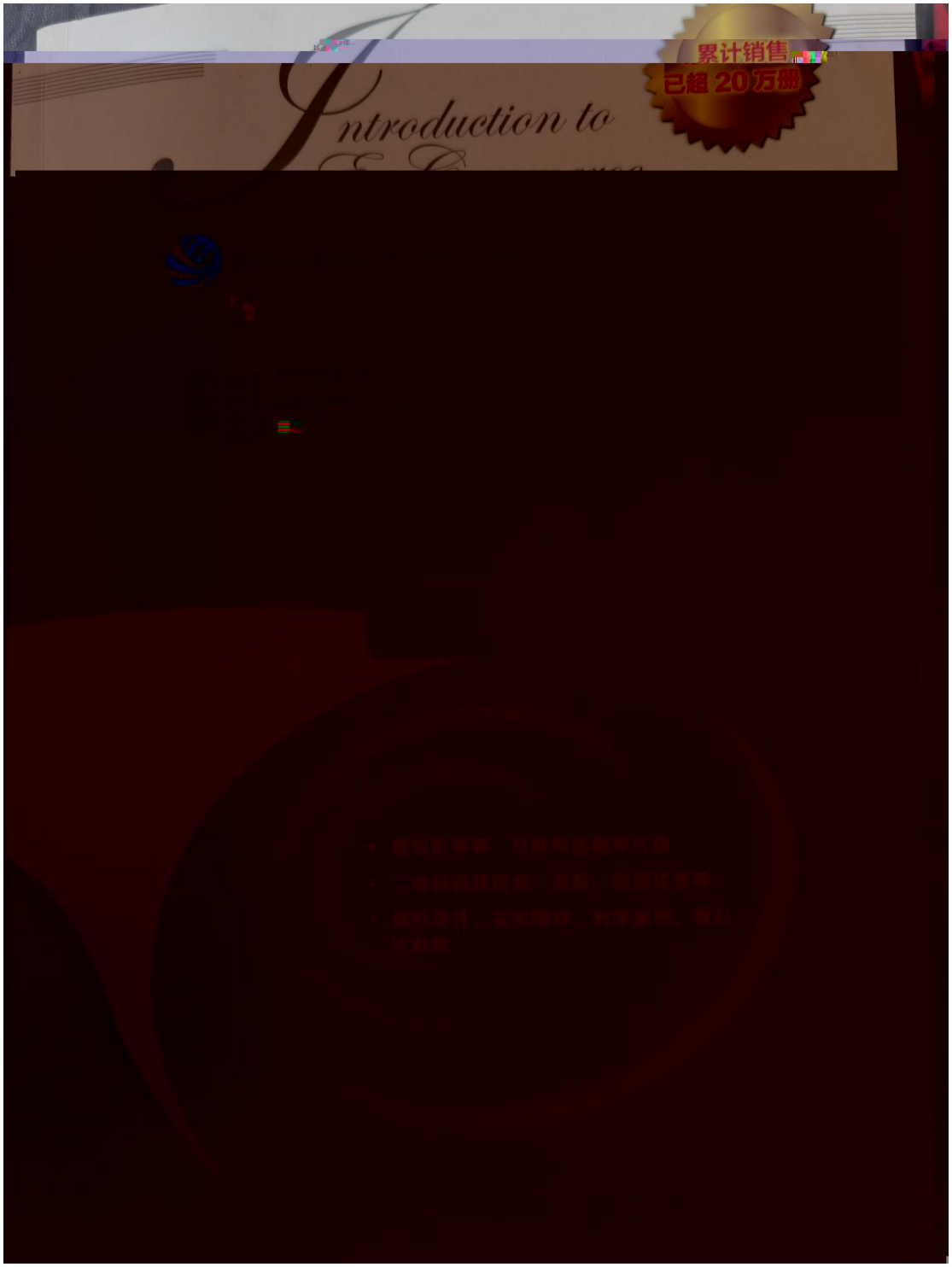
电子商务实训指导教师岗位试讲内容

教学内容

第二节：电子商务安全技术

（教材：电子商务概论 中国工信出版集团 白东蕊等主编）

重点：电子商务安全技术，可自备教具及自备案例图表等，可适当删减增加需要的少部分内容。


累计销售
已超 20万册

本案例整理自中国物流与采购网2018年3月26日发布的《电子面单将破解快递信息安全难题？》

隐藏处理。

事实上，一些业内企业早已经开始布局电子面单了。2016年6月，京东商城就已经开始试行“微笑面单”，即在包裹生成时就部分隐藏用户的姓名和手机号码信息，以“笑脸”符号代替。2017年5月，菜鸟也推出了“隐私面单”，以避免将消费者个人信息全部显示在快递面单上。顺丰自从推行电子面单以后，其电子面单覆盖率很快达到90%以上。“四通一达”等主流快递也在加快淘汰纸质面单的步伐。

启发思考：1. 电子面单与纸质面单相比具有哪些优势？

2. 电子面单应如何保证寄件人和收件人的个人信息安全？

第二节　电子商务安全技术

电子商务安全技术在电子商务系统中的作用非常重要，它守护着商家和客户的重要秘密，维护着电子商务系统的信誉和财产，同时为服务对象和被服务对象提供了极大的便利。只有采取了必要和恰当的技术手段，才能充分增强电子商务系统的可鉴别性和可靠性。电子商务系统的安全应该建立在网络安全的基础之上，通过信息安全技术的保障及安全协议的实现才能实现

1. 对称加密体制的工作过程

如图 8.2 所示，对称加密体制主要由五个部分组成：明文、加密算法、密钥、密文、解密算法。发送方用密钥 K 和加密算法 E 对明文 P 进行加密，得到密文 C，然后传输密文 C；接收方用密钥 K 和解密算法 D 对密文 C 进行解密，得到原来的明文 P。

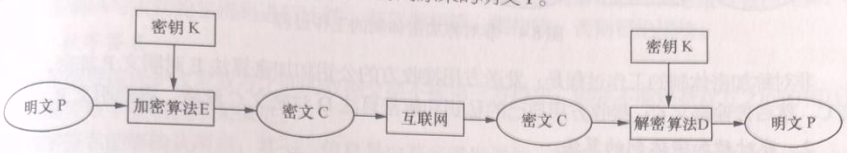


图 8.2　对称加密体制的工作过程

2. 对称加密体制的算法

经典的对称加密体制算法为数据加密标准（Data Encryption Standard，DES）。DES 算法是一种对称的分组加密算法。简单的 DES 算法是以 64 位为分组进行明文输入，在密钥的控制下产生 64 位的密文；反之，输入 64 位的密文，则输出 64 位的明文。加密过程中，密钥总长度是 64 位，但密钥表中每个字节的第 8 位都用作奇偶校验，所以实际有效密钥长度为 56 位。DES 算法可通过软件或硬件来实现。

案例 8.3

个人账户信息等一些重要信息在网络中传递之前，通信双方（如银行与用户）事先约定密钥，通过加密工具利用对称加密技术进行加密处理，然后进行安全传递；到达接收方时，接收方利用已知的密钥解密获取信息。如果传递过程中该信息被非法第三方截获，则其得到的将是看不懂的密文。因而，个人账户信息的机密性得到了保障。

加密过程示例：已知明文为“个人银行存款账户是自然人因投资、消费、结算等需要而开立的可办理支付结算业务的存款账户”，密钥为 123456，则加密得到的密文如图 8.3 所示。

启发思考：利用对称加密体制，个人账户信息在网络中传递时，如何保障个人账户信息安全？

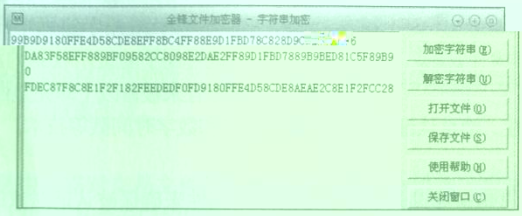


图 8.3　示例中明文加密结果

（二）非对称加密体制

非对称加密体制使用的是密钥对，即公钥（Public Key）和私钥（Private Key）。公钥是公开的，可以以文件的形式存储在密钥管理中心；与之配对的私钥以口令或密码的方式由用户记忆保存。通常用公钥加密、私钥解密来保证信息的机密性；用私钥加密、公钥解密来进行身份认证。

1. 非对称加密体制的工作过程

非对称加密体制由明文 P、加密算法 E、公钥、私钥、密文 C、解密算法 D 六个部分组成。图 8.4 所示为非对称加密体制的工作过程。

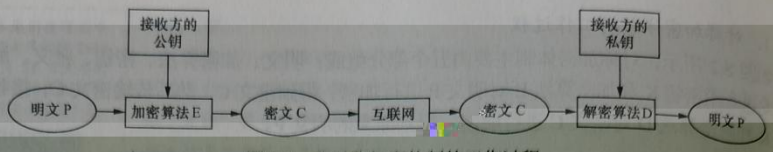


图 8.4　非对称加密体制的工作过程

非对称加密体制的工作过程是：发送方用接收方的公钥和加密算法 E 对明文 P 加密，得到密文 C，然后传输密文 C；接收方用自己的私钥和解密算法 D 对密文 C 解密，得到明文 P。

2. 非对称加密体制的算法

目前，在非对称加密体制的算法中，使用最多的是 RSA 算法。RSA 算法是 1978 年由 R.L.Rivest、A.Shamir 和 L.Adleman 设计的非对称加密体制的算法，算法以发明者姓氏的首字母来命名。它是第一种既可用于加密，又可用于数字签名的算法。

一般来说，RSA 算法只用于对少量数据进行加密，在互联网中广泛使用的电子邮件和文件加密软件 PGP（Pretty Good Privacy）就是将 RSA 算法作为传送会话密钥和数字签名的标准算法。

（三）对称加密体制与非对称加密体制的对比

在实际应用中，通常将对称加密算法和非对称加密算法结合使用，利用 DES 算法进行大容量数据的加密，而利用 RSA 算法来传送对称加密算法所使用的密钥。二者结合使用集成了两类加密算法的优点，既加快了加密速度，又可以安全、方便地管理密钥。表 8.1 为对称加密体制和非对称加密体制的对比。

表 8.1　对称加密体制和非对称加密体制的对比

比较项目	对称加密体制	非对称加密体制
代表算法	DES	RSA
密钥数目	单一密钥	密钥是成对的
密钥种类	密钥是秘密的	一个私有，一个公开
密钥管理	产生简单，管理困难	需要数字证书及可靠的第三方
相对速度	快	慢
主要用途	大容量数据加密	数字签名或对称密钥的加密

二、认证技术

在信息安全领域，常见的信息保护手段除了加密技术以外，还有认证技术。目前，认证技术有身份认证（也叫用户认证）和消息认证两种方式。身份认证用于鉴别用户的身份是否合法，消息认证可用于验证接收到的消息确实来自真正的

2. 消息认证

消息认证是指验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。消息认证常用的方法就是消息摘要，即发送方在发送的消息中附加一个鉴别码，并经加密后发送给接收方。接收方利用约定的算法对解密后的消息进行鉴别运算，将得到的鉴别码与收到的鉴别码进行比较，若二者相等，则接收，否则拒绝接收。

3. 数字签名

消息摘要能保护收发双方之间的数据交换不被第三方侵犯，但并不能规避双方之间的相互欺骗，这需要数字签名技术来保证。

系统中的密码资源。电子商务领域中常见的安全协议有安全套接层协议和安全电子交易协议等。

（1）安全套接层（Secure Socket Layer，SSL）协议是指使用公钥和私钥技术相组合的安全网络通信协议，是网景公司（Netscape）推出的基于互联网应用的安全协议。安全套接层协议指定了一种在应用层协议（如 HTTP、Telnet 和 FTP 等）和 TCP/IP 之间提供数据安全性分层的机制。

（2）安全电子交易（Secure Electronic Transaction，SET）协议是由万事达卡（Master Card）和维萨（Visa）联合网景、微软等公司，于 1997 年 6 月 1 日推出的。该协议主要是为了实现更加完善的即时电子支付。安全电子交易协议是 B2C 基于信用卡支付模式设计的，它在保留对客户信用卡认证的前提下，增加了对商家身份的认证，凸显了客户、商家、银行之间通过信用卡交易的数据完整性和不可否认性等优点。因此，它成为目前公认的基于信用卡网上交易的国际标准。

电子支付无论采用哪种支付协议，都应该考虑安全、成本和使用的便捷性这三个方面的因素。由于这三者在安全电子交易协议和安全套接层协议中的任何一个协议里都无法得到全部体现，因此造成了现阶段安全套接层协议和安全电子交易协议并存的局面。

四、防火墙技术

防火墙是一种将内部网和外部网（如互联网）相互隔离的技术。防火墙的主要作用有以下几项：通过过滤不安全的服务降低风险，强化网络安全；对网络存取和访问进行监控；防止内部信息外泄，防止外部用户非法访问或占用内部资源。另外，防火墙还支持具有互联网服务特性的企业内部网络技术体系虚拟专用网（Virtual Private Network，VPN）。

[illegible]一代防火墙产品已经呈现出一种集成多功能的设计趋势，具有虚拟专用[illegible]公钥基础设施、互联网协议安全性等多项功能，甚至防病毒和入侵检[illegible]成到防火墙产品中了。

第三节 电子商务安全管理[illegible]

[illegible]

[illegible]任的第三方机构来完成的。认证中心就是承担网上安全电子交[illegible]服务、签发数字证书并确认用户身份的服务机构。