密码学·一般概念（中）

——中国密码学会 组编

密码学（Cryptology）：研究编制、分析和破译密码的学科，包括密码算法、密码协议和密码系统等的设计与分析的原理、方法和工具。

密码系统（Cryptosystem）：由算法、协议、部件、设备及相关的技术等构成的整体，以实现某种密码功能（如加密/解密、签名/验证等）。

数据完整性（Data integrity）：数据没有遭受以非授权方式所作的篡改或破坏的性质。

解密（Decipherment/Decryption）：加密过程对应的逆过程。

扩散（Diffusion）：一种密码设计准则，输入的每一个比特的改变都会引起输出的多个比特发生改变。

数字签名（Digital signature）：附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被人（例如接收者）进行伪造。

$$\mathbb{F}_q^*$$

有限域离散对数问题（Discrete logarithm problem over finite field）：给定一个有限域和的一个生成元 g，对于的任意一个元素 h，求整数 a<q，使得 h=。

椭圆曲线离散对数问题（Discrete logarithm problem over elliptic curve）：椭圆曲线上所有的有理点外加一个无穷远点的特殊点构成的集合，按给定的加法运算构成一个 Abel 群。给定椭圆曲线 E 上一个阶为 n 的基点 P，且点 Q 属于由 P 点生成的 n 阶循环群，求整数 m，使得 Q=mP。

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

椭圆曲线（Elliptic curve）：数域上的维尔斯特拉斯方程：所确定的平面曲线。

加密（Encipherment/Encryption）：对数据进行密码变换以产生密文的过程。

有限域（Finite field）：由有限个元素组成的域。

前向保密性（Forward secrecy）：密码协议的一种属性，当前密钥泄露不影响以前使用的密钥的安全性。

初始化向量/值（Initialization vector/ Initialization value IV）：在密码交换中，为增加安全性或使密码设备同步引入的用于数据变换的起始数据。

Kerckhoffs 假设（Kerckhoffs' assumption/principle）：假定除秘密密钥之外的全部密码算法

的细节是已知的。

密钥（Key）：控制密码变换操作的关键信息或参数。

密钥协商（Key agreement/negotiation）：两个或多个实体在一个公开的信道上通过相互传送一些消息来共同建立一个共享的秘密密钥的协议。该秘密密钥是每个实体提供的消息的函数，而各个实体无法预先确定这个秘密密钥的值。

密钥确认（Key confirmation）：一个实体确信另一个已识别的实体拥有正确的密钥。

密钥周期（Key cycle）：密钥从产生开始到最终被销毁的整个生命周期。

密钥销毁（Key destruction）：将密钥通过物理或逻辑的方式消除，使其无法再恢复。

密钥加密密钥（Key-encrypting key）：又称二级密钥（Secondary key）或密钥传送密钥（Key transport key），用于对密钥进行加解密。

密钥托管（Key escrow）：通信加密的密钥可在特殊情况下被授权的第三方获得的一种安全监控管理机制。

密钥建立（Key establishment）：通信实体间建立共享密钥的过程，包括密钥协商和密钥传送等。

密钥交换（Key exchange）：通信实体间交换密钥的过程。

密钥生存期（Key lifetime）：密钥被正常使用的时间。

密钥恢复（Key recovery）：获取使用过的密钥的过程。