02

电子商务安全技术


安全协议
认证技术
加密技术

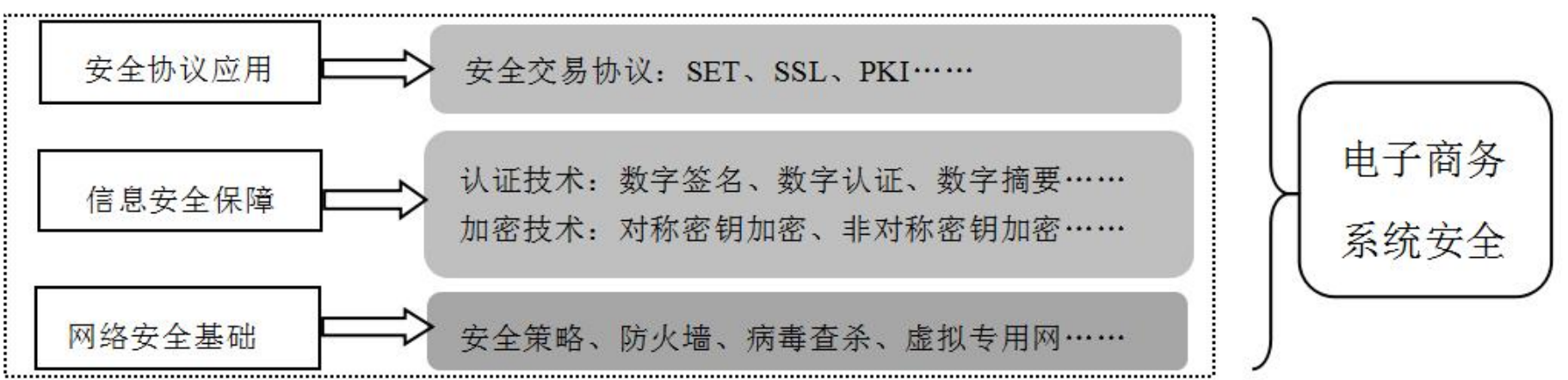
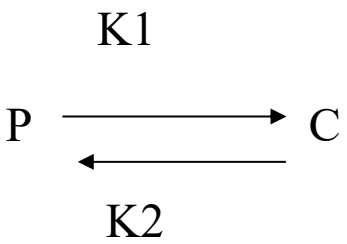


图8.1 电子商务系统安全示意图

- 有关概念：
- 1、加密（E）　　2、解密 （D）　　3、明文（P）

4、密文（C）　　5、密钥（K）



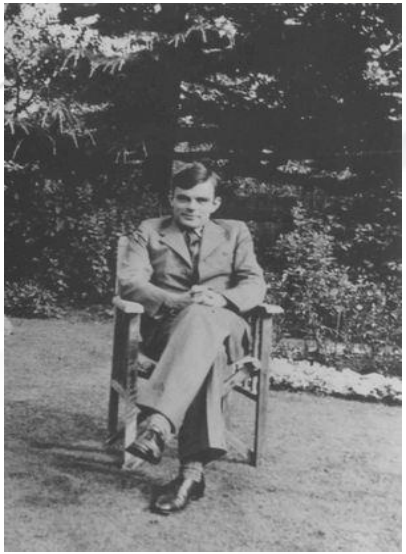
K1=K2（对称加密、单密钥、秘密加密

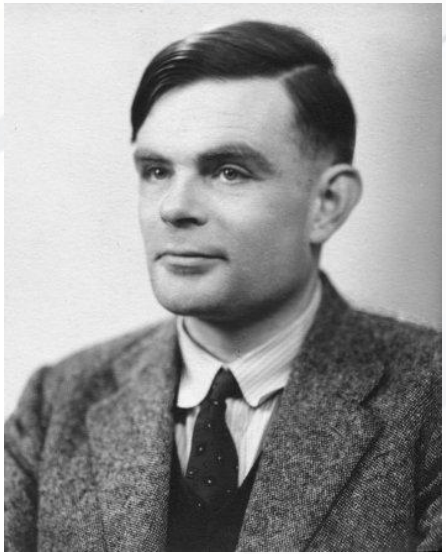
K1≠K2（非对称加密、双密钥、公开加密）

一、加密技术

加密技术是利用技术手段把原始信息变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）信息。原始信息通常被称为“明文”，加密后的信息通常被称为“密文”。

加密技术涉及两个元素：**算法和密钥**。算法是将明文与一串字符（密钥）结合起来，进行加密运算后形成密文。密钥是在将明文转换为密文或将密文转换为明文的算法中输入的一串字符，可以是数字、字母、词汇或短语。





数学大师艾伦·图灵(Alan Turing)

第二次世界大战，英国破解德国军用密码主要依靠数学家

装置2：洛仑兹密码机（金枪鱼）

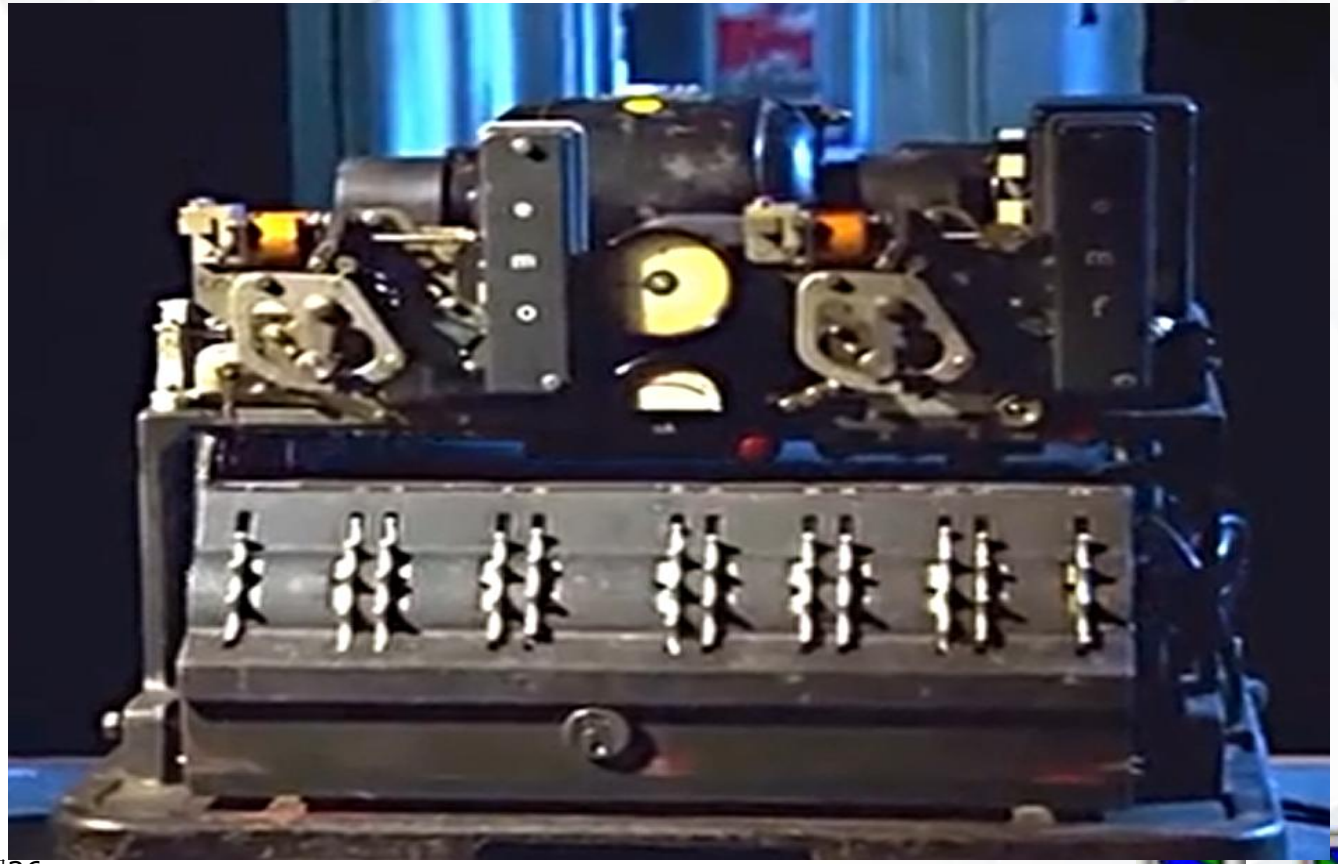


图26

金枪鱼加密机 链接

图27

第-

（一）对称加密体制

1．对称加密体制的工作过程

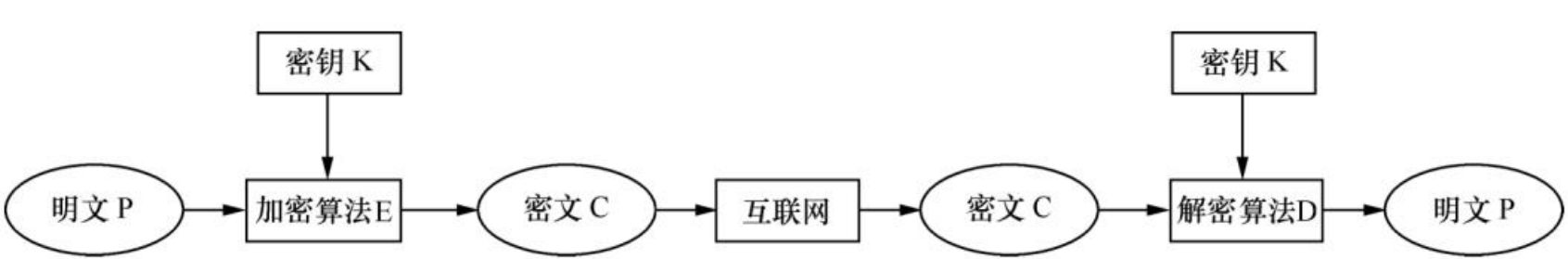


图8.1 对称加密体制的工作过程

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，由于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算法可以通过软件或硬件来实现。

案例

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8.2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的机密性？

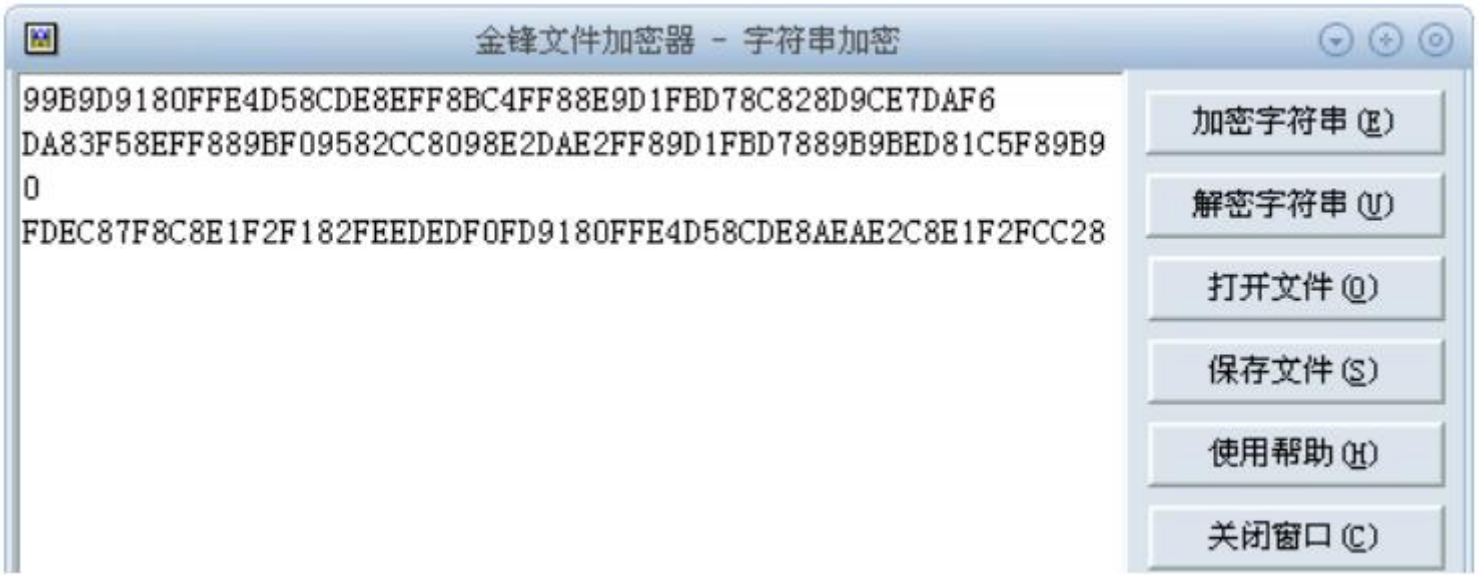


图8.2 示例中明文加密结果

（二）非对称加密体制

1．非对称加密体制的工作过程

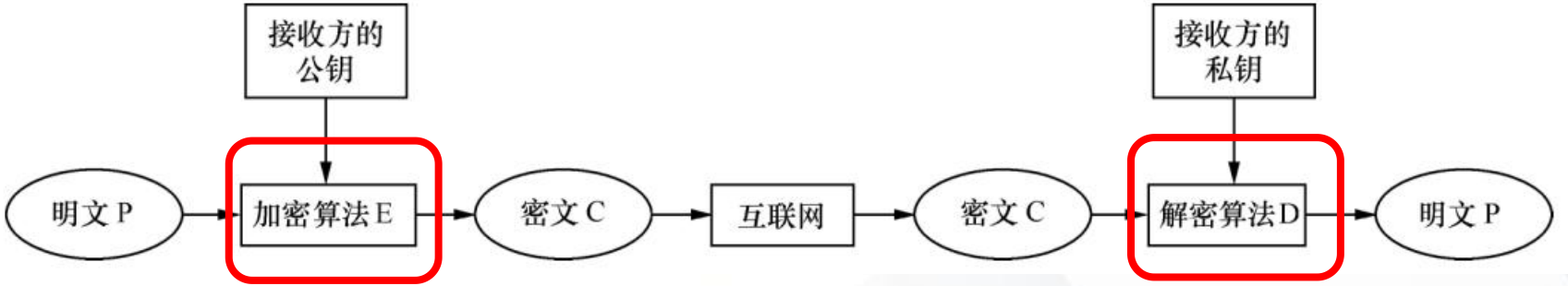


图8.3 非对称加密体制的工作过程

2．非对称加密体制的算法

目前，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。

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算法来传递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所示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

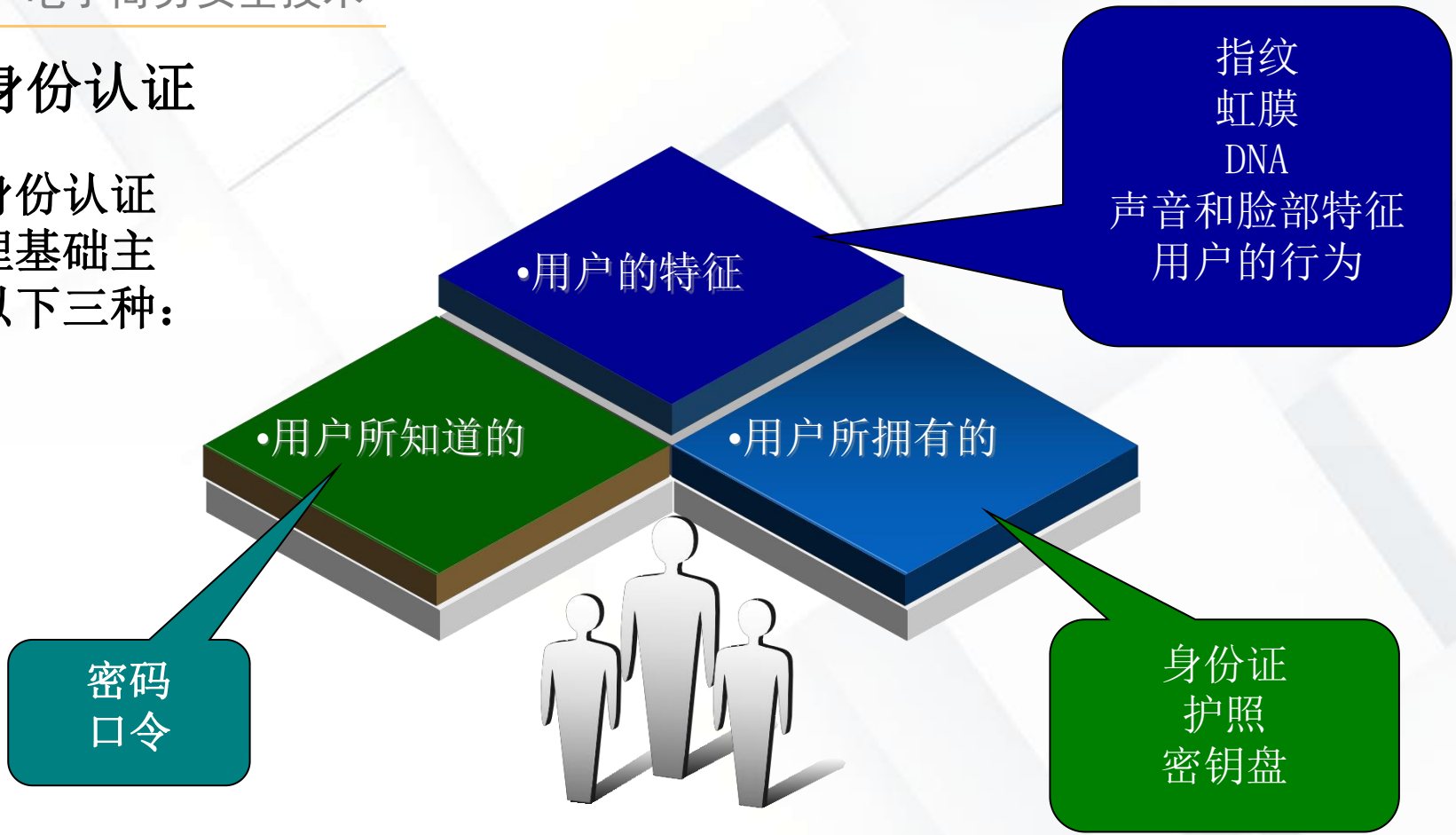
比较项目	对称加密体制	非对称加密体制
代表算法	DES	RSA
密钥数目	单一密钥	密钥是成对的
密钥种类	密钥是秘密的	一个私有，一个公开
密钥管理	产生简单，管理困难	需要数字证书及可靠的第三者
相对速度	快	慢
主要用途	大量数据加密	数字签名或对称密钥的加密

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所收到的消息确实来自真正的发送方且未被修改（即完整性），也可以用于验证消息的顺序性和及时性。**消息认证主要包括数字签名和数字时间戳等技术。**

1. 身份认证

实现身份认证的物理基础主要有以下三种：



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

数字签名能够确认两点：

- 信息是由签名者发送的；
- 信息自签发后到收到为止未曾做过任何修改。

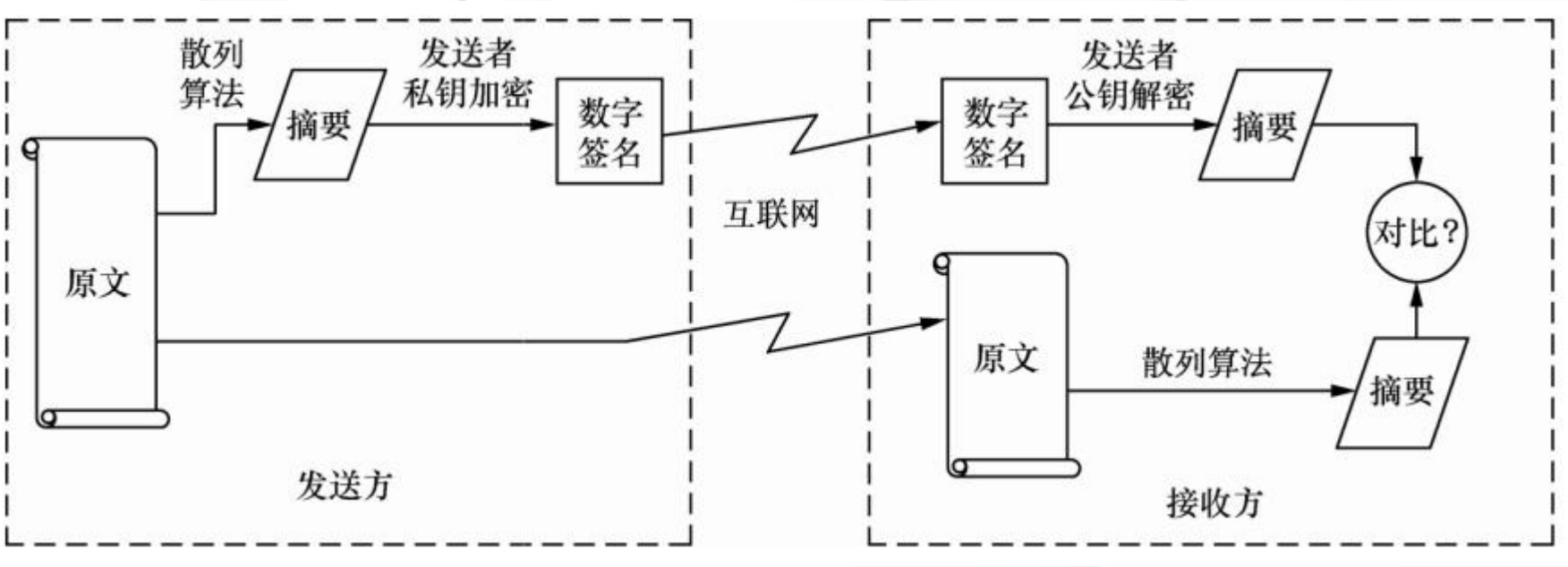


图8.4 数字签名原理示意图

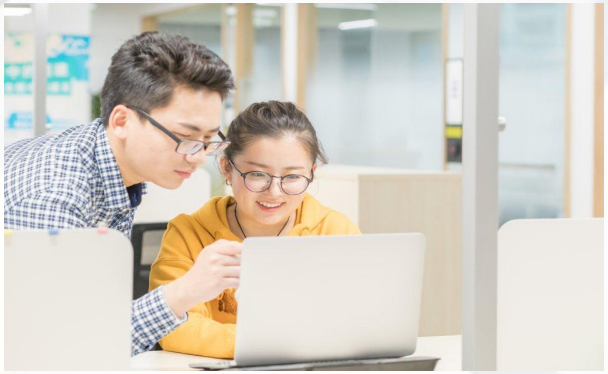
4．数字时间戳

在电子商务交易中，需对交易文件的时间信息采取安全措施。数字时间戳服务（Digital Time-stamp Service，DTS）是由专门的机构提供的对电子文件发送时间进行安全保护的服务。

数字时间戳是一个经加密后形成的凭证文档，包括以下三部分：

需加时间戳的电子文件

数字时间戳发送和接收文件的时间

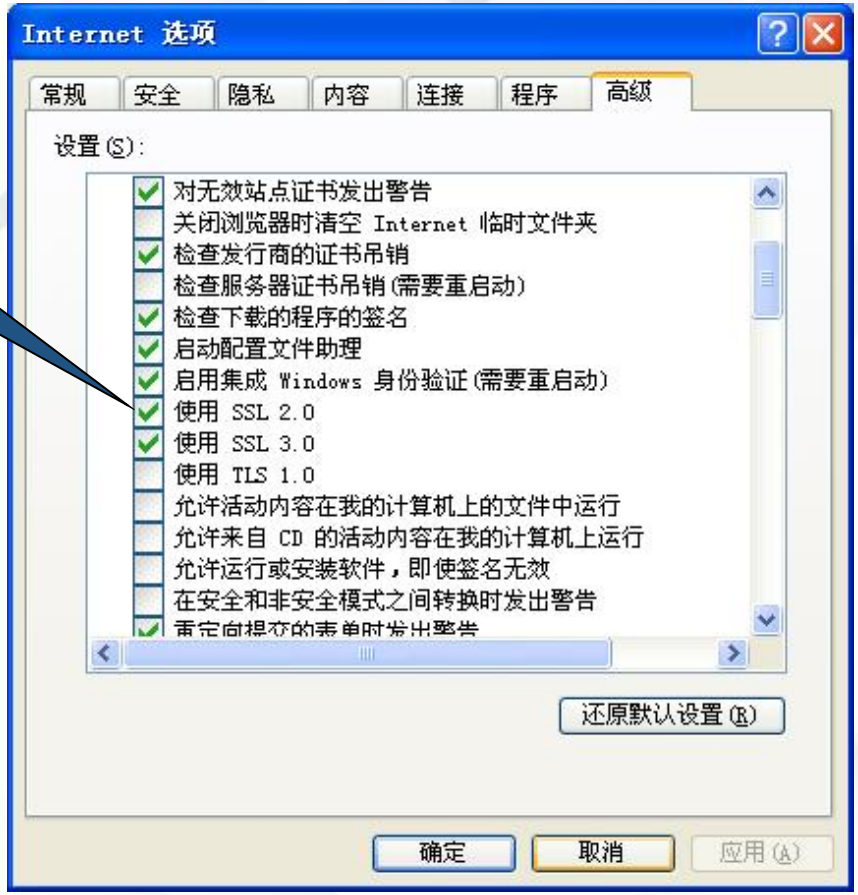


数字时间戳服务的数字签名

SSL协议

三、安全协议

（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而设计的，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；凸显客户、商家、银行之间通过信用卡交易的数据完整性和不可抵赖性等优点，因此，它成为目前公认的信用卡网上交易国际标准。

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。防火墙可以通过过滤不安全的服务，降低风险，强化网络安全策略，对网络存取和访问进行监控；防止内部信息外泄，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）。