

NEW PLAN

软考系统架构师

· — 段 新 征 程 ·



• 1.9.1 •

加密技术和认证技术



对称加密技术

信息的发送方和接收方使用同一个密钥去加密和解密数据。

特点：算法公开、加密和解密速度快，适合于对大数据量进行加密。

加密过程：明文+加密算法+私钥= $\rightarrow$ 密文

解密过程：密文+解密算法+私钥= $\rightarrow$ 明文

常见的对称加密算法：

DES、3DES、RC、IDEA、PGP、AES

缺点：加密强度不够、密钥安全管理困难



非对称加密技术

非对称加密与对称加密相比，其安全性更好。对称加密的通信双方使用相同的密钥，如果一方的密钥遭泄露，那么整个通信就会被破解。而非对称加密使用一对密钥，即公钥和私钥，且二者成对出现。私钥被自己保存，不能对外泄露。公钥指的是公共的密钥，任何人都可以获得该密钥。用公钥或私钥中的任何一个进行加密，用另一个进行解密。

常见的非对称加密算法：RSA、DSA、ECC（椭圆曲线算法）等。



非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要，但加密和解密花费的时间长、速度慢，不适用于对文件加密，而只适用于对少量数据进行加密。



信息摘要

- ◎ 信息摘要简要地描述了一份较长的信息或文件，它可以被看作一份长文件的“数字指纹”信息摘要用于创建数字签名，对于特定的文件而言，信息摘要是唯一的。
- ◎ 信息摘要可以被公开，它不会透露相应文件的任何内容。
- ◎ 原始数据不同，生成的摘要一定不同，单向不可逆。

信息摘要算法	哈希值长度	安全性
MD5	128bit	 低
SHA-1	160bit	
SHA-256	256bit	



数字签名

数字签名采用非对称密码体制（公钥密码体制），即发送者使用私钥加密数据，接收者使用对应的公钥解密数据，它具有以下功能：

- ①报文鉴别：用于证明来源，接收者可以通过签名确定是哪个发送者进行的签名；
- ②防止抵赖：防止发送者否认签名，发送者一旦签名，标记就打上了，无法抵赖；
- ③防止伪造：防止接收者伪造发送者的签名。



练习题

下列算法中属于非对称加密算法的是（ ）。 （2021年上半年）

A.DES

B.RSA

C.AES

D.MD5

参考答案： B

THE END

功不唐捐，玉汝于成！

• 开 启 新 征 程 •

