 6.4 加密技术与认证技术考点7 密码学基本概念 1数据加密技术 数据加密技术从技术上的实现分为软件和硬件两方面。按作用不同，数据加密技术主要分为数据传输、数据存储、数据完整性的鉴别及密钥管理技术这4种。从通信网络的传输方面，数据加密技术可以分为3类：链路加密方式、节点到节点方式和端到端方式。链路加密方式是一般网络通信安全主要采用的方式。节点到节点的加密方式是为了解决在节点中数据是明文的缺点，在中间节点里装有加、解密的保护装置，由这个装置来完成一个密钥向另一个密钥的变换。在端到端加密方式中，由发送方加密的数据在没有到达最终目的节点之前是不被解密的。 2保密学 保密学是研究密码系统或通信安全的科学，它包含两个分支：密码学和密码分析学。 需要隐藏的消息叫做明文。明文被变换成另一种隐藏形式被称为密文。这种变换叫做加密。加密的逆过程叫解密。对明文进行加密所采用的一组规则称为加密算法。对密文解密时采用的一组规则称为解密算法。加密算法和解密算法通常是在一组密钥控制下进行的，加密算法所采用的密钥称为加密密钥，解密算法所使用的密钥称为解密密钥。 3密码系统 密码系统通常从以下3个独立的方面进行分类： (l)按明文转化为密文的操作类型分为置换密码和易位密码 (2)按明文的处理方法可分为分组密码和序列密码。 (3)按密钥的使用个数分为对称密码体制和非对称密码体制。考点8 公开密钥加密 在非对称加密体系中，密钥被分

解为一对(即一把公开密钥或加密密钥和一把专用密钥或解密密钥)。这对密钥中的任何一把都可作为公开密钥(加密密钥)通过非保密方式向他人公开，而另一把则作为专用密钥(解密密钥)加以保存。公开密钥用于对机密性信息的加密，专用密钥则用于对加密信息的解密。专用密钥只能由生成密钥的贸易方掌握，公开密钥可广泛发布，但它只对应于生成密钥的贸易方。 RSA算法是非对称加密领域内最为著名的算法，但是它存在的主要问题是算法的运算速度较慢。因此，在实际的应用中通常不采用这一算法对信息量大的信息进行加密。对于加密量大的应用，公开密钥加密算法通常用于对称加密方法密钥的加密。 