密码学·一般概念（上）

——中国密码学会 组编

自适应选择密文攻击（Adaptive chosen-ciphertext attack）：一种特殊的选择密文攻击，密码攻击者不仅能选择加密后的密文，而且能基于以前的密码分析结果修正其选择。

自适应选择明文攻击（Adaptive chosen-plaintext attack）：一种特殊的选择明文攻击，密码攻击者不仅能选择待加密的明文，而且能基于以前的密码分析结果修正其选择。

雪崩效应（Avalanche effect）：密码变换的一种性质，输入中微小的变化可引起输出很大的变化。

布尔函数（Boolean function）：多个二进制比特输入，一个二进制比特输出的函数。

蛮力攻击/穷举攻击（Brute-force attack/Exhaustive attack）：一种密码攻击方法，对所有可能的密钥进行试探以获取实际的密钥。

选择密文攻击（Chosen-ciphertext attack）：密码攻击的一种类型，密码攻击者能选择一些特定的密文，并获得对应的明文。

选择明文攻击（Chosen-plaintext attack）：密码攻击的一种类型，密码攻击者能选择一些特定的明文，并获得对应的密文。

密码强度（Cipher strength）：对密码算法、密码协议等的抗分析攻击能力的度量。

密文（Ciphertext）：加密后的数据。

唯密文攻击（Ciphertext-only attack）：密码攻击的一种类型，密码攻击者只能得到一些密文，而无法得到对应的明文。

密文空间（Ciphertext space）：所有可能的密文组成的集合。

完备性（Completeness）：密码交换的一种性质，每一输出比特都依赖于所有输出比特。

计算复杂度（Computational complexity）：对计算所需资源（包括时间和空间等）的度量。

计算安全（Computational Security）：密码体制安全性的一种评价方式，用目前最有效的方法破译一个密码体制的计算复杂度来度量。如果该计算复杂度超过了和合理的计算资源，则称该密码体制是计算安全。

计算不可行（Computationally infeasible）：执行计算所需的资源（包括时间和空间等）实际上是无法满足的。

保密性（Confidentiality）：又称机密性，保证信息不被泄露给非授权的个人、进程等实体

的性质。

混淆/混乱（Confusion）：一种密码设计准则，使密文、明文和密钥之间的关系复杂化。

相关免疫（Correlation immunity）：密码变换的一种性质，指输出与部分输入的统计独立性。

密码算法（Crypto-algorithm/Cryptographic algorithm）：描述密码处理过程的一组运算规则或规程。

密码分析/密码攻击（Cryptanalysis/Cryptographic attack）：为了得到保密变量或包括明文在内的敏感数据而对密码系统或其输入输出进行的分析。

密码校验函数（Cryptographic check function）：一种密码变换，以秘密密钥和任意字符串作为输入，而输出通常用于数据的完整性校验。

密码校验值（Cryptographic check value）：密码校验函数的输出。

密码杂凑函数（Cryptographic hash function）：又称密码散列函数或者密码哈希函数，将一个任意长的比特串映射到一个固定长的比特串的函数，且满足下列两个特性：

（1）为一个给定的输出找出能映射到该输出的一个输入是计算不可行的；

（2）为一个给定的输入找出能映射到同一个输出的另一个输入是计算不可行的。

密码协议（Cryptographic protocol）：应用密码算法实现特定安全功能的协议。

密码同步（Cryptography synchronization）：使密码系统正确处理而进行的协作机制。