如何构建安全的电子商务网站 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/64/2021_2022__E5_A6_82_E4_BD_95_E6_9E_84_E5_c40_64788.htm 一、电子商务安全基础1、算法的介绍 常用的加密方式分为对称密钥加密和非对称密钥加密两种，也称为秘密密钥加密和公开密钥加密。对称密钥加密和解密时使用的密钥是同一个密钥，其优点是加密速度快，缺点是不能作为身份验证，密钥发放困难。常见的对称加密算法有RC2，RC4，DES，3DES，IDEA，SDBI等。 公开密钥加密和解密使用的密钥是不同的密钥，分别称为公钥和私钥，公钥可以公开，私钥则必须保密只能归密钥所有者拥有。其缺点是对大容量的信息加密速度慢，优点是可以作为身份认证，而且密钥发送方式比较简单安全。常见的公开密钥加密算法有RSA，DSA，ECA等。 另外在密码学中经常使用到的是单向散列函数（Hash函数）。Hash函数用于对要传输的数据作运算生成信息摘要，它并不是一种加密机制，但却能产生信息的数字“指纹”，它的目的是为了确保数据没有被修改或变化，保证信息的完整性不被破坏。Hash函数有三个主要特点：（1）它能处理任意大小的信息，并将其按信息摘要（Message Digest）方法生成固定大小的数据块，对同一个源数据反复执行Hash函数将总是得到同样的结果。（2）它是不可预见的。产生的数据块的大小与原始信息看起来没有任何明显关系，原始信息的一个微小变化都会对小数据块产生很大的影响。（3）它是完全不可逆的，没有办法通过生成的数据块直接恢复源数据。常见的Hash算法有MD2、MD5和SHA1等。 100Test 下载频道开通，各类考试题目直