密码学·技术机制（上）

——中国密码学会 组编

AES（Advanced Encryption Standard）美国联邦信息处理标准规定的一种分组密码算法，分组长度为 128 比特，支持 3 种密钥长度：128、192 和 256 比特长的密钥。

非对称密码算法/公钥密码算法(Asymmetric cryptography algorithm/public key crytography algorithm）加解密使用不同密钥的密码算法。其中一个密钥（公钥）公开，另一个密钥（私钥）必须保证保密，且由公钥求解私钥是不可行的。

生日攻击（Birthday attack）一种主要针对密码杂凑算法的攻击方法，试图找出两个具有相同杂凑值的消息（即找到一个碰撞）。

盲签名（Blind signature）一种特殊的数字签名，所签的消息对签名者是不可知的。

分组密码算法（Block cipher algorithm）又称块密码算法，一种对称密码算法，将明文划分成固定长度的分组进行加密。

分组密码算法工作模式 (Block cipher operation mode)分组密码算法的使用方式，主要包括电码本模式（ECB）、密码分组链接模式（CBC）、密码反馈模式（CFB）、输出反馈模式（OFB）、计数器式（CTR）等。

认证机构（Certification Authority, CA）产生、签发和注销数字证书的第三方机构，也可以为用户生成密钥。

证书签发中心（Certificate issue center）生成证书的机构。

证书撤销列表（Certificate Revocation List, CRL）失效证书的列表，由一个认证机构发布。

证书注册中心（Certificate register center）接收公钥证书的申请、注销和查验申请材料的机构。

密码分组链接工作模式（Cipher Block Chaining （CBC） operation mode）分组密码算法的一种工作模式，当前的明文分组与前一密文分组进行异或运算后再进行加密得到当前密文分组。

密码反馈工作模式（Cipher Feedback（CFB）operation mode）分组密码算法用于构造序列密码的一种工作模式。用密文依次更新存储该密码算法启动变量的反馈缓冲器。

计数器工作模式（Counter (CTR) operation mode）分组密码算法用于构造序列密码的一种工作模式。通过加密不断变化的计数器来产生密钥序列。

DES（Data Encryption Standard）美国联邦信息处理标准规定的一种分组加密算法。明文与密文分组长度为 64 比特，有效密钥长度为 56 比特。

数据源鉴别（Data origin authentication）确认接收到的数据的来源是所声称的。

字典攻击（Dictionary attack）一种攻击方式，遍历由可能的密钥组成的字典中的所有条目，以猜测密钥。

差分密码分析（Differential cryptanalysis）一种选择明文攻击，通过分析特定明文差分对相应的密文差分的影响，以获得可能性最大的密钥。

差分能量分析（Differential Power Analysis , DPA）一种密码分析方法，使用统计方法和纠错技术等对密码设备功耗的变化进行分析，以提取密码算法中有关密钥的信息。

Diffie-Hellman 算法（Diffie-Hellman algorithm）基于有限域离散对数问题的一种算法，可用于密钥协商。

电码本工作模式（Electronic CodeBook(ECB) operation mode）分组密码算法的一种工作模式，明文分组直接作为加密算法的输入，对应的输出作为密文分组。

椭圆曲线密码算法（Elliptic Curve Cryptography（ECC）algorithm）基于有限域上的椭圆曲线离散对数问题的密码算法。

椭圆曲线 DH 密钥协商协议（Elliptic Curve Diffie-Hellman（ECDH）key agreement）使用椭圆曲线密码算法实现 Diffie-Hellman 密钥协商的协议。

端到端加密（End-to-end encryption/encipherment）数据在源端进行加密，解密只发生在目的端。

实体鉴别（Entity authentication）确认一个实体所声称的身份。

Feistel 结构（Feistel structure）一种典型的迭代分组密码结构，将明文分成等长的两部分，每轮只处理一部分然后进行交换。其特点为解密交换和加密交换相同，只是子密钥使用的次序相反。