密码学·技术机制（下）

——中国密码学会 组编

输出反馈工作模式（Out Feed Back OFB operation mode）：分组密码算法用于构造序列密码的一种工作模式，用该算法当前时刻输出作为下一时刻的输入。

概率密码系统（Probabilistic cryptosystem）：使用了概率加密的密码系统。

概率加密（Probabilistic encryption）：在相同密钥下，每一个明文都有多个可能的密文，且不能检测出一个给定的密文是否是某个特定明文的加密。

伪随机数（Pseudorandom number）：用确定性算法产生的数，其统计特性与随机数类似。

伪随机序列生成器（Pseudorandom sequence generator）：产生伪随机序列的装置或算法。

公钥证书（Public key certificate）：一种数字证书，由认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

公钥基础设施（Public Key Infrastructure PKI）：用公钥密码技术建立的普通适用的基础设施，为用户提供证书管理和密钥管理等安全服务。

注册机构（Registration Authority RA）：同“证书注册中心”。

重放攻击（Replay attack）：一种主动攻击方法，攻击者通过记录通信会话，并在以后某个时刻重放整个会话或者会话的一部分。

RSA 算法（Rivest-Shamir-Adleman algorithm RSA）：一种基于大整数因子分解问题的公钥密码算法。

轮函数（Round function）：在迭代分组密码中重复使用的一种函数。

轮密钥（Round key）：又称子密钥，在迭代分组密码中每一轮使用的密钥，根据输入密钥用密钥编排算法推导得出。

S 盒（S box）：非线性变换的替代表，用以实现混淆或扩散。

SHA-1/2 算法（Secure Hash Algorithm SHA）：美国国家标准和技术研究所发布的安全杂凑算法标准：SHA-1(1995 年)和 SHA-2(2002 年)。

秘密密钥（Secret key）：对称密码系统中实体使用的密钥。

秘密分享（Secret sharing）：将秘密分解成多个子秘密，其个数达到规定数时才能恢复该秘密。

安全多方计算（Secure multi-party computation）：一种安全协议，协议参与者在不泄露各自秘密的前提下，得到由所有参与者的秘密为输入的一个函数的输出。

SSL 协议（Secure Socket Layer protocol）：一种应用于传输层的安全协议，用于构建客户机和服务器之间的安全通道。

对称密码算法（Symmetric cryptographic algorithm）：加/解密使用相同密钥的密码算法。

自同步序列密码（Self-synchronizing stream cipher）：密码失去同步后，可以自动恢复同步的序列密码。

简单能量分析（Simple Power Analysis SPA）：一种密码分析方法，通过对设备或模块的功耗情况进行监测，以揭示密码算法的功能和实现，并由此得到密钥值。

统计密码分析（Statistical cryptanalysis）：一种密码分析方法，根据密文反映出的明文统计规律进行的密码分析。

序列密码（Stream cipher）：将明文逐比特/字符加密的一种对称加密算法。

代替-置换网络（Substitution-Permutation Network SPN）：一种迭代分组密码算法结构，每一轮都含有代替和置换的操作。

3-DES triple （DES）：以 DES 为基础的三重加密算法。