7

7-7

对称密钥体制，即加密密钥与解密密钥是相同的密码体制，且收发双方必须共享密钥．对称密码的密钥是保密的，没有密钥，解密就不可行，知道算法和若干密 文不足以确定密欄．公钥密码体制中，加密密钥PK(即公钥)是向公众公开的，而解密密钥SK(即私钥或秘钥)是需要保密的，发送方拥有加密或者解密密钥．而接收方拥有另一个密钥. 两个密钥之一也是保密的，无解密密钢．解密不可行，知道算法和其中一个密钥以及若干密文不能确定另一个密钥.

优点：对称密码技术的优点在于效率高，算法简单，系统开销小．适合加密大量数据。 对称密钥算法具有加密处理简单，加解密速度抉，秘钥较短，发展历史悠久等优点.

缺点：对称密码技术进打安全通信前需要以安全方式进行密钥交换，且它的规模复杂.公钥密钥算法具有加解密速度慢、秘钥尺寸大、发展历史较短等特点.

7-9

1. 公钥密码体制的加解密过程：
2. 密钥对产生器产生出接收者B的一对密钥：加密密钥PKB和解密密钥SKB. 发送者A 所用的加密密钥PKB就是接收者B的公钥，它向公众公开. 而B所用的解密密钥SKB就是接收者B的私钥，对其他人都保密.
3. 发送者A用B的公钥PKB通过E运算对明文X加密，得出密文Y，发送给B. B用自己的私钥SKB通过D运算进行解密，恢复出明文.
4. 虽在计算机上可以容易地产生成对的PKB和SKB. 但从己知的PKB实际上不可能推导出SKB，即从PKB到SKB是”计算上不可能的”.
5. 虽然公钥可用来加密，但却不能用来解密.
6. 公钥是可以公开的，因为即使知道了某个公钥，也不可能由此得出相对应的私钥. 加密用公钥，而解密用私钥. 因此公钥公开了对解密没什么影响.
7. 在公钥密码体制中，提供安全的责任几乎全部由密文的接收者承担.密文的接收者需要生成两个密钥：一个私钥和一个公钥. 密文的接收者负责向所有需要和他通信的人分发他的公钥，这可以通过公钥分发信道来完成. 虽然不要求这个信道提供安全性，但它必须提供鉴别和完整性. 不应允许任何其他人向大家发布他自己的公钥并假冒那是密文接收者的公钥. 公钥公开分发是为了方便. 只要能够提供鉴别和完整性，那么对安全性来说，就和不公开分发公钥没有什么区别.

7-10

数字签名必须保证能够实现以下三点功能：

1. 报文鉴别：接收者能够核实发送者对报文的签名. 即接收者能够确信该报文的确是发送 者发送的. 其他人无法伪造对报文的签名.
2. 报文的完整性：接收者确信所收到的数据和发送者发送的完全一样，而没有被篡改过.
3. 不可否认：发送者事后不能抵赖对报文的签名.

现在已有多种实现数字签名的方法，但采用公钥算法要比采用对称密钥算法更容易实现，它的数字签名的原理如下：

为了进行签名，A用其私钥SKA对报文X进行D运算. A把经过D运算得到的密文传送给B. B为了核实签名，用A的公钥进行E运算，还原出明文X. 这里的D运算和E运算都不是为了解密和加密，而是为了进行签名和核实签名. 因为除A外没有别人持有A的私钥SKA，所以除A外没有别人能够用A的私钥SKA对报文X进行D运算. 这样，B就相信报文X是A签名发送的(报文鉴别). 同理， 其他人如果篡改过报文，但并不能得到A的私钥SKA来对X进行D运算. B对篡改过的报文进行E运算后，将会得出不可读的明文，就知道收到的报文被篡改过(证报文的完整性). 若A要抵赖曾发送报文给B，B可把X以及用A的私钥SKA对报文X进行D运算后的结果出示给进行公证的第三者. 第三者很容易用PKA去证实A确实发送过X给B(不可否认). 这里的关键就是没有其他人能够持有A的私钥SKA.