第六章

一、名词解释

1、选择性泄露

2、单一数字证书内容泄露

3、多个数字证书内容泄露

4、Merkle树

二、判断

1、选择性泄露的完整性是指：当证书持有者决定泄露证书私有属性信息的时候，泄露出来的值可以是未经认证的过的。（）

2、选择性泄露的访问控制指：从证书泄露出来的私有属性的值必须是证书持有者自己愿意泄露的。（）

3、在使用Hash函数的选择性泄露协议中产生随机值rv的目的是为了抵抗“字典攻击”。（）

4、Merkle树的优点是：使用很少的存储空间；缺点是：效率随着字段的增加而增加。（）

5、Huffman树需要较多的存储空间，但是效率较高。（）

三、填空题

1.选择性泄露就是在不影响双方的前提下，让证书持有者可以有选择的泄露证书和当前会话的有关信息，而隐藏无关信息，来保护双方的隐私。

2.实现数字证书的选择性泄露必须包含以下几个特性：保密性、完整性。

3从证书包含的信息数量来看，数字证书的选择性泄露分为两种：单一数字证书内容泄露和。

4.单一数字证书的优点是，这样对证书持有者来说，管理证书比较方便，缺点是，需要考虑每个属性的安全性，而且实际验证的时候，有些信息可能会缺乏一定的。

5多个数字证书的有点是，重点比较突出，缺点就是因为证书较多，管理起来比较麻烦，而且有时候，单个证书中也可能包含有敏感信息。当只用Hash函数的选择性泄露协议时，甲方认为乙方可以访问相关的信息时就把

6和发送给乙方，乙方调用Hash函数，并将Hash后的值和证书上的信息比较。

7 Hash函数的优点，缺点。

四、简答

1.比较Merkle树方案和Huffman树方案的优缺点。

2.比较单一数字证书内容泄露和多个数字证书内容泄露的优缺点。

五、计算

1.假定在20次会话中，E-mail需要出示20次，姓名需要出示12次，性别需要出示5次，而生日需要出示1次。根据Huffman编码算法，画出Huffman树。

答案：

一、

1.在不影响通信双方会话的前提下，让证书持有者可以有选择的泄露证书和当前会话的相关信息，而隐藏无关信息，来保护双方的隐私。

2.一个整数中包含有多个属性，这些属性首先处于隐藏状态。

3.通信双方之间互相展示的证书比较多，均多于一个，而每个证书上包含的属性比较少。

4.是一个Hash树，每一个叶子存放经过Hash后的散列码H（M），而根和内部节点的值是他们孩子相连接后的Hash值。

二、

1.错。必须是经过CA认证的。

2.对。

3.对。

4.错。随着字段的增加而下降。

5.错。需要的存储空间较少。

三、

1.通信

2.访问控制、性能、实用性

3.多个数字证书内容泄露

4.一张证书上会有很多信息、含有信息较多、权威性

5.属性单一

6.访问相关信息、相关随机数

7.算法简单实现容易、需要比较大的存储空间

四、

1. 解：Merkle树方案的优点：无论有多少个属性，证书上只需要存放最终的root就可以，极大地节约了证书的存储空间；缺点：随着证书属性的增加，无关信息也就随着增加，增加了计算量，效率也就下降了。Huffman树方案的优点：Huffman树考虑到了每个节点出示的概率，这就使得出示概率高的节点在树中的深度要比出示概率低的节点要低，从而减少了树的搜索路径长度，提高了效率；缺点：Huffman树构建时，每个节点的权值时根据长期统计得来的，因而在一些统计和实际并不相符合的情况下，效率不一定比Merkle树高。

2. 解：单一数字证书内容泄露的优点：一张证书上面含有很多信息，这样对证书持有者来说，管理证书比较方便；缺点：含有的信息比较多，需要考虑每个属性的安全性，而且实际验证的时候，有些信息可能会缺乏一定的权威性。多个数字证书内容泄露的优点：每个证书的属性比较单一，重点比较突出；缺点：因为证书比较多，管理起来比较麻烦，而且有时候，单个证书中也可能含有敏感信息，这就还需要用到单一数字证书内容泄露来保护相关的属性。

五、

解：书131页图6.7。