

· 03 ·

信息安全技术



对称加密技术

- ◆ 对称加密技术：数据的加密和解密的密钥(密码)是相同的，属于不公开密钥加密算法。
- ◆ 对称加密算法有两种基本类型，分别是分组密码和序列密码。分组密码是在明文分组和密文分组上进行运算，序列密码是对明文和密文数据流按位或字节进行运算。
- ◆ 优缺点分析：
 - ◆ 优点是加密速度快，适合加密大数据（大量数据）
 - ◆ 缺点是加密强度不高(因为密钥位数少)，且密钥分发困难(因为密钥还需要传输给接收方，也要考虑保密性等问题)。



对称加密技术

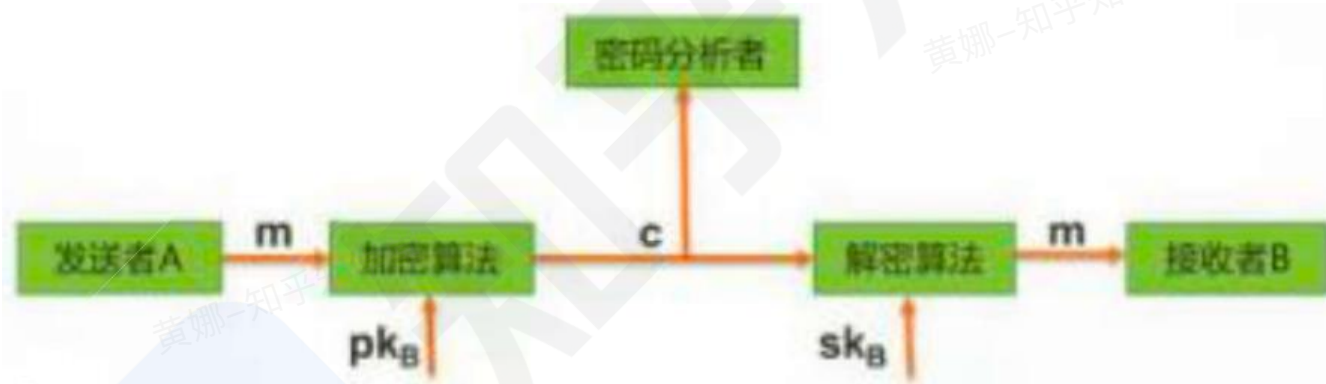
◆ 常见的对称密钥加密算法如下：

- DES (Data Encryption Standard)：美国的数据加密标准，64位密钥（其中8位用于校验，所以也可以说是56位密钥）、明文和密文都是64位分组，DES算法具有很高的安全性，但是可以用穷举搜索法对DES算法进行攻击。
- 3DES (Triple-DES)：使用112位密钥对数据进行三次加密，即用两个56位密钥K1、K2。
 - 发送方加密：K1加密->K2解密->K1加密。
 - 接收方解密：K1解密->K2加密->K1解密
- IDEA (International Data Encryption Algorithm)：国际数据加密算法，128位密钥，明文和密文都是64位，比DES的加密性好，对计算机功能要求相对低。
- AES (Advanced Encryption Standard, AES)：是美国联邦政府采用的一种区块加密标准，这个标准用来替代原先的DES。对其要求是“至少像3DES一样安全”。AES支持128、192和256位3种密钥长度，能够在世界范围内免版税使用，提供的安全级别足以保护未来20~30年内的数据，可以通过软件或硬件实现。
- RC-5：RSA数据安全公司的很多产品都使用了RC-5。



非对称加密技术

- ◆ 非对称加密技术：数据的加密和解密的密钥是不同的，分为公钥和私钥。是公开密钥加密算法。
- ◆ 其缺点是加密速度慢。优点是安全性高，不容易破解，可以适应开放性的使用环境，可以实现数字签名与验证。
- ◆ 非对称技术的原理是：发送者发送数据时，使用接收者的公钥作加密密钥，私钥作解密密钥。这样只有接收者才能解密密文得到明文。安全性更高，因为无需传输密钥。但无法保证完整性。如下：



- ◆ 常见的非对称加密算法如下：

- RSA：512位（或1024位）密钥，计算机量极大，难破解。加密/解密时要进行大指数模运算，因此加密/解密速度很慢，主要用在数字签名中。
- Elgamal、ECC（椭圆曲线算法）、背包算法、Rabin、D-H等。



数字信封

- ◆ 相比较可知，对称加密算法密钥一般只有56位，因此加密过程简单，适合加密大数据，也因此加密强度不高；而非对称加密算法密钥有1024位，相应的解密计算量庞大，难以破解，却不适合加密大数据，一般用来加密对称算法的密钥，这样，就将两个技术组合使用了，这也是数字信封的原理。
- ◆ 数字信封原理：信是对称加密的密钥，数字信封就是对此密钥进行非对称加密，具体过程：发送方将数据用对称密钥加密传输，而将对称密钥用接收方公钥加密发送给对方。接收方收到数字信封，用自己的私钥解密信封，取出对称密钥解密得原文。
- ◆ 数字信封运用了对称加密技术和非对称加密技术，本质是使用对称密钥加密数据，非对称密钥加密对称密钥，解决了对称密钥的传输问题。



考试真题

为保障数据的存储和运输安全，防止信息泄露，对一些数据进行加密。由于对称密码算法()，所以特别适合对大量的数据进行加密。

- A、比非对称密码算法更安全
- C、比非对称密码算法效率更高

- B、比非对称密码算法密钥更长
- D、还能同时用于身份认证

答案：C

考试真题

假设A和B之间要进行加密通信，则正确的非对称加密流程是()。

- ①A和B都要产生一对用于加密和解密的加密密钥和解密密钥
- ②A将公钥传送给B，将私钥自己保存，B将公钥传送给A，将私钥自己保存
- ③A发送消息给B时，先用B的公钥对信息进行加密，再将密文发送给B
- ④B收到A发来的消息时，用自己的私钥解密

A. ①②③④

B. ①③④②

C. ③①②④

D. ②③①④

答案：A

考试真题

DES 是一种()，其密钥长度为 56 位，3DES 是利用 DES 的加密方式，对明文进行 3 次加密，以提高加密强度，其密钥长度是 () 位。

A.共享密钥 B. 公开密钥 C. 报文摘要 D.访问控制

A.56 B.112 C.128 D.168

答案：A、B

试题分析：DES加密是一种对称加密算法，加密与解密密钥相同。由于DES的密钥长度较短，为了提高安全性，就出现了使用112位密钥对数据进行三次加密的算法（3DES），即用两个56位的密钥K1和K2，发送方用K1加密，K2解密，再使用K1加密；接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

考试真题

要对消息明文进行加密传送，当前通常使用的加密算法是（ ）。

A . RSA

B . SHA-1

C . MD5

D . RC5

答案：D

试题分析：

RSA是目前最有影响力和最常用的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准。RSA由于效率问题，一般不直接用于明文加密。

SHA-1与MD5属于信息摘要算法，不能用来加密数据。

RC5是一种对称密码算法，它面向字结构，便于软件和硬件的实现，适用于不同字长的微处理器。



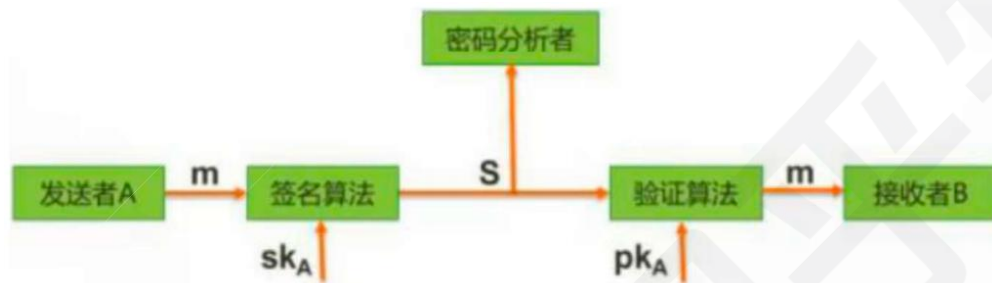
信息摘要

- ◆ 所谓信息（消息）摘要，就是一段数据的特征信息，当数据发生了改变，信息摘要也会发生改变。
- ◆ 信息摘要是由哈希函数生成的，是不可逆的算法。
- ◆ 信息摘要原理：发送方会将数据和信息摘要一起传给接收方，接收方会根据接收到的数据重新生成一个信息摘要，若此摘要和接收到的摘要相同，则说明数据正确。
- ◆ 信息摘要的特点：不管数据多长，都会产生固定长度的信息摘要；任何不同的输入数据，都会产生不同的信息摘要；单向性，即只能由数据生成信息摘要，不能由信息摘要还原数据
- ◆ 信息摘要算法：MD5（信息摘要算法，产生128位的输出）、SHA-1（安全散列算法，对长度不超过264位的消息产生160位的输出，安全性更高）。



数字签名

- ◆ 数字签名：唯一标识一个发送方。发送者发送数据时，使用发送者的私钥进行加密，接收者收到数据后，只能使用发送者的公钥进行解密，这样就能唯一确定发送方，这也是数字签名的过程。如下：



- ◆ 基于对称加密算法和非对称加密算法都可以获得数字签名，但目前主要是使用基于非对称加密算法的数字签名，包括普通数字签名和特殊数字签名。
- ◆ 普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Des/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等，特殊数字签名算法有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名和具有消息恢复功能的签名等，它与具体应用环境密切相关。



数字签名

◆ 数字签名的主要功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生，但无法保证机密性。

◆ 不管使用哪种算法，数字签名必须保证以下三点：

(1) 接收者能够核实发送者对数据的签名，这个过程称为鉴别。

(2) 发送者事后不能抵赖对数据的签名，这称为不可否认。

(3) 接收者不能伪造对数据的签名，这称为数据的完整性。

◆ 用公钥加密，私钥解密，可实现保密通信；用私钥加密，公钥解密，可实现数字签名。



公钥基础设施PKI

- ◆ 公钥基础设施PKI是以非对称密钥加密技术为基础，以数据机密性、完整性、身份认证和行为不可抵赖性为安全目的，来实施和提供安全服务的具有普适性的安全基础设施。
- 1. 数字证书：又称为数字标识，是由签证机构（Certificate Authority, CA）签发的对用户的公钥的认证，是一个数据结构，是一种信息集合。目前，国际上对证书的格式和认证方法遵从X.509体系标准。X.509证书必须包含下列信息：（1）版本号（2）序列号（3）签名算法标识符（4）认证机构（5）有效期限（6）主题信息（7）认证机构的数字签名（8）公钥信息。公钥证书主要用于确保公钥及其与用户绑定关系的安全。这个公钥就是证书所标识的那个主体的合法的公钥。任何一个用户只要知道签证机构的公钥，就能检查对证书的签名的合法性。如果检查正确，那么用户就可以相信那个证书所携带的公钥是真实的，而且这个公钥就是证书所标识的那个主体的合法的公钥。
- 2. 签证机构CA：负责签发证书、管理和撤销证书。是所有注册用户所信赖的权威机构，CA在给用户签发证书时要加上自己的数字签名，以保证证书信息的真实性。任何机构可以用CA的公钥来验证该证书的合法性。



考试真题

数字签名技术属于信息系统安全管理中保证信息 () 的技术。

A、保密性 B、可用性 C、完整性 D、可靠性

答案：C

解析：数字签名是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

甲向乙发送其数据签名，要验证该签名，乙可使用 () 对该签名进行解密。

A.甲的私钥 B.甲的公钥 C.乙的私钥 D.乙的公钥

答案：B



访问控制

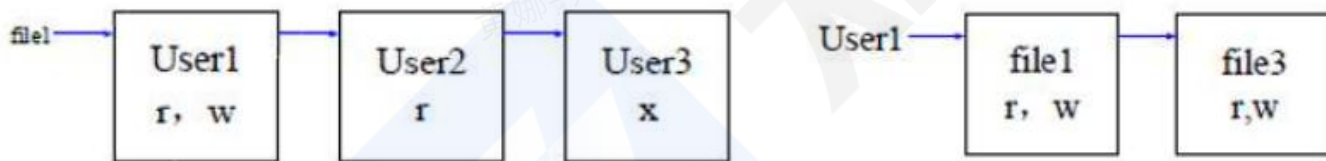
- ◆ **访问控制**是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权访问。访问控制包括3个要素，即主体、客体和控制策略。
- ◆ **访问控制**包括认证、控制策略实现和审计3方面的内容。

① **访问控制矩阵 (ACM)**。是通过矩阵形式表示访问控制规则和授权用户权限的方法。主体作为行，客体作为列。

	file1	file2	file3
User1	rw		rw
User2	r	rwX	x
User3	x	r	

② **访问控制表 (ACL)**。目前最流行、使用最多的访问控制实现技术。每个客体有一个访问控制表是系统中每一个有权访问这个客体的主体的信息。这种实现技术实际上是按列保存访问矩阵。

③ **能力表**。对应于访问控制表，这种实现技术实际上是按行保存访问矩阵。每个主体有一个能力表是该主体对系统中每一个客体的访问权限信息。使用能力表实现的访问控制系统可以很方便地查询某一个主体的所有访问权限。



④ **授权关系表**。每一行 (或者说元组) 就是访问矩阵中的一个非空元素，是某一个主体对应于某一个客体的访问权限信息。如果授权关系表按主体排序，查询时就可以得到能力表的效率；如果按客体排序，查询时就可以得到访问控制表的效率。