[考点知识]电子商务安全管理文件加密 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/169/2021_2022__5B_E8_80_83_E7_82_B9_E7_9F_A5_c40_169694.htm 一． 对本地文件进行加密和解密 1．简述现代主要的加密技术？ 答题思路：对称密码体制和非对称密码体制。对称式加密就是加密和解密使用同一个密钥，通常称之为“ Session Key ”。这种加密技术目前被广泛采用，如美国政府所采用的DES加密标准就是一种典型的“ 对称式 ”加密法，它的Session Key。长度为56Bits。非对称式加密就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“ 公钥 ”和“ 私钥 ”，它们两个必需配对使用，否则不能打开加密文件。这里的“ 公钥 ”是指可以对外公布的，“ 私钥 ”则不能，只能由持有人一个人知道。常有的有DES、IDEA、AES等算法。在教材中的介绍比较简单，有兴趣的读者可以通过搜索引擎搜索更多详细的介绍。 2．针对以物理途径访问系统的人，如何保护磁盘文件不会被窃取？（考虑数据加密） 答题思路：以Win2000为例，个人计算机系统的标准安全措施是试图在使用硬盘引导之前从软盘引导。用户可以用它来防止驱动器失灵和损坏的引导分区，它增加了引导不同的操作系统的便利。不幸的是，这意味着能够以物理途径访问系统的人可以使用工具来读取Windows NTFS磁盘结构，来绕过Windows 2000操作系统文件访问控制的内置安全特性。许多硬件配置提供了类似于引导密码的特性用来限制此类访问。这种特性并没有广泛使用，在多用户共享一个工作站的特定环境中，它们就不能很好地发挥作用。即使这些特性是通用的，这种提供密码的保护

也并不是很强。这些安全关系的根源是敏感信息，它们通常是作为未保护的文件存在于你的磁盘中。如果Windows 2000是唯一可以运行的操作系统并且你的硬盘不会被物理拆除的话，你可以限制访问存储在NTFS分区中的敏感信息。如果有人能够从物理上访问计算机或者磁盘驱动器的话，他们想获得这些信息并不难。使用允许从MS-DOS和UNIX操作系统访问NTFS文件的工具可以更加容易地绕过NTFS安全。数据加密是这个问题的唯一解决方案。使用EFS，NTFS文件中的数据在磁盘上是加密的。这里使用的加密技术是基于公钥的，并且作为综合系统服务运行的，这就使得它容易管理、很难攻击并且对于用户是透明的。如果试图访问加密的NTFS文件用户有那个文件的密钥，他就能够打开这个文件，并且像普通文档一样透明地使用它。没有此文件密钥的用户就无法访问。二． 对邮件进行加密解密 1．简述目前安全电子邮件技术。 答题思路：（1）端到端的安全电子邮件技术；（2）传输层的安全电子邮件技术；（3）邮件服务器的安全与可靠性。详细内容请参考教材。 2．PGP技术的核心内容是什么？ 答题思路：PGP（Pretty Good Privacy）技术是一个基于不对称加密算法RSA公钥体系的邮件加密技术，也是一种操作简单、使用方便、普及程度较高的加密软件。PGP技术不但可以对电子邮件加密，防止非授权者阅读信件；还能对电子邮件附加数字签名，使收信人能明确了解发信人的真实身份；也可以在不需要通过任何保密渠道传递密钥的情况下，使人们安全地进行保密通信。PGP技术创造性地把RSA不对称加密算法的方便性和传统加密体系结合起来，在数字签名和密钥认证管理机制方面采用了无缝结合的巧妙设计，使其几乎成

为最为流行的公钥加密软件包。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com