**华 中 科 技 大 学**

**研究生课程考试答题本**

考生姓名 彭克超

考生学号 M201773169

系、年级 计算机科学与技术硕17级

类 别 全日制专业硕士

考试科目 密码学与访问控制理论

考试日期 2017年11月24日

评 分

|  |  |  |  |
| --- | --- | --- | --- |
| 题号 | 得分 | 题号 | 得分 |
| 1 |  | 9 |  |
| 2 |  | 10 |  |
| 3 |  | 11 |  |
| 4 |  | 12 |  |
| 5 |  | 13 |  |
| 6 |  | 14 |  |
| 7 |  | 15 |  |
| 8 |  | 16 |  |

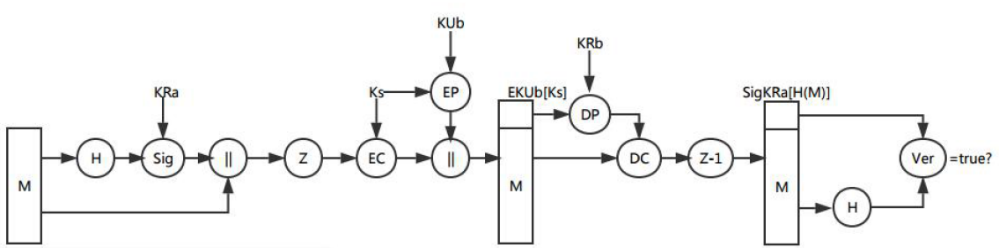
|  |  |
| --- | --- |
| 总分： | 评卷人： |

注：1.无评卷人签名试卷无效。

2.必须用钢笔或圆珠笔阅卷，使用红色，用铅笔阅卷无效。

1. **试利用公钥密码、对称密码、散列函数和压缩函数，设计一个具有压缩、加密、数据鉴别和数字签名功能的数字信封。(6分)**

解：设计的数字信封如下图所示：



H：散列函数，EP：RSA加密，DP：RSA解密，Z：压缩，Z-1：解压缩，EC：对称加密，DC：对称解密，Ks：随机会话密钥，KUa：a的公钥，KUb：b的公钥， KRa：a的密钥，KRb：b的密钥。

发送方：

a.对M使用Hash函数得到H(M)

b.使用KRa对H(M)进行签名，得到SigKRa(H(M))

c.将SigKRa(H(M))和M拼接，得到SigKRa(H(M))||M

d.压缩SigKRa(H(M))||M，得到Z(SigKRa(H(M))||M)

e.使用Ks对Z(SigKRa(H(M))||M)进行对称加密，得到ECKs(Z(SigKRa(H(M))||M))

f.使用KUb对Ks进行RSA加密，得到EPKUb(Ks)

g.拼e、f结果，得到EPKUb(Ks)||ECKs(Z(SigKRa(H(M))||M))

h.发送数据

接收方：

a.使用KRb对EPKUb(Ks)进行RSA解密，得到Ks

b.使用解密得到的Ks对ECKs(Z(SigKRa(H(M)||M))进行对称解密，得到Z(SigKRa(H(M))||M)

c.对Z(SigKRa(H(M))||M)进行解压缩，得到SigKRa(H(M))||M

d.使用KUa对SigKRa(H(M))进行RSA解密，得到H(M)

e.对明文M使用Hash函数，得到H(M)’

f.比较H(M)和H(M)’

1. **假设RSA公钥密码体制中，加密密钥****，**
   1. **试根据加密密钥求出解密密钥.**
   2. **若密文为，试求明文。(均要求写过程，6分)**

解：

（1）n=p×q=31×29=899

ϕ(n)=(p-1) ×(q-1)=840

由ed mod ϕ(n)=1,得17d mod 840=1

利用辗转相除法可得d=593

（2）由题可知，c=58，得m= =

试用平方-乘算法平方-乘算法

Square-Multiply(a, b, n)

z=1

for i=l-1 down to 0 {

z = z^2 mod n

if bi=1 {

z = (z×a) mod n

}

}

return z

计算（58^593）mod899

b=593，二进制为1001010001（10位）

计算过程列表如下：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| bi | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| z | 58 | 667 | 783 | 116 | 870 | 232 | 783 | 870 | 841 | 29 |

由上表计算过程可知，明文为29。

1. **设H是128比特的HASH函数，R1，R2，R3函数反向将128比特散列值均匀地映射为6字符的口令，利用H和3个R函数可以形成一条长度为3的彩虹链：**

**其中 均是长度为6的字符串，字符取值范围为10个数字和26个小写字母。试问：若生成 条这样的彩虹链（互不相同），最终，不同的链尾（）大约有多少个？（8）**

解：

令 ， ，

不同的个数 ，

因为 ，

再计算不同的pass1的个数 ，

同理可以求得不同的pass2的个数 ，

不同的pass3的个数 ，

由以上过程可以计算出，不同的链尾（pass3）大约有9931509个。

1. **试证明:明文空间为的加密方案Π=(Gen,Enc,Dec)对上任意概率分布，任何明文*m*∈和任何密文*c*∈且，都有，当且仅当对于所有敌手*A*都有：. (8分)**

证明：（1）证明必要性：

对于M上的某一特殊分布，Pr[M=m0]= Pr[M=m1]=1/2,其中m0，m1由敌手A输出，满足完善保密性。根据定义3，对任意密文c∈，有Pr[C=c|M=m0]=Pr[C=c|M=m1]，即

（2）证明充分性：

反证法，若该加密方案不满足完善保密的定义，则由定义3，存在m0，m1属于M，c∈X，使Pr[C=c|M=m0]≠Pr[C=c|M=m1]。此时，若敌手A在实验中输出m0，m1，则>1/2。与前提矛盾。所以该方案满足完善保密性，根据定义1，得证充分性。

1. **考虑一个密码体制，其中****。假设加密矩阵如下：**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***a*** | ***b*** | ***c*** |
| ***K*1** | **3** | **2** | **1** |
| ***K*2** | **1** | **3** | **2** |

**若，**

* 1. **试判断该密码方案是否为完善保密的。（3分）**
  2. **试说明是否可能通过调整明文的分布改变该密码方案的完善性。（3分）**

答：a）要计算是否具有完善保密性，只需要验证Pr[M=m│C=c]=Pr[M=m]对∀m∊M，∀c∊C都成立。本题中：

Pr[C=1]=Pr[M=c]Pr[C=1|M=c]+Pr[M=a]Pr[C=1|M=a]=0.25\*0.5+0.5\*0.5=0.375

由贝叶斯公式可得：

Pr[M=a|C=1]=Pr[C=1|M=a]\*Pr[M=a]/Pr[C=1]=0.5\*0.5/0.375=0.667 ≠ Pr[M=a]=0.5,即Pr[M=a|C=1] ≠ Pr[M=a]

通过上述计算，可知该密码体制不是完善保密的。

b）不能通过改变明文M 的分布改变该加密方案的完善性。密码方案的完善保密性要求对于任意的明文分布都是完善保密的，不存在“对特定明文分布满足完善保密”。

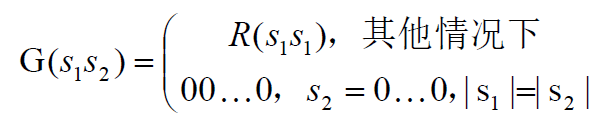
1. **令是一个伪随机数发生器，并且****，其中表示二进制串长度,**

**（1）定义，试问仍然是伪随机数发生器吗？ (4分)**

**（2）定义，其中，*n*为正偶数，试问仍然是伪随机数发生器吗？ (2分)**

解：（1）不一定是伪随机发生器。

令R(\*)为一个伪随机发生器，定义G(s1s2)满足：



可以证明G(s1s2)是一个伪随机发生器

此时，** =** 0…0，显然不是伪随机数

所以不一定是伪随机发生器。

（2）仍然是伪随机发生器。

s1…sn是均匀随机的，则s1…sn/2也是均匀随机的，由G是伪随机发生器可知，也是伪随机发生器。

1. **考虑一个CBC加密模式的变体：每次当一个消息被加密时，发送方只是简单地对IV加1（而不是每次随机选择IV）.说明该方案是非CPA安全的.(6分)**

解：该方案不是CPA安全的，因为存在如下的敌手攻击方法：

1. 预查询

敌手向加密机发送m0=0…00，返回加密结果c0，由于iv是公开的，敌手同时获得了iv。且得到c0=F(iv)

1. 构造

构造m1、m2

若IV最后一位为0，则构造m0=0…01 m1=1…11

若IV最后一位为1，则构造m0=0…10 m1=1…11

1. 区分

将m0 m1发送到加密机，返回s；

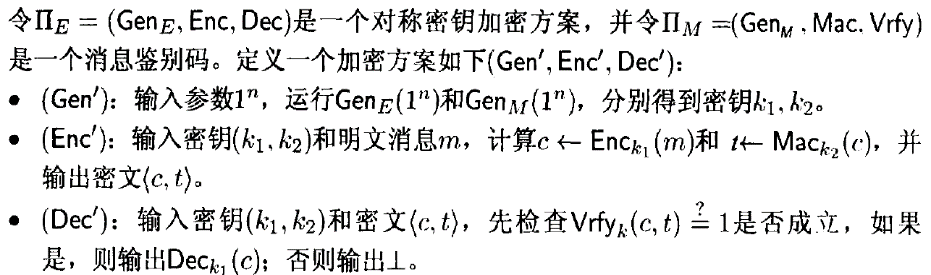
已知，所以，若，则输出0，否则输出1。可知能够以几乎1的概率判断成功。故不是CPA安全的。

1. **证明分组加密的计数器模式不是CCA安全的.(6分)**

证明：敌手在CCA 条件下，修改密文c 中某一分组ci 中某一个比特得到ci’，请求随机预言机解密修改后的密文c’，由于分组加密的计数器模式中只存在异或逻辑与伪随机置换，此时得到的明文m’与原始的明文m 只存在一个比特的差距，找到对应比特修改后即可得到正确的明文，故分组加密的计数器模式不是CCA 安全的。

1. **设是一个CPA安全的对称密钥加密方案，试将其改进为一个CCA安全的加密方案，并简要说明理由. (6分)**

解：（1）改进方法如下：



（2）理由如下：

敌手对于解密预言机的询问有两种方式：一种是敌手从其加密预言机得到的密文，另一种不是。第一种解密询问并不是很有用，因为敌手已经知道密文所对应的明文；对于第二种类型的密文而言，因为是一个安全的消息鉴别码，在一定概率情况下可认为所有这种密文是无效的，所以解密预言机会简单的返回失败，第二种解密询问也是没有用的。因此改进的加密方案的安全性可转化为初始加密方案的CPA 安全性上。

1. **设是一个单向置换，试利用该单向置换构造一个明文、密钥、密文均为*n*比特的CPA安全的对称加密方案.(6分)**

答：OFB,CFB.CTR 都可以利用单向置换来获得CPA安全的对称的加密方案，选择CTR作为对称加密方案的模式，f作为其中的加密函数，其中最重要的是每次消息加密，CTR随机均与选择时，该方案是CPA安全的。

这里还有几个额外的步骤:

(a) 长度为n的IV均匀随机地从{0,1}n中选择,这里考虑过构造一个

伪随机发生器，但是种子又从何而来，因此作罢；

(b) 对称加密函数设计为c←f(m⊕k),其中k是长度为n的密钥，这里k均匀随机地从{0.1}n中选择；

(c) 将上面的IV和k通过非对称加密附带在消息中。

整个流程图如下:

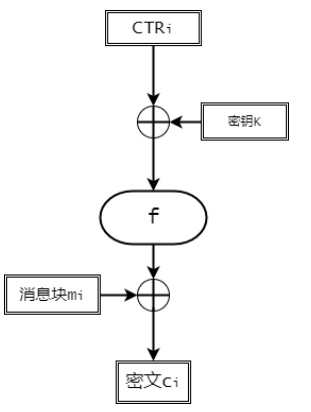


图1：CTR加密单元

1. **SSL是当前最常用的身份认证与密钥交换协议，包括握手协议、记录协议和报警协议，试利用所学的密码学和安全协议的知识分析SSL握手协议的安全性及应用. (10分)**

[附：SSL握手协义简化版]

**第一阶段**，版本、算法协商。

(1)C-〉S：Supported Version，RC，Session id，Supported Cipher suite，Supported Compression method，分别表示支持的最高版本、客户端随机数（28比特）、会话ID，支持的密码套件名称(例如：SSL\_DHE\_RSA\_WITH\_DES\_CBC\_SHA)、支持的压缩方法。

(2) S-〉C：Version，RS，Session id，Cipher suite，Compression method，分别表示选择的版本、服务器端随机数（28比特）、会话ID，选择的密码套件名称、选择的压缩方法。

**第二阶段**，服务器发送证书给客户端。

(3)S-〉C：Certs of Server，表示服务器的相关证书RSA或者DSA证书等。

(4) S-〉C(可选)：将用在密钥交换过程的相关公钥参数，以及这些参数的数字签名发送给客户端。仅当(3)中所提供的消息不足时才发送此消息，与认证方式的选择有关（RSA或者DH协议等），例如，若选择RSA方式交换密钥，由于（3）中已提供，则可省；如果选择DH协议，则会发送以及它们的数字签名.在选择RSA方式交换密钥的时候，也可以选择重新生成一个临时的、不同于签名的RSA加密密钥发给客户端。

(5) S-〉C(可选)：Request of Client Certs，请求客户端发送证书进行验证，仅当服务器强制客户端认证时，服务器端才发送此消息，消息中会包含服务端支持的证书类型和所有Server端信任的证书发行机构的DN（Distinguished Name）列表.

**第三阶段**，由客户端端发送证书给服务器端。

(6)C-〉S(可选)：Certs of Client，表示客户端的相关证书，仅当服务器强制客户端认证时，客户端才发送此消息.

(7) C-〉S：，例如，若选择RSA认证，则用服务器的公钥加密预备主密钥*PM*给服务器；若选择DH认证，则发送给服务器，服务器可以根据自己生成PM.

(8) C-〉S (可选)：，客户端的签名，仅当服务器强制客户端认证时，客户端才发送此消息，其中，主密钥的生成方式如图（1）.

**第四阶段**，客户端和服务器端分别生成：HMAC消息鉴别码密钥Auth.Key，分组加密初始向量IV，分组加密密钥Enc.Key，生成方法如图（2）、图（3）。

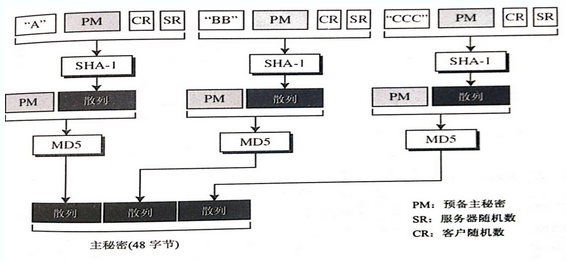


图1由预备主密钥PM生成主密钥M

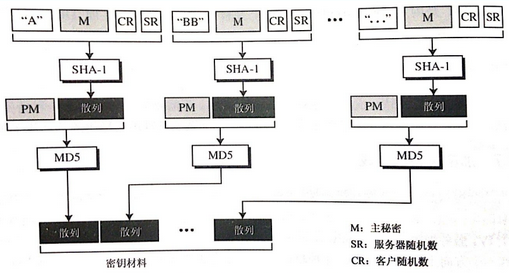


图2由M生成密钥材料

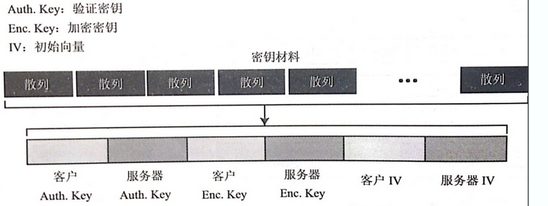


图3从密钥材料提取所需密钥

以后，客户端用客户端的Auth.key,IV,Enc.Key加密消息发送给服务器端，而服务器端则用服务器端的Auth.key,IV,Enc.Key加密消息发送给客户端，加密是单向的。

**第五阶段**，客户端和服务器端分别发表握手协义结束申明。使用HMAC算法计算收到和发送的所有握手消息、主密钥M和常数串“cient/server finished”的摘要，然后通过一个伪随机函数PRF计算出结果，用对称加密算法加密后发送给对方，对方收到后验证其正确性。

解：（1）SSL握手协议的安全性：

1）协商密钥时，由于加入了随机数可抵抗重放攻击；

2）密钥协商过程中采用了DH 协议或RSA 加密，可以抵抗窃听攻击；

3）对DH 协议加上数字签名进行改进，可以抵抗中间人攻击；

4）由于SSL 主要提供了保密性、完整性、认证性，但并不对消息做签名，所以不能够防止抵赖；

5）SSL 是选择密文安全的，采用的加密方案是CBC 方式，在此基础上还增加了HMAC 的消息鉴别码；

6）加密数据时，由于记录协议中引入了序号保证重放时可被检测出来，可以抵抗重放攻击；

7）采用双向加密方式，客户端和服务器端加密所用的密钥不同。

（2）SSL握手协议的应用：

1）单向认证：又称匿名SSL连接，这是SSL安全连接的最基本模式，它便于使用，主要的浏览器都支持这种方式，适合单向数据安全传输应用。在这种模式下客户端没有数字证书，只是服务器端具有证书，以不在认用户访问的是自己要访问的站点。典型的应用就是用户进行网站注册时彩ID＋口令的匿名认证。

2）双方认证：是对等的安全认证，这种模式通信双方都可以发起和接收SSL连接请求。通信双方可以利用安全应用程序（控键）或安全代理软件，前者一般适合于B/S结构，而后者适用于C/S结构，安全代理相当于一个加密/解密的网关，这种模式双方皆需安装证书，进行双向认证。这就是网上银行的B2B的专业版等应用。

3）电子商务中的应用。电子商务与网上银行交易不同，因为有商户参加，形成客户――商家――银行，两次点对点的SSL连接。客户，商家，银行，都必须具证书，两次点对点的双向认证。

1. **CPABE是一种基于密文策略的属性加密算法，假设一个单位的组织机构图如图1所示，试利用CPABE设计一种密钥管理和加密方案，实现如下安全要求：(8分)**
   1. **同一部门的用户之间可以互访加密文件；**
   2. **不同部门的用户之间不能互访加密文件；**
   3. **上级部门的用户可以查看下级部门用户的加密文件。**

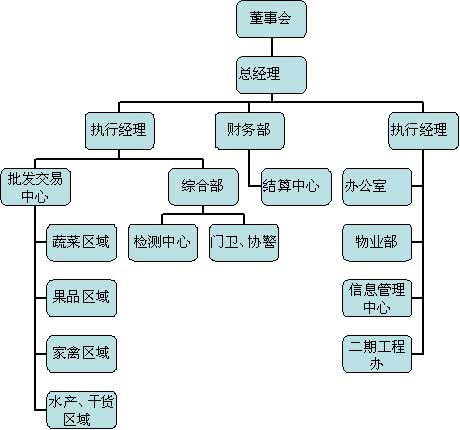


图1某单位组织机构图

解：（1）定义属性集合：某部门的属性集合为自己所在部门及其所有下属部门的属性集合，具体如下

**董事会：Prop0**={董事会，总经理，执行经理1，财务部，执行经理2，批发交易中心，综合部，结算中心，办公室，物业部，信息管理中心，二期工程办，蔬菜区域，果品区域，家禽区域，水产、干货区域，检测中心，门卫、协警}

**总经理：Prop1**={总经理，执行经理1，财务部，执行经理2，批发交易中心，综合部，结算中心，办公室，物业部，信息管理中心，二期工程办，蔬菜区域，果品区域，家禽区域，水产、干货区域，检测中心，门卫、协警}

**执行经理1：Prop2**={执行经理1，批发交易中心，综合部，蔬菜区域，果品区域，家禽区域，水产、干货区域，检测中心，门卫、协警}

**财务部：Prop3**={财务部，结算中心}

**执行经理2：Prop4**={执行经理2，办公室，物业部，信息管理中心，二期工程办}

**批发交易中心：Prop5**={批发交易中心，蔬菜区域，果品区域，家禽区域，水产、干货区域}

**综合部：Prop6**={综合部，检测中心，门卫、协警}

**结算中心：Prop7**={结算中心}

**办公室：Prop8**={办公室}

**物业部：Prop9**={物业部}

**信息管理中心：Prop10**={信息管理中心}

**二期工程办：Prop11**={二期工程办}

**蔬菜区域：Prop12**={蔬菜区域}

**果品区域：Prop13**={果品区域}

**家禽区域：Prop14**={家禽区域}

**水产、干货区域：Prop15**={水产、干货区域}

**检测中心：Prop16**={检测中心}

**门卫、协警：Prop17**={门卫、协警}

（2）密钥管理和加密方案：系统共用一个公钥，并根据属性集合来分配私钥（即给每个属性集合分配一个私钥），然后运用密钥对部门文件进行加密。

由属性集合的定义可以看出：同一部门的用户拥有相同密钥，上级部门的密钥体系包含下级部门的密钥体系，而不同部门的体系密钥之间没有交集。由此可知，该方案满足题目要求。

1. **1）试描述自主访问控制与强制访问控制的区别？(2分)**

**2）试描述BLP模型的安全特性，它们反映了什么样的安全策略？(2分)**

**3）基于属性的访问控制模型能否实现自主访问控制和强制访问控制策略？说明理由。(6分)**

答：1）自主访问控制：是指由用户有权对自身所创建的访问对象（文件、数据表等）进行访问，并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限。

强制访问控制：是指由系统（通过专门设置的系统安全员）对用户所创建的对象进行统一的强制性控制，按照规定的规则决定哪些用户可以对哪些对象进行什么样操作系统类型的访问，即使是创建者用户，在创建一个对象后，也可能无权访问该对象。

强制访问控制一般与自主访问控制结合使用，在自主访问控制的基础上，施加一些更强的访问限制。用户可以利用自主访问控制来防范其它用户对自己客体的攻击，强制访问则提供了一个不可逾越的、更强的安全保护层。

2）BLP模型的安全特性定义了系统状态的安全性，体现了BLP模型的安全策略，具体如下：

a. 自主安全性：状态v=(b,M,f)满足自主安全性，当且仅当对所有的(si,oj,x)∈b,有x∈Mij

此条性质是说，若(si,oj,x)∈b，即如果在状态v，主体si获得了对客体oj的x访问权，那么si必定得到了相应的自主授权。

b．简单安全性：状态v=(b,M,f)满足简单安全性，当且仅当对所有的(s,o,x)∈b,有(i) x=e或x=a或x=c或**(ii)** (x=r或x=w)且(f1(s)≥f2(o),f3(s)⊇f4(o))。

w权表示可读、可写，即主体对客体的修改权。

c．\*—性质：状态v=(b,M,f)满足\*—性质，当且仅当对所有的s∈S，若o1∈b(s:w,a)，o2∈b(s:r,w)，则f2(o1)≥f2(o2)，f4(o1) ⊇ f4(o2)，其中符号b(s:x1,x2)表示b中主体s对其具有访问特权x1或x2的所有客体的集合。

* o1∈b(s:w,a)，意味着s对o1有w权或a权，此时信息经由s流向o1
* o2∈b(s:r,w)，意味着s对o1有r权或w权，此时信息可由o2流向s
* 因此，在访问集b中以s为媒介，信息就有可能由o2流向o1。
* 所以要求o1的安全级必须支配o2安全级
* 当s对o1，o2均具有w权时，两次运用该特性， f2(o1)≥f2(o2)，f4(o1) ⊇ f4(o2)及f2(o2)≥f2(o1)，f4(o2) ⊇ f4(o1)
* 则要求o1的安全级必须等于o2安全级

显然\*—性质反映了BLP模型中信息只能由低安全级向高安全级流动的安全策略。

1. ABAC通过属性来对主体的访问进行控制，基本可以适应绝大部分的场景。通过对访问控制策略的制定，可以轻松实现DAC、MAC以及RBAC的功能。

① ABAC 通过设定访问控制策略，描述主体在何时何种环境下可以对客体进行何种操作。这种访问控制策略可以实现DAC。

② ABAC 通过给主体、客体的属性集合中加上安全标签属性(安全级别)。通过设定访问控制策略，可以实现MAC。  
③ ABAC通过给主体、客体的属性集合中加上角色。通过设定访问控制策略，可以实现RBAC。

1. **如果你是一个网站的建设者，如何利用腾迅QQ提供的OAUTH2.0接口对用户的身份进行快捷认证，使得腾迅的合法用户能访问你的网站？（8分）**

解：（1）授权：获取授权码Authorization Code

说明：第一步QQ必须得到要登录系统的授权信息，如果授权全成功，则会跳转到回调地址，同时授权码以参数形式，追加回调地址上。

（2）登录：通过Authorization Code获取Access Token

说明：获取网址中的code值，这个就是Authorization Code，通过它，可以获取访问令牌。这个访问令牌，事实上是给登录系统用的，主要是允许访问QQ的授权服务。

（3）获取用户openid

说明：先说一下openid，它是此网站上或应用中唯一对应用户身份的标识，与QQ号一一对应。网站或应用可将此ID进行存储，便于用户下次登录时辨识其身份，或将其与用户在网站上或应用中的原有账号进行绑定。有了它以后就可以确定当前登录的QQ，获取到QQ登录用户的基本信息了。

（4）调用OpenAPI获取各种信息以及用户授权的资源。