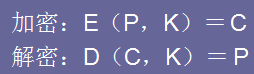
**大概念**：

对称算法

同一个密钥可以用作信息的加密和解密。

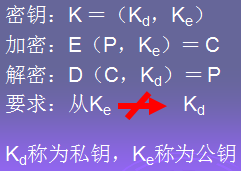
在对称加密算法中，数据发信方将明文（原始数据）和加密密钥（mi yao）一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原文，则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。



常用的算法有：DES、3DES、TDEA、Blowfish、RC2、RC4、RC5、IDEA、SKIPJACK、AES等

非对称算法

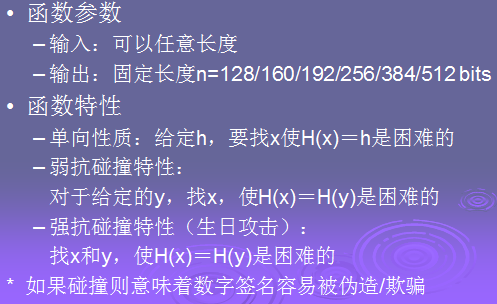
非对称加密算法需要两个密钥来进行加密和解密，这两个秘钥是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥）



认证码

消息认证码MAC，发送方利用密钥从明文产生一个固定长度的短数据块（MAC），和消息一起传输。接收方考察是否一致，以判断MAC和/或消息是否被改动过。

散列函数



签名

**小词汇**：

wireshark，

[网络封包](http://baike.baidu.com/view/6102086.htm)分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。

会话密钥、

保证用户跟其它计算机或者两台计算机之间安全通信会话而随机产生的加密和解密密钥。会话密钥有时称对称密钥，因为同一密钥用于加密和解密。

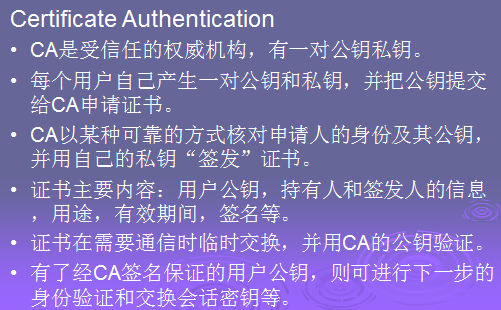
混合密码体制、

混合密码体制指用公钥密码加密一个用于对称加密的短期密码，再由这个短期密码在对称加密体制下加密实际需要安全传输的数据。

公钥/私钥/证书/CA、

公钥（Public Key）与[私钥](http://baike.baidu.com/view/493846.htm" \t "_blank)（Private Key）是通过一种算法得到的一个[密钥](http://baike.baidu.com/view/934.htm" \t "_blank)对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。

公钥的发布体制---证书体系(CA)，是PKI的核心和基础。



分组算法、

明文被分为固定长度的块（即分组），对每个分组用相同的算法和密钥加/解密。分组一般为64比特，或者也可变长。密文分组和明文分组同样长。

流算法、

使用密钥为种子产生伪随机序列并和明文XOR产生密文，两次异或即解密。

单表算法（monoalphabetic），

在加密时用一张自制字母表上的字母来代替明文上的字母（比如说A——Z，B——D）来达到加密。

LFSR、

[线性反馈移位寄存器](https://www.baidu.com/s?wd=%E7%BA%BF%E6%80%A7%E5%8F%8D%E9%A6%88%E7%A7%BB%E4%BD%8D%E5%AF%84%E5%AD%98%E5%99%A8&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YkP16zP1FBP1F9PWDkrHI-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3ErH0YPHfkn16)(LFSR)是一个产生二进制位序列的机制。这个寄存器由一个初始化矢量设置的一系列信元组成，最常见的是，密钥。

DES：

DES算法把64位的明文输入块变为数据长度为64位的密文输出块，其中8位为奇偶校验位，另外56位作为密码的长度。首先，DES把输入的64位数据块按位重新组合，并把输出分为L0、R0两部分，每部分各长32位，并进行前后置换，最终由L0输出左32位，R0输出右32位，根据这个法则经过16次迭代运算后，得到L16、R16，将此作为输入，进行与初始置换相反的逆置换，即得到密文输出。

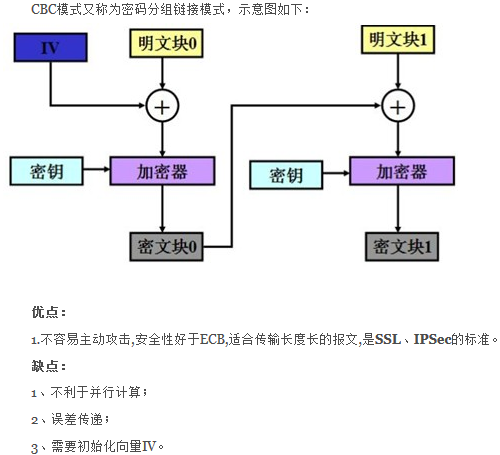
3DES、

AES、

S-Box、

密码置换盒，256项\*32bits，二级加密装置。把二进制数输入S-box，它们就会转化为既定的数字。

CBC、



ECB、

ECB（Electronic Codebook，电码本）模式是分组密码的一种最基本的工作模式。在该模式下，待处理信息被分为大小合适的分组，然后分别对每一分组独立进行加密或解密处理。

IV、

在有线等效保密（[WEP](http://baike.baidu.com/view/32853.htm)）协议中，IV是用来和密钥组合成密钥种子，作为RC4算法的输入，来产生加密字节流对数据进行加密的。标准的64比特WEP使用40比特的钥匙接上24比特的初向量(Initialization Vector，IV) 成为 RC4 用的钥匙。

Salt、

在密码学中，是指通过在密码任意固定位置插入特定的字符串，让散列后的结果和使用原始密码的散列结果不相符，这种过程称之为“加盐”。

nonce、

在密码学中Nonce是一个只被使用一次的任意或非重复的随机数值，在加密技术中的初始向量和加密散列函数都发挥着重要作用，在各类验证协议的通信应用中确保验证信息不被重复使用以对抗重放攻击(Replay Attack)。

RC4、

密钥长度可变的流加密算法簇。其核心部分的S-box长度可为任意，但一般为256字节。该算法的速度可以达到[DES](http://baike.baidu.com/view/7510.htm" \t "_blank)加密的10倍左右，且具有很高级别的非线性。

MD5、

MD5即Message-Digest Algorithm 5（信息-摘要算法5），用于确保信息传输完整一致。是计算机广泛使用的哈希算法之一，主流编程语言普遍已有MD5实现。将数据（如汉字）运算为另一固定长度值，是杂凑算法的基础原理，MD5的前身有MD2、MD3和MD4。

SHA1、

安全[哈希算法](http://baike.baidu.com/view/273836.htm" \t "_blank)（Secure Hash Algorithm）主要适用于[数字签名](http://baike.baidu.com/view/7626.htm" \t "_blank)标准 （Digital Signature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。对于长度小于2^64位的消息，SHA1会产生一个160位的[消息摘要](http://baike.baidu.com/view/2396437.htm" \t "_blank)。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，那么这时候就会产生不同的消息摘要。



SHA2、

MAC、

消息认证码，发送方利用密钥从明文产生一个固定长度的短数据块（MAC），和消息一起传输。接收方考察是否一致，以判断MAC和/或消息是否被改动过。

HMAC、

带Key的Hash函数，利用HASH函数从报文和密钥产生MAC码。

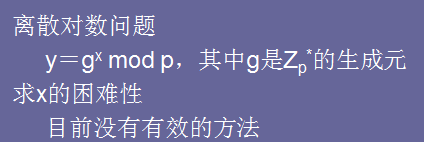
Diffie-Hellman key agreement protocol、

Diffie-Hellman密钥交换协议/算法，这种密钥交换技术的目的在于使得两个用户安全地交换一个秘密密钥以便用于以后的报文加密. Diffie-Hellman密钥交换算法的有效性依赖于计算离散对数的难度.

Challenge–response authentication、

一般用户之间的基于共享秘密的鉴别，这个思路也用在基于公钥的鉴别体制中。

离散对数问题DLP、



整数分解问题Integer factorization、

给出一个正整数，将其写成几个素数的乘积。

SSL/OpenSSL/HTTPS、

SSL协议位于[TCP/IP协议](http://baike.baidu.com/view/7649.htm" \t "_blank)与各种[应用层](http://baike.baidu.com/view/239619.htm)协议之间，为[数据通讯](http://baike.baidu.com/view/1474554.htm)提供安全支持。

Secure Socket Layer，为[Netscape](http://baike.baidu.com/view/153922.htm" \t "_blank)所研发，用以保障在Internet上数据传输之安全，利用[数据加密](http://baike.baidu.com/view/696431.htm" \t "_blank)(Encryption)技术，可确保数据在网络上之传输过程中不会被截取及窃听。

OpenSSL 是一个安全[套接字](http://baike.baidu.com/view/538713.htm" \t "_blank)层密码库，囊括主要的[密码算法](http://baike.baidu.com/view/8790.htm)、常用的[密钥](http://baike.baidu.com/view/934.htm)和证书封装管理功能及[SSL](http://baike.baidu.com/view/16147.htm)协议，并提供丰富的应用程序供测试或其它目的使用。

HTTPS（全称：Hyper Text Transfer Protocol over Secure Socket Layer），是以安全为目标的[HTTP](http://baike.baidu.com/view/9472.htm" \t "_blank)通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL。

VPN/OpenVPN、

虚拟专用网络的功能是：在[公用网络](http://baike.baidu.com/view/11793923.htm" \t "_blank)上建立[专用网络](http://baike.baidu.com/view/2150902.htm)，进行[加密](http://baike.baidu.com/view/40927.htm)通讯。PN网关通过对[数据包](http://baike.baidu.com/view/25880.htm)的加密和数据包目标地址的转换实现[远程访问](http://baike.baidu.com/view/183974.htm)。

penVPN无疑是Linux下开源VPN的先锋，提供了良好的性能和友好的用户GUI。OpenVPN 是一个基于 OpenSSL 库的应用层 VPN 实现。和传统 VPN 相比，它的优点是简单易用。

PGP/GPG、

PGP(Pretty Good Privacy)，是一个基于RSA公钥加密体系的邮件[加密软件](http://baike.baidu.com/view/586876.htm" \t "_blank)。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上[数字签名](http://baike.baidu.com/view/7626.htm)从而使收信人可以[确认](http://baike.baidu.com/subview/346882/19980122.htm)邮件的发送者，并能确信邮件没有被篡改。

GPG是加密和数字签名的免费工具，大多用于加密信息的传递。除了仅用密码加密外，GPG最大的不同是提供了“公钥/私钥”对

分布式拒绝服务攻击(DDoS)、

分布式拒绝[服务](http://baike.baidu.com/view/133203.htm" \t "_blank)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

rootkit、

Rootkit是一种特殊的[恶意软件](http://baike.baidu.com/view/362867.htm" \t "_blank)，它的功能是在安装目标上隐藏自身及指定的文件、进程和[网络链接](http://baike.baidu.com/view/3220831.htm)等信息，比较多见到的是Rootkit一般都和[木马](http://baike.baidu.com/view/931.htm)、[后门](http://baike.baidu.com/view/20922.htm)等其他恶意程序结合使用。

BOF、

(Before of File)指示当前记录位置位于 Recordset 对象的第一个记录之前。

74/75 crack、

(PKCS)是由美国RSA[数据安全](http://baike.baidu.com/subview/2308446/2308446.htm)公司及其合作伙伴制定的一组公钥密码学标准

PKCS#5、

描述一种利用从口令派生出来的[安全密钥](http://baike.baidu.com/view/5095671.htm" \t "_blank)加密字符串的方法。使用MD2或MD5 从口令中派生密钥，并采用DES-CBC模式加密。主要用于加密从一个计算机传送到另一个计算机的私人密钥，不能用于加密消息

PKCS#3、

定义[Diffie-Hellman](http://baike.baidu.com/subview/551692/551692.htm)[密钥](http://baike.baidu.com/view/934.htm)交换协议

PCKS#1

定义RSA[公开密钥](http://baike.baidu.com/view/1145160.htm)算法加密和签名机制，主要用于组织[PKCS#7](http://baike.baidu.com/view/886424.htm)中所描述的[数字签名](http://baike.baidu.com/view/7626.htm" \t "_blank)和[数字信封](http://baike.baidu.com/view/22171.htm)

**问答**

1. 对称密码算法的基本要素：substitution和transposition；现代对称算法的基本特点和元素。

代换（替代）：明文元素映射为密文元素

置换：把明文元素重排

5个基本元素：明文、密文、密钥、加密算法、解密算法

特征：运算类型：代换、置换

密钥：对称密钥非对称密钥、密钥空间的大小

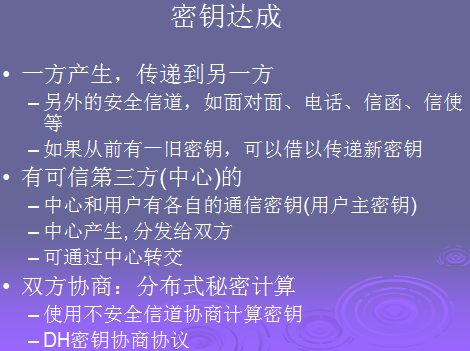
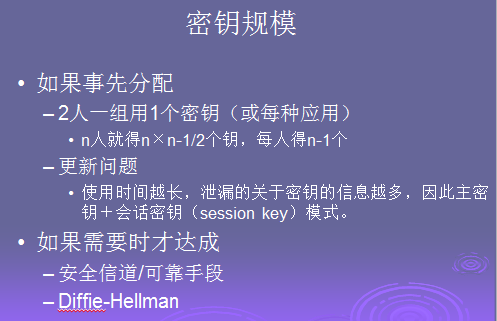
处理明文的方法：分组算法、流算法

基本原则：算法公开、密钥的随机性

1. 对称算法DES/AES/RC4/3DES的基本结构，以及安全特性与适用场合。

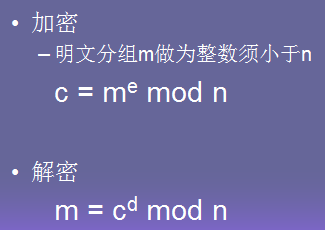
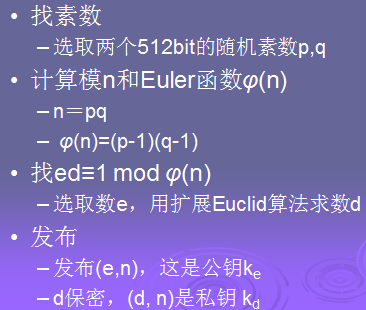
http://wenku.baidu.com/link?url=7UXiTIFbH18Ei4QQd3U2LUwT42I3uE8LNONgqAghUENVKZyT4WdIiIj1ZK1ATRU6djyOxUc6yLwoAcAE48H1jC74PJb0ssQuWfeYzFiPoXS

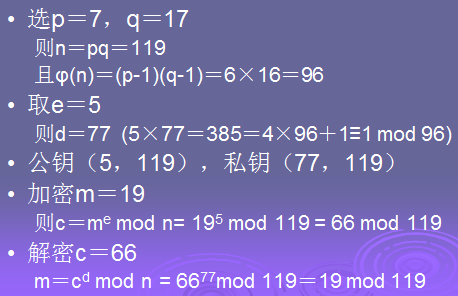
1. 对称密钥的达成方法。

Diffie-hellman

1. 密码算法与协议中的数学元素：模运算、逆元、群、多项式环、DLP、IF等。
2. RSA，从原理机制到计算。





1. ECC，从DLP开始到签名
2. 总结一下数学元素：RSA/DLP问题，XymodZ/CRT定理，Lagrange插值等
3. 加密应用方案：从pkcs#5到PGP，到“文件夹加密大师”。
4. 结合具体实例分析，考虑比如这3个应用：电商及网银、无纸化办公、QQ或微信。有哪些安全问题和需求、目前是怎么做得，仍存在什么安全问题，该怎么注意安全，该怎么改进或解决。
5. 系统安全方面，考虑和分析一些需求背景和案例，比如对于恶意程序/漏洞的机制与防范、打击和抑制盗版等。
6. 登录专题
7. 《网络安全法》专题