密码学·技术机制（中）

——中国密码学会 组编

有限自动机密码（Finite State Machine, FSM）基于可逆有限自动机理论构造的密码算法。

群签名（Group signature）允许群中任何一个成员代表该群签名，该签名可用群公钥公开验证而不泄露签名者的身份。在发生纠纷时，只有特定的群管理员可以打开签名，确认签名成员的身份。

IDEA（International Data Encipher Algorithm）一种分组密码算法，是欧洲的密码标准，明文和密文分组长度均为 64 比特，密钥长度为 128 比特。

IKE（Internet Key Exchange Protocol）由 IETF（互联网工程任务组，The Internet Engineering Task Force）制定的密钥协商协议，定义了通信双方进行身份鉴别、协商加密算法以及生成共享的会话密钥的一种方法。

IPSec 协议（Internet Protocol Security）：由 IETF 设计的端到端的确保基于 IP 通信数据安全性的一种网络层协议，可以提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务，可弥补 TCP/IP 协议体系的安全漏洞。

ISAKMP 协议（Internet Security Association and Key Management Protocol）：IPSec 协议中使用的一种安全联系和密钥管理协议，用于在两个主机间通信时鉴别通信身份和协商安全参数。

密钥分发中心（Key Distribution Center KDC）：一种集中式密钥管理中的可信方，提供集中式的密钥生成并分发给用户。

带密钥的杂凑函数（Keyed hash function）：一种密码杂凑函数，密钥作为其输入参数之一，输出值随密钥而变化。

密钥产生函数（Key generating function）：含秘密参数的多输入函数，其输出是密钥。在未知秘密参数时，推导出密钥是计算不可行的。

密钥管理（Key management）：根据安全策略，对密钥的产生、登记、认证、注销、分发、安装、存储、归档、撤销、衍生和销毁等操作制定并实施一组确定的规则。

密钥管理中心（Key Management Center KMC）：负责密钥管理的可信方。

密钥序列（Key stream）：序列密码中用于加/解密的伪随机序列。

密钥序列生成器（Key stream generator）：序列密码中产生密钥序列的装置或算法。

背包密码（Knapsack cipher）：一种基于背包问题的公开密钥密码算法。

线性密码分析（Linear cryptanalysis）：一种已知明文攻击，利用明文、密文和密钥之间的若干比特的线性关系进行分析。

线性反馈移位寄存器（Linear feedback shift register）：由移位寄存器和线性反馈逻辑组成的一类移位寄存器。

链路加密（Link encryption）：在链路层上对数据进行加密。

逐链加密（Link-by-link encryption）：在通信系统的每段链路上对数据分别进行加密。

消息鉴别码算法（MAC algorithm）：带密钥的密码杂凑算法，可用于数据源鉴别。

中间人攻击（man-in-the-middle attack）：一种主动攻击，攻击者拦截并有选择地修改通信数据，以冒充通信中的实体。

假冒攻击（Masquerade attack）：一种实体非法冒充另一个实体的攻击。

MD5 算法（MD5 algorithm）：一种密码杂凑算法，其输出为 128 比特。

消息鉴别码（Message Authentication Code MAC）：又称消息认证码，是消息鉴别码算法的输出。

多重加密（Multiple encryption）：相同或不同密码算法的级联。

一次一密（One-time pad）：密钥使用一次后就不再使用的加密方法。