （2） pgp 用发送者的公钥采用 rsa 算法解密，回复散列码
- （3） pgp 将此消息派生出散列码与解密的散列码比较，若两者一直，消息得到确认予以接收。

2. 消息加密

pgp 提供的密钥仅使用一次，每次随机产生一组 128bit 的随机数作为密钥，密钥使用接受者公开的 rsa 算法加密。

发送者

- （1） pgp 产生 128bit 随机数，仅做这次消息的密钥
- （2） pgp 以此消息密钥采用 idea 算法对消息加密

- (3) pgp 以接收者的公开密钥采用 rsa 算法加密消息密钥，将结果附到消息后。接受者用公开密钥 id 附到已加密的消息密钥之后

接收者：

- (1) pgp 取得附加的消息密钥 ID, 从秘密密钥中提取正确的秘密密钥
- (2) 接受者提供密语，以启动 pgp 解密者的秘密密钥
- (3) pgp 用上面的密钥，采用 rsa 算法解密并回复消息密钥
- (4) pgp 用上面的密钥采用 idea 算法解密消息

对统一消息采用两种密码服务, 对原文消息产生数字签名附加到消息后面, 对压缩后, 对已压缩的原文和签名利用 idea 算法进行加密, 且消息密钥用 rsa 加密。

- 1. 需求分析
加密过程

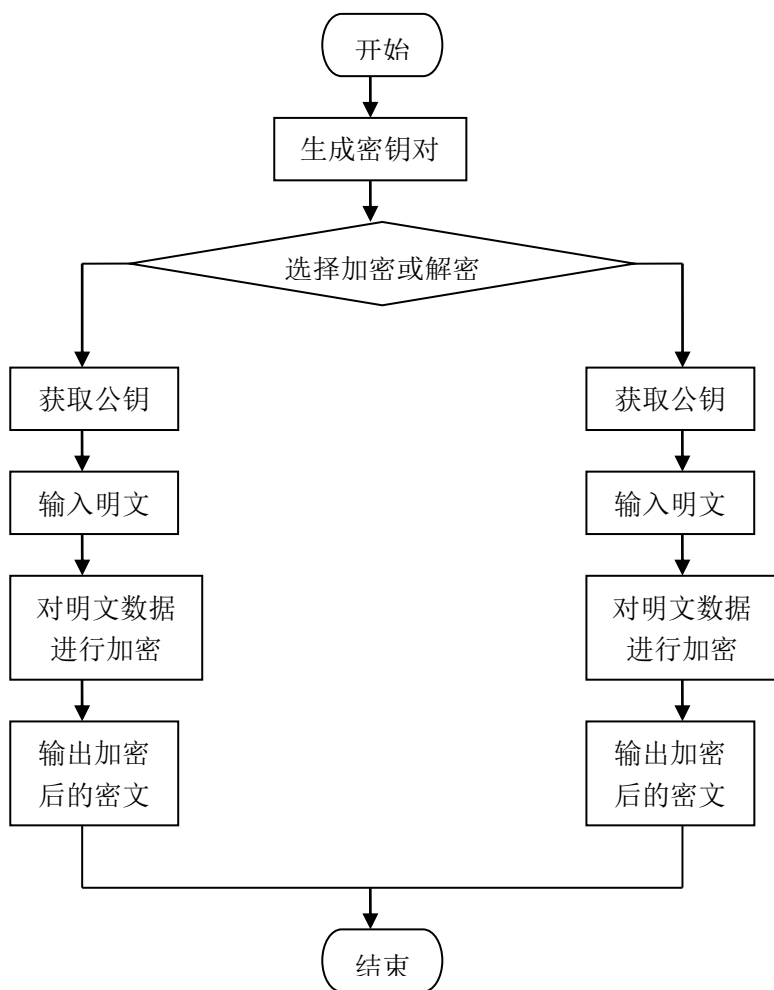


图 1 加解密流程图

程序数据流

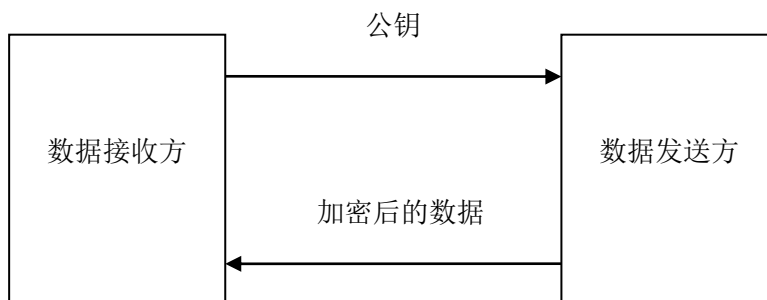


图 2 程序数据流

加密原理

$$\text{明文} = \text{密文}^D \pmod{N}$$

也就是说对密文进行D次方后除以N的余数就是明文，这就是RSA解密过程。知道D和N就能进行解密密文了，所以D和N的组合就是私钥

$$\text{私钥} = (D, N)$$

从上述可以看出RSA的加密方式和解密方式是相同的

加密是求“E次方的mod N”;解密是求“D次方的mod N”

E是加密(Encryption)的首字母

D是解密 (Decryption) 的首字母

N是数字 (Number) 的首字母。

公钥	(E, N)
私钥	(D, N)
密钥对	(E, D, N)
加密	密文 = 明文 ^E mod N
解密	明文 = 密文 ^D mod N

表一 密钥对和加密流程

生成密钥对

公钥是 (E, N)，私钥是 (D, N) 所以密钥对即为 (E, D, N)

密钥对生成步骤如下：

->求N

->求L (L为中间过程的中间数)

->求E

->求D

1.求N

准备两个质数p, q。这两个数不能太小, 太小则会容易破解, 将p乘以q就是N

$$N=p*q$$

2.求L

L 是 $p-1$ 和 $q-1$ 的最小公倍数, 可用如下表达式表示 $L=\text{lcm}(p-1, q-1)$

3.求D

数D是由数E计算出来的。D、E和L之间必须满足以下关系:

$$1 < D < L$$

$$E * D \bmod L = 1$$

只要D满足上述2个条件, 则通过E和N进行加密的密文就可以用D和N进行解密。

简单地说条件2是为了保证密文解密后的数据就是明文。

现在私钥自然也已经生成了, 密钥对也就自然生成了。

4.求N

$$N = p * q ; p, q \text{ 为质数}$$

求 $L = \text{lcm}(p-1, q-1)$; L为 $p-1$ 、 $q-1$ 的最小公倍数

求E $1 < E < L$, $\text{gcd}(E, L) = 1$; E, L最大公约数为1 (E和L互质)

求D $1 < D < L$, $E * D \bmod L = 1$

具体实践：

5.1 求N

我们准备两个很小对质数，

$$p = 17$$

$$q = 19$$

$$N = p * q = 323$$

5.2 求L

$$L = \text{lcm}(p-1, q-1) = \text{lcm}(16, 18) = 144$$

144为16和18对最小公倍数

5.3 求E

求E必须要满足2个条件： $1 < E < L$ ， $\text{gcd}(E, L) = 1$

即 $1 < E < 144$ ， $\text{gcd}(E, 144) = 1$

E和144互为质数，5显然满足上述2个条件

故 $E = 5$

此时公钥 $= (E, N) = (5, 323)$

5.4 求D

求D也必须满足2个条件： $1 < D < L$ ， $E * D \bmod L = 1$

即 $1 < D < 144$ ， $5 * D \bmod 144 = 1$

显然当 $D = 29$ 时满足上述两个条件

$$1 < 29 < 144$$

$$5 * 29 \bmod 144 = 145 \bmod 144 = 1$$

此时私钥 $= (D, N) = (29, 323)$

5.5 加密

准备的明文必须时小于N的数，因为加密或者解密都要mod N其结果必须小于N

假设明文 = 123

则

$$\text{密文} = \text{明文}^E \bmod N = 123^5 \bmod 323 = 225$$

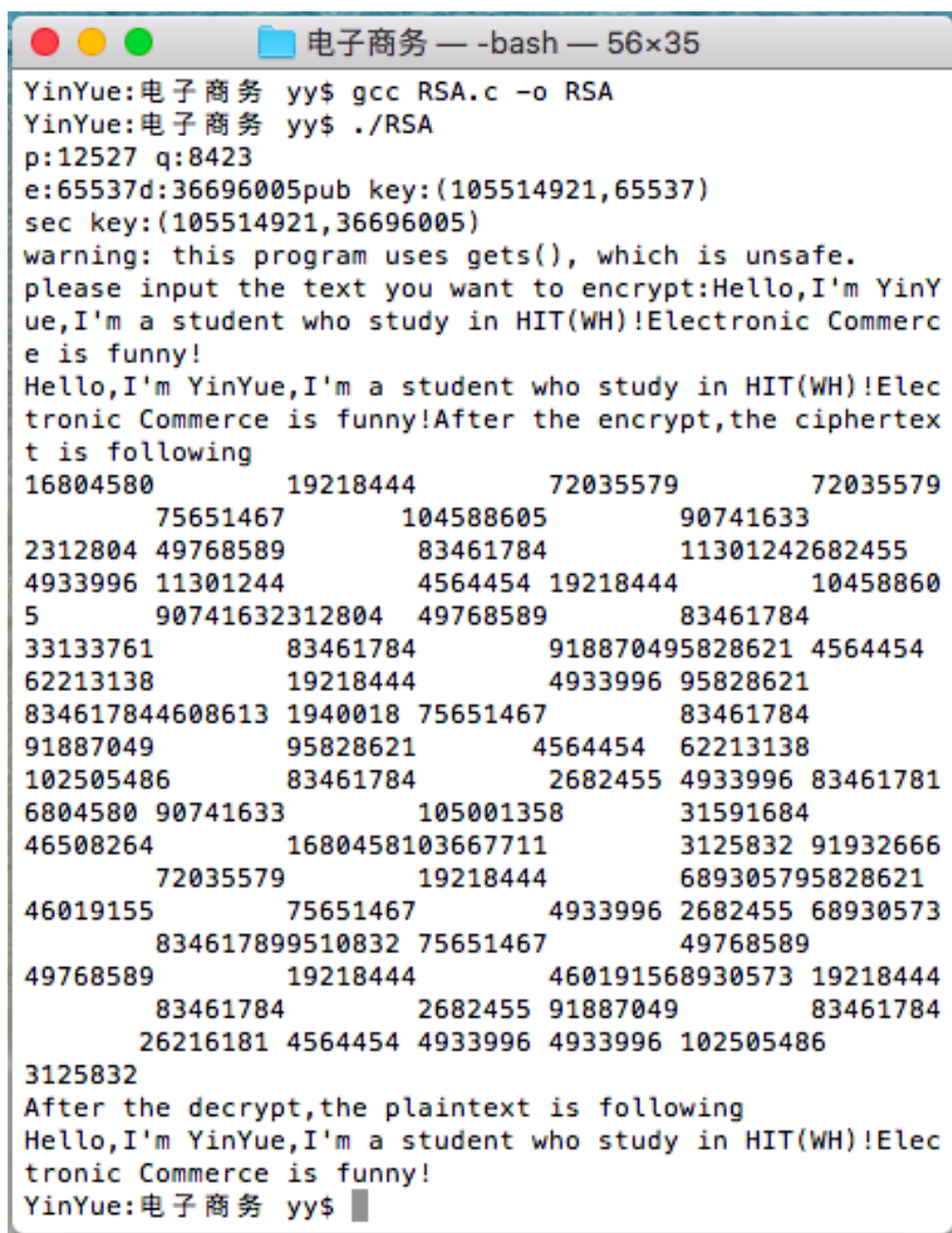
5.6 解密

$$\text{明文} = \text{密文}^D \bmod N = 225^{29} \bmod 323 = 123$$

解密后的明文为123。

二. 程序源代码及结果

程序截图：



```

YinYue:电子商务 yy$ gcc RSA.c -o RSA
YinYue:电子商务 yy$ ./RSA
p:12527 q:8423
e:65537d:36696005pub key:(105514921,65537)
sec key:(105514921,36696005)
warning: this program uses gets(), which is unsafe.
please input the text you want to encrypt:Hello,I'm YinY
ue,I'm a student who study in HIT(WH)!Electronic Commere
is funny!
Hello,I'm YinYue,I'm a student who study in HIT(WH)!Elec
tronic Commerce is funny!After the encrypt,the ciphertex
t is following
16804580      19218444      72035579      72035579
      75651467      104588605      90741633
2312804 49768589      83461784      11301242682455
4933996 11301244      4564454 19218444      10458860
5      90741632312804 49768589      83461784
33133761      83461784      918870495828621 4564454
62213138      19218444      4933996 95828621
834617844608613 1940018 75651467      83461784
91887049      95828621      4564454 62213138
102505486      83461784      2682455 4933996 83461781
6804580 90741633      105001358      31591684
46508264      1680458103667711      3125832 91932666
      72035579      19218444      689305795828621
46019155      75651467      4933996 2682455 68930573
      834617899510832 75651467      49768589
49768589      19218444      460191568930573 19218444
      83461784      2682455 91887049      83461784
      26216181 4564454 4933996 4933996 102505486
3125832
After the decrypt,the plaintext is following
Hello,I'm YinYue,I'm a student who study in HIT(WH)!Elec
tronic Commerce is funny!
YinYue:电子商务 yy$

```

图 3 加解密过程展示

```

#include <stdio.h>
#include <stdlib.h>
#include <time.h>

```

为了保证计算不会越界，计算时采用无符号 long long 型，长度为 64 位

```
typedef unsigned long long ull;
```

gcd 用于计算两个数的最大公约数，这里采用欧几里得的辗转相除法。

辗转相除法就是把上一轮有余数的除法计算中，除数变为下一轮计算的被除数，余数变为下一轮计算的除数，一直这样计算下去，直到最后一次计算余数为零，在最后一轮计算中的被除数，即为所求的最大公约数。

举例： 105 和 85 的最大公约数

第一轮计算 $105 \div 85 = 1 \dots 20$

第二轮计算 $85 \div 20 = 4 \dots 5$

第三轮计算 $20 \div 5 = 4$

第三轮没有余数，因此 105 和 85 的最大公约数就是第三轮计算的被除数 5。

```
ull gcd(ull a,ull b){  
    int t;  
    while(b){  
        t=a;  
        a=b;  
        b=t%b;  
    }  
    return a;  
}
```

产生密钥对

```
void generateKey(ull p,ull q,ull* e,ull* d){
```

产生公钥:

在这里, e 任意取, 但是需要满足 e 和 $(p-1) * (q-1)$ 的最大公因数为 1

```
//generatePubKey
```

```
int r;
```

```
(*e)=2;
```

```
r=(p-1)*(q-1);
```

```
(*e)=65537;
```

```
while((*e)<1||(*e)>r||gcd((*e),r)!=1){
```

```
    (*e)++;
```

当 e 等于 -1 是说明 e 已经达到最大值溢出

```
    if((*e)==-1){
```

```
        printf("error,can't find e,overflow\n");
```

```
        return;
```

```
    }
```

```
}
```

```
printf("e:%llu",*e);
```

产生私钥:

在这里, d 需要满足 e 乘 d 除以 r 的余数为 1

```
//generateSecKey
```

```
*d=1;
```

```
while((*e)*(*d)%r!=1){
```

```
    *d=rand()%r;
```

```
    //(*d)++;
```

```
    //printf("d:%llu",*d);
```

当 d 等于-1 是说明 e 已经达到最大值溢出

```
        if((*d)==-1){
            printf("error,can't find b,overflow\n");
            return;
        }
    }
    printf("d:%llu",*d);
}
/*
```

```
ull MulMod(ull a,ull b,ull mod){
    int num1[64],num2[64],res[128];
    int opr1,opr2,i;
    ull o1,o2;
    for(opr1=0,opr2=0;opr1<64;opr1++){
        num1[opr1]=0;
        num2[opr1]=0;
        res[opr2++]=0;
        res[opr2+0
    o1=1;o2=1;
    for(opr1=0;opr1<64;opr1++){
        num1[opr1]=(a&o1)?1:0;
        o1<<=1;
    }
    for(opr2=0;opr2<64;opr2++){
        num2[opr2]=(a&o2)?1:0;
        o2<<=1;
    }
    for(opr1=0;opr1<64;opr1++){
        for(opr2=0;opr2<64;opr2++){
            if(num1[opr1]&num2[opr2])
```

```
        res[opr1+opr2-1]++;
    }
    for(i=0;i<128;i++){
        if(res[i]>1){
            res[i]=0;res[i+1]++;
        }
    }
}

o2=1;
for(i=0;i<64;i++){
    if(res[i])
        o1+=o2;
    o2<<=1;
}
return o1;
}
*/
/*
ull powAndMod(ull x,ull m,ull mod){
    ull y;
    y=1;
    while(m!=0){
        if(m%2==1){
            y=(x*y)%mod;
            m--;
        }else{
            x=(x*x)%mod;
            m/=2;
        }
    }
}
```

```

    }
    return y;
}
*/

```

快速指数求余

朴素模幂运算是非常的无法容忍的，模运算是非常的消耗内存资源的，在计算的次数非常的大时，我们是没办法忍受这种时间耗费的

$(a*b)\%c=(a\%c)*(b\%c)\%c$ 这个是成立的，也是我们实现快速幂的基础

对于任何一个整数的模幂运算 $a^b\%c$

对于 b 我们可以拆成二进制的形式 $b=b_0+b_1*2+b_2*2^2+\dots+b_n*2^n$

这里我们的 b_0 对应的是 b 二进制的第一位

那么我们的 a^b 运算就可以拆解成

$a^{b_0}*a^{b_1*2}*\dots*a^{(b_n*2^n)}$

对于 b 来说，二进制位不是 0 就是 1，那么对于 b_x 为 0 的项我们的计算结果是 1 就不用考虑了，我们真正想要的其实是 b 的非 0 二进制位

那么假设除去了 b 的 0 的二进制位之后我们得到的式子是

$a^{(b_x*2^x)}*\dots*a^{(b_n*2^n)}$

这里我们再应用我们一开始提到的公式，那么我们的 $a^b\%c$ 运算就可以转化为

$(a^{(b_x*2^x)\%c})*\dots*(a^{(b_n*2^n)\%c})$

```

ull quickMod(ull a,ull b,ull mod){

```

```

    //a^10%c=a^(1*2^3+0*2^2+1*2^1+0*2^0)%c=((a^(2^3)%c)*(a^(2^1)%c
))%c

```

```

    ull aus=1;

```

```

    while(b){

```

```

        if(b&0x1)

```

```

            aus=aus*a%mod;

```

```

        a=a*a%mod;
    }
}

```

```

    b>=1;
}
return aus;
}

```

欧拉定理:

对于和 m 互素的 x , 有 $x^{\varphi(m)} \equiv 1 \pmod{m}$

证明:

设所有 n 以下和 n 互质的数依次为 $X_1, X_2, \dots, X_{\varphi(n)}$

设 k 为一个与 n 互质的数, 那么设 $A = \{kX_1, kX_2, \dots, kX_{\varphi(n)}\}$

那么 A 中没有两个数模 n 同余

证明: 假设 $ak \equiv bk \pmod{n}$

那么有 $ak - bk = nq$, 即 $(a-b)k = nq$, 所以左式模 n 为 0

然而 k 与 n 互质, $1 < (a-b) < n$, 所以 $(a-b)$ 也模 n 不等于 0

那么显然上式不成立

得证

A 中所有数的余数都与 n 互质

证明: 假设 $\gcd(kX_i \bmod n, n) = r$

那么 $kX_i = nq + pr$

那么 kX_i 也有因子 r , 那么 kX_i 与 n 不互质, 显然不可能

得证

那么由以上两个结论可知 A 中的数模 n 的余数应该与 $X_1, X_2, \dots, X_{\varphi(n)}$ 唯一对应。

即 $X_1 * X_2 * \dots * X_{\varphi(n)} \equiv kX_1 * kX_2 * \dots * kX_{\varphi(n)} \pmod{n}$

也就是说 $0 \equiv (k^{\varphi(n)} - 1) * X_1 * X_2 * \dots * X_{\varphi(n)} \pmod{n}$

显然 $X_1 * X_2 * \dots * X_{\varphi(n)}$ 是与 n 互质的, 所以 $k^{\varphi(n)} - 1 \equiv 0 \pmod{n}$

$k^{\varphi(n)} \equiv 1 \pmod{n}$

得证

费马小定理:

特别的，当 p 为素数时， x 无法被 p 整除， $\phi(p)=p-1$ ，于是便有费马小定理 $X^{p-1} \equiv 1 \pmod{p}$

在 p 是素数时，对任意正整数 x 都有 $X^p \equiv X \pmod{p}$

于是对于 a 的逆元 x ，有 $ax \equiv 1 \pmod{m}$ ，对于 a, m 互素且 m 为素数时，有 $x = a^{m-2}$ ，于是我们可以通过快速幂快速求出 a 的逆元。

另外，借助素数筛，我们还可以很快的求出 $1-n$ 的欧拉函数值。每当我们找到一个素数，就把他的倍数的欧拉函数值乘上 $(p-1)/p$ 。

而且，借助费马小定理我们可以实现对除法取模。

```
int fermatPrime(ull num){
    //a^(n-1)=1(mod n)
    int i;
    for(i=0;i<5;i++){
        if(quickMod(1+rand()%(num-1),num-1,num)!=1)
            break;
    }
    if(i==5)return 1;
    return 0;
}
```

```
void generateBigPrime(ull* p,ull* q){
    int i;
    ull temp;
    srand((unsigned)time(NULL));
    do{
        *p=0;
        for(i=0;i<1;i++){
            temp=rand()%65535;
            temp<<=16*i;
            *p|=temp;
        }
    } while(*p==0);
}
```

```
    }  
//    printf("p:%llu\tq:%llu\n",*p,*q);  
    }while(!fermatPrime(*p));  
  
    do{  
        *q=0;  
        for(i=0;i<1;i++){  
            temp=rand()%65535;  
            temp<<=16*i;  
            *q|=temp;  
        }  
        }while(p==q||!fermatPrime(*q));  
        printf("p:%llu\tq:%llu\n",*p,*q);  
    }
```

加密函数

逐个字节对该数进行加密，执行密文=明文^E(mod N)

```
void enc(char plaintext[],ull ciphertext[],ull n,ull e){  
    int i;  
    for(i=0;plaintext[i]!=0;i++){  
        ciphertext[i]=quickMod((ull)plaintext[i],e,n);  
        printf("%c",plaintext[i]);  
    }  
    ciphertext[i]=0;  
}
```

解密函数

逐个字节对该数进行加密，执行明文=密文^D(mod N)

```
void dec(ull ciphertext[],char plaintext[],ull n,ull d){
    int i;
    for(i=0;ciphertext[i]!=0;i++)
        plaintext[i]=(char)quickMod(ciphertext[i],d,n);
    ciphertext[i]=0;
}
```

打印大数串

```
void printfx(ull ciphertext[]){
    int i;
    for(i=0;ciphertext[i]!=0;i++){
        printf("%llu\t",ciphertext[i]);
    }
    printf("\n");
}
```

```
int main(){
    /* prime p q
    *  $n=p*q$   $r=(p-1)(q-1)$ 
    *  $e < r$   $\gcd(e,r)=1$   $(e*d) \bmod r=1$ 
    * pub key (n,e) sec key (n,d)
    * plaintext A ciphertext B
    *  $A=B^e \pmod n$   $B=A^d \pmod n$ 
    * e d can be exchanged
    */
    ull p=0,q=0;
    ull e,d;
    /*
    p=1725580387;
    q=1816490293;
```

```
e=65537;
d=5685353;
*/
char text[1000];
ull textx[1000];
generateBigPrime(&p,&q);
generateKey(p,q,&e,&d);
//printf("p:%llu\tq:%llu\te:%llu\td:%llu\n",p,q,e,d);

printf("pub key:(%llu,%llu)\nsec key:(%llu,%llu)\n",p*q,e,p*q,d);

printf("please input the text you want to encrypt:");
gets(text);
enc(text,textx,p*q,e);
printf("After the encrypt,the ciphertext is following\n");
printfx(textx);
dec(textx,text,p*q,d);
printf("After the decrypt,the plaintext is following\n");
printf("%s\n",text);
return 0;
}
```

实验 3：电子商务商品购物车和订单生成系统实训编程

（4 学时）

1 掌握 B TO C 电子商务在线购物车和订单支持的功能和生成方法，掌握可实现的功能：

- （1）允许用户在网站搜索选择自己感兴趣的商品
- （2）允许用户在线购买商品并对购物进行管理
- （3）系统自动生成订单处理
- （4）系统能够显示完成整个购物过程

2 可以编程实现电子商务平台部分功能

实 验 报 告 3

一、需求分析、程序数据流与功能图

需求分析

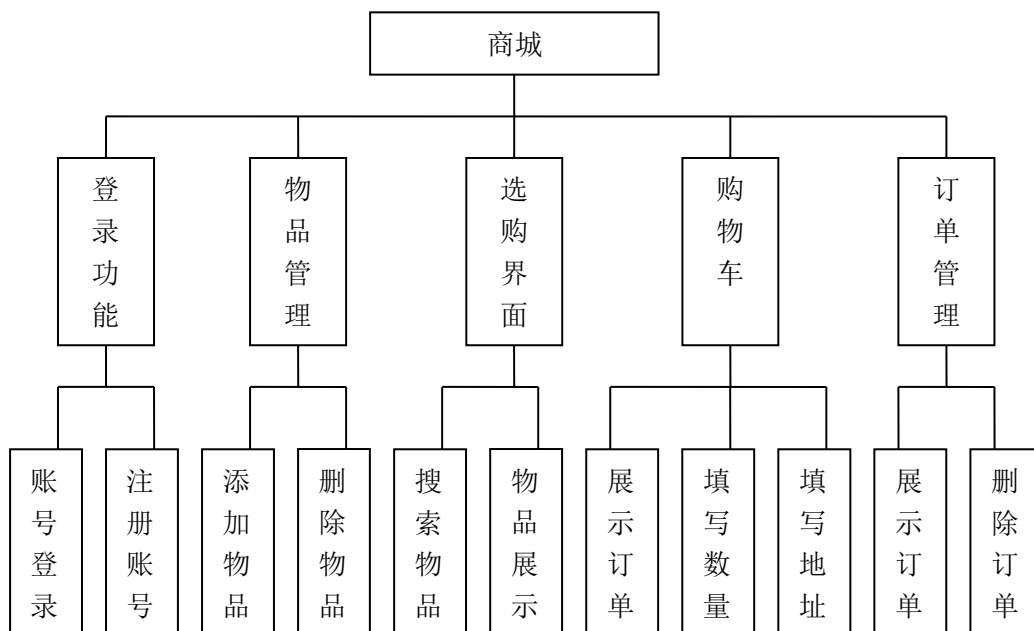


图 1 需求分析

E-R 图

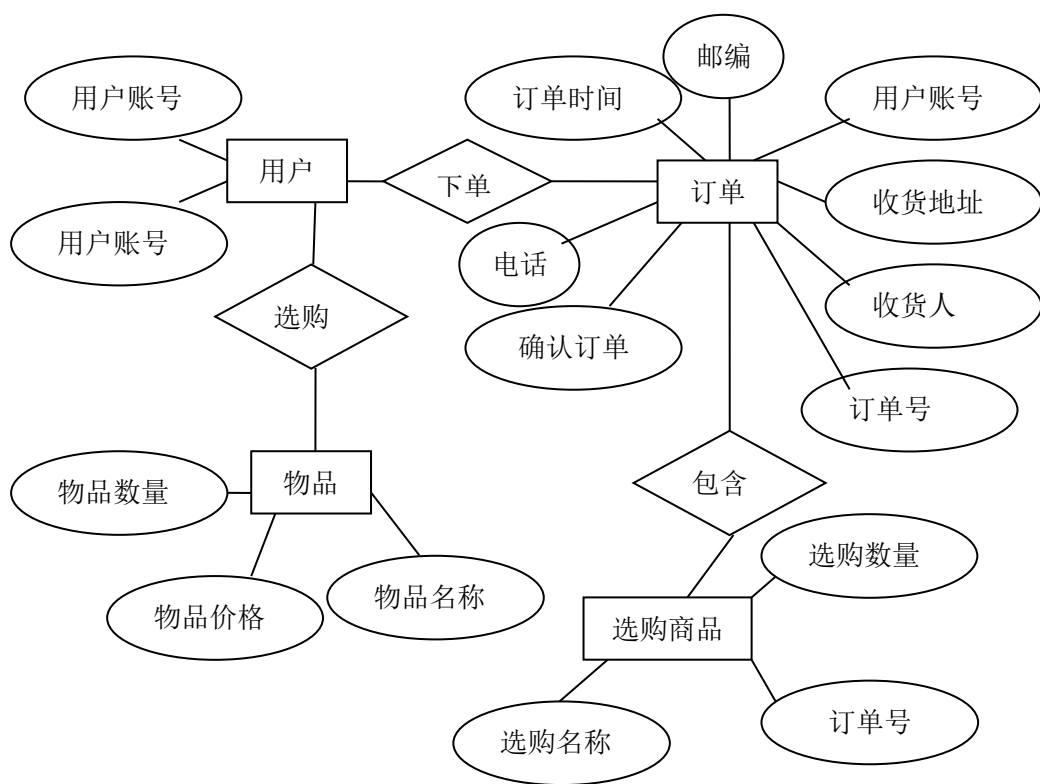


图 2 E-R 图

程序数据流

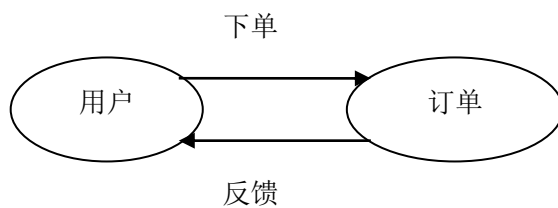


图 3 数据流

功能图

订单流程图

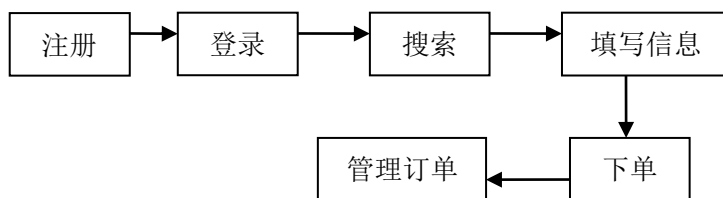


图 4 订单流程图

购物流程图

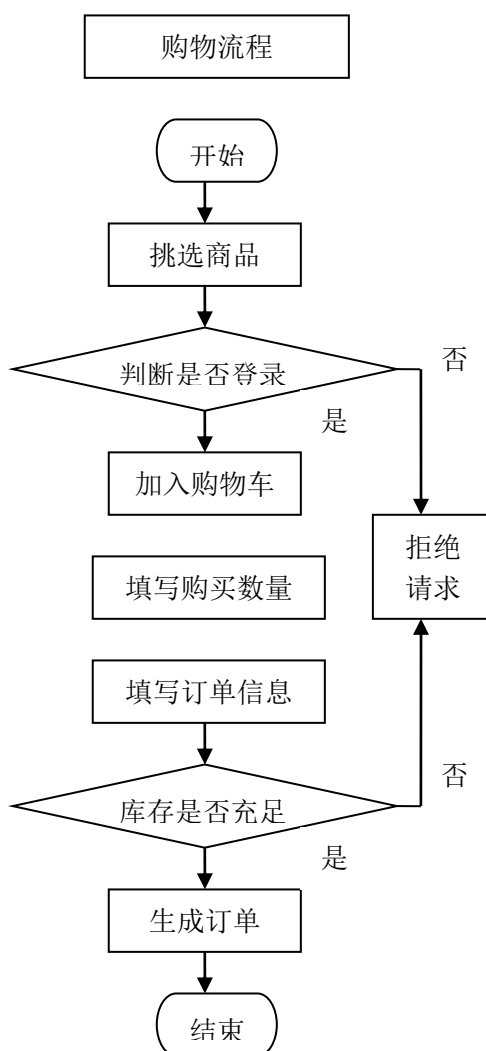


图 5 购物流程图

货物搜索流程图

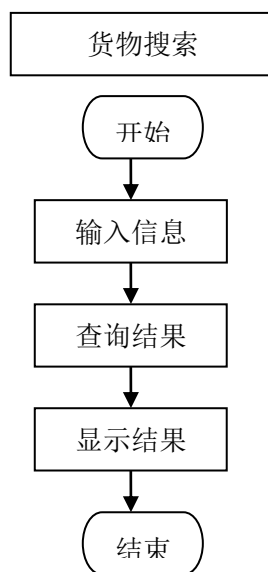


图 6 货物搜索

加货流程图

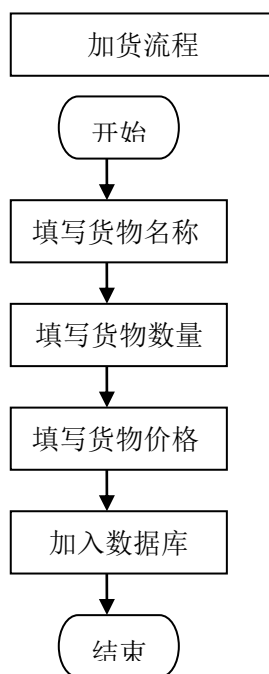


图 7 加货流程

二、 程序源代码及结果

create.sql 数据库创建

--账号表

CREATE TABLE account

```
(  
    username varchar(20) NOT NULL ,  
    password varchar(20) NOT NULL  
);
```

--购物清单表

CREATE TABLE buy

```
(  
    ONum int NOT NULL ,  
    BCount int NULL ,  
    BName varchar(20) NOT NULL  
);
```

--货物表

CREATE TABLE goods

```
(  
    GName varchar(20) NOT NULL ,  
    GPrice float NULL ,  
    GCount int NULL  
);
```

--订单表

CREATE TABLE orders

```
(  
    ONum int NOT NULL ,  
    OTime datetime NULL ,  
    username varchar(20) NOT NULL ,  
    consignee varchar(20) NULL ,
```

```
location varchar(50) NULL ,  
zipcode varchar(20) NULL ,  
tel varchar(20) NULL ,  
cfm int NOT NULL  
);
```

conn.asp 数据库连接

<% '每个 asp 页面都要用，需要连接数据库

```
Set conn=Server.createobject("adodb.connection")
```

```
'conn.Open "test"
```

```
StrConn="driver={SQL
```

```
Server};server=qds167524598.my3w.com;uid=qds167524598;pwd=yinyue12  
3;database=qds167524598_db"
```

```
Conn.open StrConn
```

```
If conn.State <> 1 Then
```

```
Response.write "Faild to connect Sql!"
```

```
Response.End
```

```
End If
```

```
%>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
```

index.asp 选购商品界面及功能模块（首页）

预览页面: <http://shop.wifewifi.com/>



图 8 选购商品

M15	1000	8000	加入购物车
M14EBR	1000	26000	加入购物车
M16	3000	5000	加入购物车
M200	2000	5000	加入购物车
M240B	1000	33000	加入购物车
M249	3000	39000	加入购物车
M37	2295	40000	加入购物车
M4A1	5999	19000	加入购物车
M60	4998	18000	加入购物车
MG3	2992	45000	加入购物车
MP5	1000	8000	加入购物车
P228	1000	6000	加入购物车
QBZ03	1000	23000	加入购物车
QBZ95	3000	26000	加入购物车
RPK	2995	35000	加入购物车
SCAR	1000	23000	加入购物车
SPAS12	1000	16000	加入购物车
Thompson M1921	4000	35000	加入购物车
USP	2998	3000	加入购物车
UZI	1000	8000	加入购物车
Ultimax100	3000	16000	加入购物车
XM1014	3000	20000	加入购物车
XM8	5000	14500	加入购物车

清算

图 9 选购商品

```

<!--#include file="conn.asp"-->
<html>
<head>
<title>殷悦的商城</title>
</head>
<body>

```

```

<p align="right">
  用户:<%Response.write Session("username")%>
  <a href="login">登录</a>
  <a href="?submit=logout">注销</a>
  <a href="">管理</a>
</p>
<% '如果有提交, 就调用页面自身
  Dim submit '判断 GET 类型
  submit=Trim(Request("submit"))
  If submit="logout" Then '退出登录
    Session("username")=""
    Response.write "<script LANGUAGE='javascript'>alert('已经退出登录!');window.location.href='index.asp'</script>"
  ElseIf submit="buy" Then '加入购物车
    If Session("username")="" Then '没登录先登录
      Response.write "<script LANGUAGE='javascript'>alert('未登录, 请先登录!')</script>"
    Else
      Dim GName
      GName=Trim(Request("GName"))
      Dim a,b,c
      '查找数据库里未被确认的订单, 就是购物车里的订单

      strSql="select ONum from orders where cfm=0 and
      username='"&Session("username")&"';"
      Set rs=conn.execute(strSql)
      If rs.eof Or rs.bof Then '如果没有就创建订单
        strSql="select isnull(max(ONum)+1,1) as ONum from
orders" '如果数据库里一个订单也没有, 就用序号 1, 如果有, 就去最大
订单号加一作为订单号, mysql 用 ifnull, sql server 用 isnull

```

```

        Set rs=conn.execute(strSql)
        strSql="insert into orders(ONum,OTime,username,cfm)
values ('"&rs("ONum")&"','"&now()&"','"&Session("username")&"','0')"' 插入
订单号，时间，用户名
        conn.execute(strSql)
    End If
    strSql="select * from buy where ONum='"&rs("ONum")&"'
and BName='"&Request("GName")&"'"判断是否有重名的，避免重复添加
    Set rs2=conn.execute(strSql)
    If rs2.eof Or rs2.bof Then'如果为选购过，就加入选购列表
        strSql="insert into buy(ONum,BName) values
('"&rs("ONum")&"','"&Request("GName")&"')"'插入订单号和选购物品名
    End If
    conn.execute(strSql)
    Response.write "<script LANGUAGE='javascript'>alert('已
加入购入车!')</script>"
    '下面的为当时在 sql server 中的测试语句，可以用但是 mysql 和 sql server
语句大多不通用，所以下面的没有用
    'sql server
    'strSql= "if not exists (select * from orders where
cfm=0 and username='"&Session("username")&"') "
    'strSql=strSql&"begin"
    'strSql=strSql&"declare @a int"
    'strSql=strSql&"select @a=(isnull(max(ONum),0)+1) from
orders where cfm=1 and username='"&Session("username")&"'"
    'strSql=strSql&"insert into
orders(ONum,OTime,username,cfm) "
    'strSql=strSql&"values
(@a,'"&now()&"','"&Session("username")&"','0')"

```

```

'strSql=strSql&"end"
'strSql=strSql&"declare @b int"
'strSql=strSql&"select @b=ONum from orders where cfm=0
and username='"&Session("username")&"'"
'strSql=strSql&"insert into buy(ONum,BName) values
(@b,'"&Session("username")&"'"

```

```

'Response.write strSql
'Set rs=server.CreateObject("adodb.recordset")
'rs.open strSql,conn,1,1
End If
End If
%>
<p align="center">
<a href="index.asp">选择商品</a> ->
<a href="shoppingCart.asp">购物车</a> ->
<a href="order.asp">管理订单</a>
</p>
<p align="center"><font face="隶书" size="5">殷悦的商城</font></p>
<form method="GET" action="">
  <p align="center">
    <input type="text" name="search" size=20></input>
    <input type="submit" value="搜索" name="submit">
  </p>
</form>
<hr>
<p align="center">
  <table border="4" width="80%">
    <tr>
      <th width="25%">商品名</th>

```



```

        <th width="25%">数量</th>
        <th width="25%">价格</th>
        <th width="25%">操作</th>
    </tr>
<%
    Dim search
    search=Trim(Request("search"))
    If search <> "" Then
        strSql="select  GName,GPrice,GCount  from  goods  where
GName='"&search&""'"如果要搜索，就搜索名字
    Else
        strSql="select  GName,GPrice,GCount  from  goods"“如果不搜
索，就展示全部物品
    End If
    Set rs=server.CreateObject("adodb.recordset")
    rs.open strSql,conn,1,1
    If Not rs.eof And Not rs.bof Then
        Do While Not rs.eof'循环显示购物车中的所有物品
%>
    <tr>
        <th><%=rs("GName")%></th>
        <th><%=rs("GCount")%></th>
        <th><%=rs("GPrice")%></th>
        <th>
            <a href="?submit=buy&GName=<%=rs("GName")%>">加
入购物车</a>
        </th>
    </tr>
<%
    rs.movenext

```

```
        Loop
    End If
    rs.close
%>

</table>
</br>
<input                                type="button"
onclick="javascript:top.location='shoppingCart.asp';" value="清算">
    </p>
</body>
</html>
```

shoppingCart.asp 购物车界面及模块

预览地址: <http://shop.wifewifi.com/shoppingCart.asp>

用户:yin_yue [登录](#) [注销](#) [管理](#)

[选择商品](#) -> [购物车](#) -> [管理订单](#)

购物车

订单信息

用户	yin_yue
订单号	14
订单时间	2018-1-1 19:55:58

商品信息

商品名	数量	价格
AK47	<input type="text" value="1"/>	12000
AN94	<input type="text" value="2"/>	26000
M16	<input type="text" value="3"/>	5000
M4A1	<input type="text" value="4"/>	19000
M60	<input type="text" value="5"/>	18000

物流信息

收货人	<input type="text" value="YinYue"/>
收货地址	<input type="text" value="ShanDong,WeiHai,HIT(WH)"/>
邮编	<input type="text" value="264209"/>
电话	<input type="text" value="17863137381"/>

Display a menu

图 10 购物车

```
<!--#include file="conn.asp"-->
```

```
<html>
```

```
<head>
```

```

<title>殷悦的商城</title>
</head>
<body>
    <p align="right">
        用户:<%Response.write Session("username")%>
        <a href="login">登录</a>
        <a href="?submit=logout">注销</a>
        <a href="">管理</a>
    </p>
    <%
        If Session("username")="" Then
            Response.write "<script LANGUAGE='javascript'>alert('未登
录，请先登录!')</script>"
        End If
        Dim submit
        submit=Trim(Request("submit"))
        If submit="logout" Then'将 sesion 置空就退出登录
            Session("username")=""
            Response.write "<script LANGUAGE='javascript'>alert('已经退
出登录!');window.location.href='index.asp'</script>"
        End If
    %>
    <p align="center">
        <a href="index.asp">选择商品</a> ->
        <a href="shoppingCart.asp">购物车</a> ->
        <a href="order.asp">管理订单</a>
    </p>
    <p align="center"><font fane="隶书" size="5">购物车</font></p>
    <hr>
    <%

```

```

If Trim(Request("submit"))<>" " Then'有提交 GET 请求
    strSql="select      ONum      from      orders      where
username='"&Session("username")&" and cfm=0"'找到购物车的订单号，
cfm 字段为 0 说明没提交订单，就是购物车啦
    Set rs=conn.execute(strSql)
    strSql="update      orders      set
consignee='"&Request("consignee")&"',location='"&Request("location")&"',z
ipcode='"&Request("zipcode")&"',tel='"&Request("tel")&"      where
ONum='"&rs("ONum")&"'"提交后将收货人，收货地址，邮编，电话存入
对应的订单号
    Set rs2=conn.execute(strSql)
    strSql="select BName,GCount from buy left join goods on
buy.BName=goods.GName where ONum='"&rs("ONum")&"'"左连数据库
货物，获得物品价格和库存量
    Set rs3=conn.execute(strSql)
    If Not rs3.eof And Not rs3.bof Then
        Do While Not rs3.eof
            'Response.write
Request(rs3("BName"))&rs3("GCount")
            If CInt(Request(rs3("BName")))>=CInt(rs3("GCount"))
Then'如果购买的数量超过库存量，就报库存不足错误
                Response.write "<script
LANGUAGE='javascript'>alert(' 库存 不 足 ， 请 重 新 选 择 货 物 数 量
');history.go(-1)</script>"
                Response.End
            End If
            rs3.movenext
        Loop
    End If
    rs3.close

```

```

        strSql="select      BName      from      buy      where
ONum=""&rs("ONum")&""
        Set rs2=conn.execute(strSql)
        If Not rs2.eof And Not rs2.bof Then
            Do While Not rs2.eof
                strSql="update                buy                set
BCount=""&Request(rs2("BName"))&"" where ONum=""&rs("ONum")&""
and BName=""&rs2("BName")&""
                conn.execute(strSql)
                strSql="update                goods                set
GCount=GCount-""&Request(rs2("BName"))&"" where
GName=""&rs2("BName")&""'购买后，物品表的剩余数量就减掉购买量
                'Response.write strSql
                'Response.End
                conn.execute(strSql)
                rs2.movenext
            Loop
        End If
        strSql="update      orders      set      cfm=1      where
ONum=""&rs("ONum")&""'将订单确认设为 1 表示已经确认的订单
        Set rs2=conn.execute(strSql)
        rs.close
        Response.write "<script LANGUAGE='javascript'>alert('已生成
订单!)</script>"
    End If
%>
<form>
<p align="center">
    订单信息
    <table border="2" width="80%">

```

```

        <tr>
            <th width="40%">用户</th>
            <th
                width="60%"><%Response.write
Session("username")%></th>
        </tr>
        <tr>
            <th width="40%">订单号</th>
            <th width="60%">
                <%
                    strSql="select  ONum,OTime  from  orders  where
username='"&Session("username")&"' and cfm=0"
                    Set rs=conn.execute(strSql)
                    If rs.eof Or rs.bof Then
                        Response.write "购物车为空,请先选择商品"
                        Response.end
                    Else
                        Response.write rs("ONum")
                    End If
                %>
            </th>
        </tr>
        <tr>
            <th width="40%">订单时间</th>
            <th width="60%"><%=rs("OTime")%></th>
        </tr>
    </table>
    商品信息
    <table border="3" width="80%">
        <tr>
            <th width="40%">商品名</th>

```

```

        <th width="30%">数量</th>
        <th width="30%">价格</th>
    </tr>
<%
    strSql="select BName,GPrice from buy left join goods on
buy.BName=goods.GName where ONum='"&rs("ONum")&""'"左连货物，获
取货物价格
    Set rs2=conn.execute(strSql)
    If Not rs2.eof And Not rs2.bof Then
        Do While Not rs2.eof
%>
        <tr>
            <th><%=rs2("BName")%></th>
            <th><input type="text" name=<%=rs2("BName")%>
size=10></input></th>
            <th><%=rs2("GPrice")%></th>
        </tr>
<%
        rs2.movenext
        Loop
    End If
    rs.close
    rs2.close
%>
</table>
物流信息
<table border="2" width="80%">
    <tr>
        <th width="40%">收货人</th>
        <th width="60%"><input type="text" name="consignee"

```



```
size=20></th>
    </tr>
    <tr>
        <th width="40%">收货地址</th>
        <th width="60%"><input type="text" name="location"
size=20></th>
    </tr>
    <tr>
        <th width="40%">邮编</th>
        <th width="60%"><input type="text" name="zipcode"
size=20></th>
    </tr>
    <tr>
        <th width="40%">电话</th>
        <th width="60%"><input type="text" name="tel"
size=20></th>
    </tr>
</table>
<br>
<input type="submit" value="生成订单" name="submit">
<input type="button" onclick="javascript:top.location='order.asp';"
value="查看清单">
</p>
</form>
</body>
</html>
```

order.asp 订单界面

演示地址: <http://shop.wifewifi.com/order.asp>



图 11 订单管理

shop.wifewifi.com

收货人	YinXiansheng
收货地址	BeiJing,GuGong
邮编	100000
电话	110

删除订单

订单信息

用户	yin_yue
订单号	14
订单时间	2018-1-1 19:55:58
总价	245000

商品信息

商品名	数量	价格
AK47	1	12000
AN94	2	26000
M16	3	5000
M4A1	4	19000
M60	5	18000

物流信息

收货人	YinYue
收货地址	ShanDong,WeiHai,HIT(WH)
邮编	264209
电话	17863137381

删除订单

Display a menu

图 12 订单管理

```
<!--#include file="conn.asp"-->
<html>
<head>
<title>殷悦的商城</title>
</head>
<body>
  <p align="right">
    用户:<%Response.write Session("username")%>
    <a href="login">登录</a>
    <a href="?submit=logout">注销</a>
    <a href="">管理</a>
  </p>
  <%
    If Session("username")="" Then
      Response.write "<script LANGUAGE='javascript'>alert('未登
录, 请先登录!)</script>"
    End If
    Dim submit
    submit=Trim(Request("submit"))
    If submit="logout" Then
      Session("username")=""
      Response.write "<script LANGUAGE='javascript'>alert('已经退
出登录!');window.location.href='index.asp'</script>"
    End If
  %>
  <p align="center">
    <a href="index.asp">选择商品</a> ->
    <a href="shoppingCart.asp">购物车</a> ->
    <a href="order.asp">管理订单</a>
  </p>
```

```

<p align="center"><font face="隶书" size="5">管理订单</font></p>
<hr>
<%
    If Trim(Request("del"))<>" " Then'提交删除订单
        strSql="select      ONum      from      orders      where
username=""&Session("username")&"      and      cfm=1      and
ONum=""&Request("del")&"'"判断确实是该用户的订单才让删除，其他用户
没有删除该订单的权限，防止通过 GET 删除别人的订单
        Set rs=conn.execute(strSql)
        strSql="delete from orders where ONum=""&rs("ONum")&"'"
删除订单
        'Response.write strSql
        Set rs2=conn.execute(strSql)
        strSql="delete from buy where ONum=""&rs("ONum")&"'"删除
除货物
        Set rs2=conn.execute(strSql)
        'Response.write strSql
        'Response.End
        rs.close
    End If
%>
<p align="center">
<%
    strSql="select  ONum,OTime,consignee,location,zipcode,tel  from
orders where username=""&Session("username")&" and cfm=1 order by
ONum desc"
    Set rs=conn.execute(strSql)
    If rs.eof Or rs.bof Then
        Response.write "暂无提交的订单"

```

```

        Response.End
    Else
        Do While Not rs.eof
%>
</p>
<p align="center">
    订单信息
    <table border="2" width="80%">
        <tr>
            <th width="40%">用户</th>
            <th
                                width="60%"><% Response.write
Session("username")%></th>
        </tr>
        <tr>
            <th width="40%">订单号</th>
            <th width="60%"><%=rs("ONum")%></th>
        </tr>
        <tr>
            <th width="40%">订单时间</th>
            <th width="60%"><%=rs("OTime")%></th>
        </tr>
        <tr>
            <th width="40%">总价</th>
            <th width="60%">
                <%
                    strSql="select sum(BCount*GPrice) as total from buy
left    join    goods    on    buy.BName=goods.GName    where
ONum='"&rs("ONum")&"'"
                    Set rs2=conn.execute(strSql)
                    Response.write rs2("total")
                %></th>

```

```
</table>
```

商品信息

```
<table border="3" width="80%">
```

```
<tr>
```

```
<th width="40%">商品名</th>
```

```
<th width="30%">数量</th>
```

```
<th width="30%">价格</th>
```

```
</tr>
```

```
<%
```

```
    strSql="select BName,BCount,GPrice from buy left join goods on  
buy.BName=goods.GName where ONum='"&rs("ONum")&"'"
```

```
    Set rs2=conn.execute(strSql)
```

```
    If Not rs2.eof And Not rs2.bof Then
```

```
        Do While Not rs2.eof
```

```
%>
```

```
<tr>
```

```
<th><%=rs2("BName")%></th>
```

```
<th><%=rs2("BCount")%></th>
```

```
<th><%=rs2("GPrice")%></th>
```

```
</tr>
```

```
<%
```

```
    rs2.movenext
```

```
    Loop
```

```
End If
```

```
%>
```

```
</table>
```

物流信息

```
<table border="2" width="80%">
```

```
<tr>
```

```
<th width="40%">收货人</th>
```

```

        <th width="60%"><%=rs("consignee")%></th>
    </tr>
    <tr>
        <th width="40%">收货地址</th>
        <th width="60%"><%=rs("location")%></th>
    </tr>
    <tr>
        <th width="40%">邮编</th>
        <th width="60%"><%=rs("zipcode")%></th>
    </tr>
    <tr>
        <th width="40%">电话</th>
        <th width="60%"><%=rs("tel")%></th>
    </tr>
</table>

<br>
<input type="button"
onclick="javascript:top.location='?del=<%=rs("ONum")%>';" value="删除订
单">

<%
    rs.movenext
    rs2.close
%>
<hr>
<%
Loop
End If
rs.close
%>

```


</p>

</body>

</html>