电子商务安全技术：数据加密技术电子商务考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/515/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_515839.htm 加密技术是信息安全技术中一个重要的组成部分。所谓加密，就是用基于数学方法的程序和保密的密钥对信息进行编码，把计算机数据变成一堆杂乱无章难以理解的字符串，也就是把明文变成密文。这样，即使别人得到了密文，也无法辨认原文。所以，加密可以有效地对抗信息的被拦截以及被窃取。加密是由加密过程和解密过程组成的。一般地，发送方在发送消息前先用加密程序将明文加密成密文，接收方在接收到消息后，用解密程序将密文再解密成明文。所以说，解密是加密的逆过程。在进行加密过程时需要两个输入项：一个是明文，还有一个是称为加密密钥的独立数据值。与此类似，解密过程则需要密文和解密密钥。密钥从表面上来看就像是一串随机的二进制位串，密钥的长度即位数取决于特定的加密系统。加密最明显的作用就是提供机密性。这里，明文代表了未经保护的敏感数据，而相应的密文则可以在不被信任的环境中传输，因为如果加密系统比较好的话，那些没有解密密钥的人就无法把密文恢复成明文，从而密文对他来说根本就没有意义。除了提供机密性外，加密系统还可以提供其他安全功能。 加密系统有两种基本的形式：对称加密系统，也称为私有密钥加密系统；不对称加密系统，也称为公开密钥加密系统。两种加密系统有不同的特点，采用不同的方式来提供安全服务。 一、对称加密系统 （一）对称加密对称 加密系统早在 20 世纪 70 年代就开始在商业网络中运用了。对称加密又叫做私

有密钥加密，其特点是数据的发送方和接收方使用的是同一把私有密钥，即把明文加密成密文和把密文解密成明文用的是同一把私有密钥。利用私有密钥进行对称加密的过程是：首先发送方用自己的私有密钥对要发送的信息进行加密；接着发送方将加密后的信息通过网络传送给接收方；然后接收方用发送方进行加密的那把私有密钥对接收到的加密信息进行解密，得到信息明文。 对称加密系统对于一个比较好的对称加密系统来说，除非在解密时能提供正确的密钥，否则是不可能利用解密功能来获得明文信息的。对称加密系统既可以对密码块进行操作，也可以对密码流进行操作。在密码块加密方式中，加密是对 n 位长度的固定大小的明文块进行操作，形成也是 n 位长度的固定大小的密文块。这里，n 的长度一般为 64 或 128 位。解密则是对 n 位长度的密文块进行操作，形成 n 位长度的明文块。在密码流加密方式中，加密是对明文信息或任意长度的数据流进行操作，形成同样长度的密文。密码流加密一般是将数据作为字符序列进行处理，这里的一个字符可以是一位，也可以是某个固定长度的位数。密码流一般是建筑在密码块的基础之上的，所以可以根据各种不同的密码块的运作模式来定义密码流的功能。由美国联邦政府和 ISO 标准定义的密文块链（CBC）和密文反馈（CFB）是两种常用的操作模式。使用对称加密对信息进行加密和解密的速度很快，效率也很高，但需要仔细保存密钥。 使用对称加密技术可以简化加密的处理，进行电子商务的交易双方不必彼此研究和交换专用的加密算法，而可以采用相同的加密算法并只需要交换共享的专用密钥。如果进行通信的双方能够确保专用密钥在密钥交换阶段未曾泄露过，那

么数据的机密性和完整性就可以通过随数据一起发送的数据摘要来实现。由于加密与解密有着共同的算法，从而计算速度非常迅速，且使用方便，计算量小，加密效率高，所以对称加密算法广泛用于对大量数据文件的加密过程中。对称加密技术的主要缺点是密钥的管理比较困难，因为交易双方必须要持有同一把密钥，且不能让他人知道。一旦密钥泄露，则信息就失去了保密性，发送方和接收方再进行通信就必须要使用新的密钥。而把新密钥发送给接收方也是件困难的事情，因为必须要对传送的新密钥进行加密，而这就又要求有一把新密钥。采用私有密钥的另一个问题是其规模很难适应互联网这样的大环境，因为如果某一交易方有 n 个贸易关系的话，那他就要维护 n 把专用密钥，因为每把密钥对应了一个交易方。 （二）对称加密算法 对称加密算法有很多，下面是几种常见的对称加密算法： 1、 数据加密标准（DES） DES 于 1977 年被接纳为美国联邦标准，又于 1981 年被采纳为金融业标准，是近 20 年来用于保护不加密的政府信息和金融业交易信息的主要算法。DES是一种密码块加密方法，采用了64位长度的数据块和56位长度的密钥。DES可以有效地抵御攻击，从其诞生一直到1998年都没有被公开破解过。但是1998年，Electronic Frontier基金会耗资250000美元建造了一个用来破解 DES算法的处理器，名叫“ Deep Crack ”。“ Deep Crack ”能在三天的时间里击败 RSA安全公司的挑战，破解 DES 密钥。随后，解决类似的挑战就变得更快更容易了。 2、 高级加密标准（AES） 基于对 DES 存在某些缺陷的认识，1997 年美国商务部开始了 AES 研究项目，该研究项目的目的是要建立更强大的算法标准来代替 DES。AES 是一种密码

块加密方法，可以对 28 位的密码块进行处理，密钥的长度可以是 128、192 和256 位。AES 算法是根据比利时密码专家 Joan Daemen 博士和 VincentRiijmen博士设计的 Rijndael密钥系统来定义的，目的是希望成为被正式采纳的政府标准，并最终能够被广泛地应用。 3、三重 DES 使用多重加密方法可以增加 DES 的有效密钥长度。三重 DES 加密首先用密钥 a对 64 位的信息块进行加密，再用密钥 b 对加密的结果进行解密，然后用密钥 c对解密结果再进行加密。其中使用了两个或三个 56 位的密钥（密钥 a和密钥 c有时是相同的）。通常人们认为这种算法要比 DES 更强大。但是三重DES 也有一个缺点，那就是需要使用相对较多的处理器资源，尤其是在使用软件进行处理时更是如此。 （三）消息验证码 假定从发送方发送给接收方的消息不需要保密，但接收方需要确信该消息不是伪造的，这就可以用消息验证码（MAC）来进行必要的保护。消息验证码也称为完整性校验值或信息完整校验。MAC 是附加的数据段，是由消息的发送方发出，与明文一起传送并与明文有一定的逻辑联系。MAC 的值与输入消息的每一位都有关系，如果在消息中的任何一位 MAC 生成后发生了改变，则就会产生出不同的 MAC 值，接收方就能知道该消息的完整性已遭到了破坏。 基于收到的信息，接收方利用信息内容重新计算 MAC，并比较两个 MAC值。这类似于用于通信系统的普通错误校验过程，例如，在消息上附加一个称为循环冗余校验值（CRC）的数据字段。不过这里有一个主要的不同，即必须考虑到可能会发生的蓄意攻击。如果某个主动的攻击者改变了消息，那就无法防止攻击者重新计算和替换附加在消息中的 CRC，接收方也就不可能觉察出数据已被篡改

。为防止这类攻击，生成 MAC 时需要使用一个消息接收方也知道的密钥。接收方拥有可以生成 MAC 的密钥，在接收消息时可以对消息内容与 MAC是否一致进行确认。这样，如果消息被篡改了，就肯定能检查出来。常用的两种生成 MAC 的方法是：（1）基于散列函数的方法：对某个位串运用散列函数生成 MAC，该位串中既包含了消息数据位，又包含了数据的加密密钥。这种方法称为密钥散列函数HMAC。（2）基于对称加密的方法：使用对称加密系统来生成 MAC。这一方法已在1986 年形成标准，并广泛应用于金融行业。 二、不对称加密系统 （一）公开密钥加密 不对称加密又叫做公开密钥加密，需要采用两个在数学上相关的密钥对公开密钥和私有密钥来对信息进行加解密。公开密钥加密技术是在 1976 年由斯坦福大学的 Whitfield Diffie 和 MartinHellman 提出来的。与对称加密系统相比，公开密钥加密技术需要使用一对相关的密钥：一个用来加密，另一个用来解密。该技术的设想是，密钥对是与相应的系统联系在一起的，其中私有密钥是由系统所保密持有的，而公开密钥则是公开的，但知道公开密钥并不能推断出私有密钥。依据公开密钥是用作加密密钥还是解密密钥，公开密钥加密系统有两种基本的模式：加密模式和验证模式。 1、加密模式 在加密模式中，公开密钥系统对于信息的加密和解密过程为：（1）发送方用接收方的公开密钥对要发送的信息进行加密；（2）发送方将加密后的信息通过网络传送给接收方；（3）接收方用自己的私有密钥对接收到的加密信息进行解密，得到信息明文。在这一过程中，只有真正的接收方才能解开密文，因为私有密钥是在接收方的手中。这一点似乎和对称加密很相似，但不同处

在于任何拥有该接收方公开密钥的发送方都可以向该接收方发送信息，而不是仅限于与接收方拥有同一把密钥的发送方。 2. 验证模式 在验证模式中，公开密钥系统对于信息的加密和解密过程为：（1）发送方用自己的私有密钥对要发送的信息进行加密；（2）发送方将加密后的信息通过网络传送给接收方；（3）接收方用发送方的公开密钥对接收到的加密信息进行解密，得到信息明文。公开密钥系统：验证模式在这个过程中，任何能够成功地解密接收到的密文的接收方，都能肯定该消息确实是来自发送方，因为只有发送方才拥有与解密公钥相对应的加密私钥，从而验证了该信息确实来自发送方。通过使用私有密钥作为加密密钥，公开密钥加密系统可以用来进行数据发送方的验证并确保信息的完整性。这种公开密钥加密系统的验证模式为数字签名系统奠定了基础。一般来说，既能以加密模式又能以验证模式运作的公开密钥加密系统被称为可逆的公开密钥加密系统。有些公开密钥加密系统只能运作在验证模式而不能运作在加密模式，这种系统被称为不可逆的公开密钥加密系统。与对称密钥加密系统相比，公开密钥加密系统的功能更为强大。但公开密钥加密系统对算法的设计提出了更高的挑战，因为公开密钥代表了在攻击该算法时所要用到的额外信息。现有的公开密钥系统依赖的是假设某个特定已知的数学问题是很难解决的。百考试题收集 （二）RSA 算法 目前著名的公开密钥加密系统是于 1977 年由美国麻省理工学院的三位教授 Ronald Rivest、AdiShamir、Leonard Adleman 联合发明的，所以一般把三位教授姓名的首位字母结合起来，称其为 RSA 加密算法。RSA 算法是一种可逆的公开密钥加密系统。它是通过一个称为公

共模数的数字来形成公开密钥的，公共模数是通过两个形成私人密钥的两个质数的乘数来获得的。一个 RSA 密钥对是这样计算的：选择一个整数 e作为公共指数，再任选两个很大的质数 p和 q，它们满足如下条件：即（p-1）与 e没有公约数，（q-1）与 e也没有公约数。公共模数 n 是 p与 q的乘积，即 n=pq。由 n 和 e共同组成公开密钥。然后确定一个私有指数 d，使（de-1）可被（ p -1）和（ q -1）整除。由 n和 d（或者 p，q和 d）共同组成私有密钥。公共指数和私有指数极为重要，根据模数算法，d 是 e的反函数。也就是说，对于任意的信息 M，有：（Me）dmod n =M mod n对信息 M 的加密过程涉及对 Memod n 的计算。只要知道了公开密钥，即 n和 e，就可以加密。而解密信息M`的过程则涉及对 M`dmod n 的计算，这时需要使用私有密钥。RSA 的安全性依赖于，寻找较大的质数相对容易，但要找到积为该数字的两个因数却很困难。如果该数字相当大，则寻找因数需要大量的处理资源，想要计算所有的范围是不可能的。举一个直观的例子，假设要求你取出 437 的两个因数，也就是找到哪两个数相乘等于 437，大多数人会发现即使借助计算器和数学计算也很难得到这个答案。但是，如果要求计算 23 乘以 19 的积，同样的问题很快就能得到解决，答案是 437。虽然有些人能用心算，但当数据非常大，如达到成千上百位的时候，即使是计算机也很难计算出它们的因数来。RSA 的强度经常受到怀疑，因为破解它的方法非常清楚：可以用任何已知的因式分解方法来分解该模数。因此，RSA 的强度主要依赖于分解因数所需要的时间和设备成本。在将来考虑 RSA 的强度时必须要考虑到设备成本正在不断下降、因子分解技术正在不断提高这两点。

在破解 RSA 方面比较著名的事件发生在 1999 年。由 RSA 算法的创始人 Rivest、Shamir、Adleman 提出的 RSA-155数字，通过国际协作，由许多科学家和学生在近 300 台工作站和个人计算机以及一台超级计算机上通过共享处理，最终被分解了出来。分解工作总共花了 5.2个月。作为一种可行的算法，只要增大 RSA 的模数，将大大增加分解因数所需要的代价。就目前而言，1024 位的模数对于大多数的商业用途来说还是足够强大的。若干年后，或许将使用 2048 位的模数密钥，更加增强其安全性。（三）加密与验证模式的结合 对于公开密钥加密系统的两种模式来说，如果只是单独使用其中的一种模式，那就无法在保障信息机密性的同时又验证发送方的身份，但在电子商务的安全中又需要同时实现这两个目的。为此，需要把这两种模式结合起来使用。 两种模式的结合使用过程为：（1）发送方用自己的私有密钥对要发送的信息进行加密，得到一次加密信息；（2）发送方再用接收方的公开密钥对已加密的信息再次加密；（3）发送方将两次加密后的信息通过网络传送给接收方；（4）接收方用自己的私有密钥对接收到的两次加密信息进行解密，得到一次加密信息；（5）接收方再用发送方的公开密钥对一次加密信息进行解密，得到信息明文。 加密与验证模式的结合在这个过程中，发送方为了证明该信息确实是自己发送的，所以用了自己的私有密钥来对信息加密，同时，为了让只有真正的接收方才能解开该消息，所以用了接收方的公开密钥再次对已加密的信息进行加密。接收方收到信息后，首先要用自己的私有密钥才能解开该密文，从而保障了信息的机密性，随后，接收方再用发送方的公开密钥对已解密一次的信息再次解密，

得到真正的信息，从而保证了对于发送方身份的验证。 三、两种加密方法的联合使用 由于公开密钥加密必须要由两个密钥的配合使用才能完成加密和解密的全过程，因而有助于加强数据的安全性。但是，公开密钥加密也有其缺点，主要是加密和解密的速度很慢，用公开密钥加密算法加密和解密同样的数据所花费的时间是利用私有密钥加密算法的 1000 倍。所以，公开密钥加密不适合对大量的文件信息进行加密，一般只适用于对少量数据如对密钥进行加密。正是因为公开密钥加密和私有密钥加密各有所长，所以在实际应用中，往往将公开密钥加密与私有密钥加密算法结合起来使用，以起到扬长避短的目的。 在实际运用中，用户如果要对数据进行加密，需要生成一对自己的密钥对。密钥对中的公开密钥是公开的，但私有密钥则由密钥的主人妥善保管。发送方和接收方在对文件进行加密和解密时的实际过程如下：（1）发送方生成一个私有密钥，并对要发送的信息用自己的私有密钥进行加密；（2）发送方用接收方的公开密钥对自己的私有密钥进行加密；（3）发送方把加密后的信息和加密后的私有密钥通过网络传输到接收方；（4）接收方用自己的私有密钥对发送方传送过来的私有密钥进行解密，得到发送方的私有密钥；（5）接收方用发送方的私有密钥对接收到的加密信息进行解密，得到信息的明文。 因为只有接收方才拥有自己的私有密钥，所以即使其他人得到了经过加密的发送方的私有密钥信息，也无法进行解密，从而保证了这把私有密钥的安全性。在上述过程中，实际上分别实现了两次加密解密过程，即文件信息本身的加密解密和发送方私有密钥的加密解密，这是通过私有密钥加密和公开密钥加密算法的结合

来实现的。 通过公开密钥加密技术实现对发送方私有密钥的管理，使相应的密钥管理变得简单和更加安全，同时还解决了对称加密中存在的可靠性问题和鉴别问题。发送方可以为每次交换的信息生成惟一的一把私有密钥，并用接收方的公开密钥对该密钥进行加密，然后再将加密后的密钥与用该密钥加密的信息一起发送给相应的接收方。由于对每次信息交换都对应生成了惟一的一把密钥，因此，各交易方就不再需要对密钥进行维护和担心密钥的泄露或过期。这种方式的另一优点是即使泄露了一把密钥，也只不过影响一笔交易，而不会影响到交易双方之间所有的交易关系。这种方式还提供了交易伙伴间发布私有密钥的一种安全途径。值得注意的是，能否切实有效地发挥加密系统的作用，其关键点在于密钥的管理，包括密钥的生成、分发、安装、保管、使用以及作废的全过程。F8F8" 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