电子商务安全解决方案的探讨电子商务师考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_645605.htm 对数据进行有效加密与解密,称为密码技术,即数据机密性技术。其目的是为了隐蔽数据信息,将明文伪装成密文,使机密性数据在网络上安全地传递而不被非法用户截取和破译。伪装明文的操作称为加密,合法接收者将密文恢复出原明文的过程称为解密,非法接收者将密文恢复出原明文的过程称为破译。密码是明文和加密密钥相结合,然后经过加密算法运算的结果。 加密包括两个元素,加密算法和密钥。加密时所使用的信息变换规则称为加密算法,是用来加密的数学函数,一个加密算法是将普通的文本(或者可以理解的信息)与一串字符串即密钥结合运算,产生不可理解的密文的步骤。密钥是借助一种数学算法生成的,它通常是由数字、字母或特殊符号组成的一组随机字符串,是控制明文和密文变换的唯一关键参数。对于相同的加密算法,密钥的位数越多,破译的难度就越大,安全性就越好。目前,电子商务通信中常用的有私有(对称)密钥加密法和公开(非对称)密钥加密法。 一、私有密钥加密法 (一)定义 私有密钥加密,指在计算机网络上甲、乙两用户之间进行通信时,发送方甲为了保护要传输的明文信息不被第三方窃取,采用密钥A对信息进行加密而形成密文M并发送给接收方乙,接收方乙用同样的一把密钥A对收到的密文M进行解密,得到明文信息,从而完成密文通信目的的方法。这种信息加密传输方式,就称为私有密钥加密法。上述加密法的一个最大特点是,信息发送方与信息接收方均需采用同样的密钥,具有对称性,所以私有密钥加密又称为对称密

钥加密。 (二)使用过程 具体到电子商务,很多环节要用到私有密钥加密法。例如,在两个商务实体或两个银行之间进行资金的支付结算时,涉及大量的资金流信息的传输与交换。这里以发送方甲银行与接收方乙银行的一次资金信息传输为例,来描述应用私有密钥加密法的过程:银行甲借助专业私有密钥加密算法生成私有密钥A,并且复制一份密钥A借助一个安全可靠通道(如采用数字信封)秘密传递给银行乙.银行甲在本地利用密钥A把信息明文加密成信息密文.银行甲把信息密文借助网络通道传输给银行乙.银行乙接受信息密文.银行乙在本地利用一样的密钥A把信息密文解密成信息明文。这样银行乙就知道银行甲的资金转账通知单的内容,结束通信。 (三)常用算法 世界上一些专业组织机构研发了许多种私有密钥加密算法,比较著名的有DES算法及其各种变形、国际数据加密算法IDEA等。DES算法由美国国家标准局提出, 1977年公布实施,是目前广泛采用的私有密钥加密算法之一,主要应用于银行业中的电子资金转账、军事定点通信等领域,比如电子支票的加密传送。经过20多年的使用,已经发现DES很多不足之处,随着计算机技术进步,对DES的破解方法也日趋有效,所以更安全的高级加密标准AES将会替代DES成为新一代加密标准。 (四)优缺点 私有密钥加密法的主要优点是运算量小,加解密速度快,由于加解密应用同一把密钥而应用简单。在专用网络中由于通信各方相对固定、所以应用效果较好。但是,私有密钥加密技术也存在着以下一些问题:一是分发不易。由于算法公开,其安全性完全依赖于对私有密钥的保护。因此,密钥使用一段时间后就要更换,而且必须使用与传递加密文件不同的途径来传递密钥,即需要一个传递私有密钥的安全秘密渠道,这样秘密渠道的安全性

是相对的,通过电话通知、邮寄软盘、专门派人传送等方式均存在一些问题。 二是管理复杂,代价高昂。私有密钥密码体制用于公众通信网时,每对通信对象的密钥不同,必须由不被第三者知道的方式,事先通知对方。随着通信对象的增加,公众通信网上的密码使用者必须保存所有通信对象的大量的密钥。这种大量密钥的分配和保存,是私有密钥密码体制存在的最大问题。 三是难以进行用户身份的认定。采用私有密钥加密法实现信息传输,只是解决了数据的机密性问题,并不能认证信息发送者的身份。若密钥被泄露,如被非法获取者猜出,则加密信息就可能被破译,攻击者还可用非法截取到的密钥,以合法身份发送伪造信息。在电子商务中,有可能存在欺骗,别有用心者可能冒用别人的名义发送资金转账指令。因此,必须经常更换密钥,以确保系统安全。四是采用私有密钥加密法的系统比较脆弱,较易遭到不同密码分析的攻击。五是它仅能用于对数据进行加解密处理,提供数据的机密性,不能用于数字签名。 二、公开密钥加密法 (一)定义与应用原理 公开密钥加密法是针对私有密钥加密法的缺陷而提出来的。是电子商务应用的核心密码技术。所谓公开密钥加密,就是指在计算机网络上甲、乙两用户之间进行通信时,发送方甲为了保护要传输的明文信息不被第三方窃取,采用密钥A对信息进行加密而形成密文M并发送给接收方乙,接收方乙用另一把密钥B对收到的密文M进行解密,得到明文信息完密文通信目的的方法。由于密钥A、密钥B这两把密钥中其中一把为用户私有,另一把对网络上的大众用户是公开的,所以这种信息加密传输方式,就称为公开密钥加密法。与私有(对称)密钥加密法的加密和解密用同一把密钥的原理不同,公开密钥加密法的加密与解密所用密钥是不同

的,不对称,所以公开私有密钥加密法又称为非对称密钥加密法。 公开密钥加密法的应用原理是:借助密钥生成程序生产密钥A与密钥B,这两把密钥在数学上相关,对称作密钥对。用密钥对其中任何一个密钥加密时,可以用另一个密钥解密,而且只能用此密钥对其中的另一个密钥解密。在实际应用中,某商家可以把生成的密钥A与密钥B做一个约定,将其中一把密钥如密钥A保存好,只有商家自己知道并使用,不与别人共享,叫作私人密钥.将另一把密钥即密钥B则通过网络公开散发出去,谁都可以获取一把并能应用,属于公开的共享密钥,叫做公开密钥。如果一个人选择并公布了他的公钥,其他任何人都可以用这一公钥来加密传送给那个人的消息。 私钥是秘密保存的,只有私钥的所有者才能利用私钥对密文进行解密,而且非法用户几乎不可能从公钥推导出私钥。存在下面两种应用情况:一是任何一个收到商家密钥B的客户,都可以用此密钥B加密信息,发送给这个商家,那么这些加密信息就只能被这个商家的私人密钥A解密。实现保密性。二是商家利用自己的私人密钥A对要发送的信息进行加密进成密文信息,发送给商业合作伙伴,那么这个加密信息就只能被公开密钥B解密。这样,由于只能应用公开密钥B解密,根据数学相关关系可以断定密文的形成一定是运用了私人密钥A进行加密的结果,而私人密钥A只有商家拥有,由此可以断定网上收到的密文一定是拥有私人密钥A的商家发送的。 (二)使用过程 具体到电子商务,很多环节要用到公开密钥加密法,例如在网络银行客户与银行进行资金的支付结算操作时,就涉及大量的资金流信息的安全传输与交换。以客户甲与乙网络银行的资金信息传输为例,来描述应用公开密钥加密法在两种情况下的使用过程。首先,网络银行乙通过公开密

钥加密法的密钥生成程序,生成自己的私人密钥A与公开密钥B并数学相关,私人密钥A由网络银行乙自己独自保存,而公开密钥B已经通过网络某种应用形式(如数字证书)分发给网络银行的众多客户,当然客户甲也拥有一把网络银行乙的公开密钥B。 1、客户甲传送一“ 支付通知 ”给网络银行乙,要求“ 支付通知 ”在传送中是密文,并且只能由网络银行乙解密知晓,从而实现了定点保密通信。客户甲利用获得的公开密钥B在本地对“ 支付通知 ”明文进行加密,形成“ 支付通知 ”密文,通过网络将密文传输给网络银行乙。网络银行乙收到“ 支付通知 ”密文后,发现只能用自己的私人密钥A进行解密形成“ 支付通知 ”明文,断定只有自己知晓“ 支付通知 ”的内容,的确是发给自己的。 2、网络银行乙在按照收到的“ 支付通知 ”指令完成支付转账服务后,必须回送客户甲“ 支付确认 ”,客户甲在收到“ 支付确认 ”后,断定只能是网络银行乙发来的,而不是别人假冒的,将来可作支付凭证,从而实现对网络银行业务行为的认证,网络银行不能随意否认或抵赖。网络用户乙在按照客户甲的要求完成相关资金转账后,准备一个“ 支付确认 ”明文,在本地利用自己的私人密钥A对“ 支付确认 ”明文进行加密,形成“ 支付确认 ”密文,通过网络将密文传输给客户甲。客户甲收到“ 支付确认 ”密文后,虽然自己有许多密钥,有自己的,也有别人的,却发现只能用获得的网络银行乙的公开密钥B进行解密,形成“ 支付确认 ”明文,由于公开密钥B只能解密由私人密钥A加密的密文,而私人密钥A只有网络银行乙所有,因此客户甲断定这个“ 支付确认 ”只能是网络银行乙发来的,不是别人假冒的,可作支付完成的凭证。 (三)算法 当前最著名、应用最广泛的公开密钥系统是RSA (取自三个创始人的名字的第一个

字母)算法。目前电子商务中大多数使用公开密钥加密法进行加解密和数字签名的产品和标准使用的都是RSA算法。RSA算法是基于大数的因子分解,而大数的因子分解是数学上的一个难题,其难度随数的位数加多而提高。 (四)优缺点 优点是可以在不安全的媒体上通信双方交换信息,不需共享通用密钥,用于解密的私钥不需发往任何地方,公钥在传递与发布过程中即使被截获,由于没有与公钥相匹配的私钥,截获公钥也没有意义。能够解决信息的否认与抵赖问题,身份认证较为方便。密钥分配简单,公开密钥可以像电话号码一样,告诉每一个网络成员,商业伙伴需要好好保管的只是一个私人密钥。而且密钥的保存量比起私人密钥加密少得多,管理较为方便。最大的缺陷就在于它的加解密速度。 三、两种加密法的比较 通过DES算法和RSA算法的比较说明公开密钥加密法和私有密钥加密法的区别:在加密、解密的处理效率方面, DES算法明显优于RSA算法,即DES算法快得多.在密钥的分发与管理方面, RSA算法比DES算法更加优越.在安全性方面,只要密钥够长,如112b密钥的DES算法和1024b的RSA算法的安全性就很好,目前还没找到在可预见的时间内破译它们的有效方法.在签名和认证方面,DES算法从原理上不可能实现数字签名和身份认证,但RSA算法能够方便容易的进行数字签名和身份认证。 基于以上比较的结果可以看出,私有密钥加密法与公开密钥加密法各有长短,公开密钥加密在签名认证方面功能强大,而私有密钥加密在加/解密速度方面具有很大优势。为了充分发挥对称加密法和非对称加密法各自的优点,在实际应用中通常将这两种加密法结合在一起使用,比如:利用DES来加密信息,而采用RSA来传递对称加密体制中的密钥。这样不仅数据信息的加解密速度快,

同时保障了密钥传递的安全性。数据加密技术是信息安全的基本技术,在网络中使用的越来越广泛。针对不同的业务要求可以设计或采取不同的加密技术及实现方式。另外还要注意的是,数据加密技术所讨论的安全性只是暂时的,因此还要投入对密码技术新机制、新理论的研究才能满足不断增长的信息安全需求。