Broadview
www.broadview.com.cn

安全技术大系

# Cryptology Terminology
# 密码术语

中国密码学会 组编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Broadview
www.broadview.com.cn
博文视点·IT出版旗舰品牌
技术凝聚实力·专业创新出版

# 密码术语

密码技术是信息安全的核心技术，密码标准化是信息安全标准化的重要组成部分。本书编入了当前密码标准化领域需要规范的密码基础术语181条，分为一般概念、技术机制和密码设备三类。这些基础术语的选择和定义的表述均遵照有关术语标准编写，力求做到预定受众明确、专业领域清晰、术语概念体系完整、定义表述准确、编写流程规范。

该书包含了密码领域的基础术语和定义，它的出版将有利于密码技术的研究和应用。本书既可作为密码有关标准的参照，也可供从事信息安全、计算机、通信、电子工程等领域工作的科技人员参考。

上架建议：网络安全

网上订购：www.dearbook.com.cn
第二书店·第一服务

策划编辑：毕　宁
责任编辑：葛　娜
责任美编：侯士卿

本书贴有激光防伪标志，
凡没有防伪标志者，属盗版图书。

ISBN 978-7-121-08737-0

定价：10.00元

电子工业出版社

安全技术大系

# Cryptology Terminology
# 密码术语

中国密码学会 组编

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

## 内 容 简 介

密码技术是信息安全的核心技术，密码标准化是信息安全标准化的重要组成部分。本书编入了当前密码标准化领域需要规范的密码基础术语181条，分为一般概念、技术机制和密码设备三类。这些基础术语的选择和定义的表述均遵照有关术语标准编写，力求做到预定受众明确、专业领域清晰、术语概念体系完整、定义表述准确、编写流程规范。

该书包含了密码领域的基础术语和定义，它的出版将有利于密码技术的研究和应用。本书既可作为密码有关标准的参照，也可供从事信息安全、计算机、通信、电子工程等领域工作的科技人员参考。



**图书在版编目（CIP）数据**

密码术语 / 中国密码学会组编. —北京：电子工业出版社，2009.6
（安全技术大系）
ISBN 978-7-121-08737-0

Ⅰ. 密… Ⅱ. 中… Ⅲ. 密码—术语—汇编 Ⅳ. TN918.1-61

中国版本图书馆 CIP 数据核字（2009）第 065961 号

策划编辑：毕 宁
责任编辑：葛 娜
印 刷：北京智力达印刷有限公司
装 订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：850×1168 1/32 印张：2.75 字数：26.4 千字
印 次：2009 年 6 月第 1 次印刷
印 数：5000 册 定价：10.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

# 序

为了适应当前密码领域蓬勃发展的需要，由四川大学信息安全研究所牵头编写了这本“密码术语”，该书包含了密码领域的基础术语和定义，相信它的出版将有利于密码技术的研究和应用。

参与该书编写的有胡勇，任德斌，吴少华，欧晓聪，周安民，刘嘉勇，方勇等人，龚奇敏教授担任责任专家。初稿完成后，我们征求了部分大专院校、科研院所和相关企业密码专家的意见，国家密码管理局组织专家对书稿进行了审定。在此，向所有为此书的出版付出辛勤劳动的同行们表示衷心的感谢！

由于我们编辑出版“密码术语”的工作经验有限，书中内容如有不妥之处，欢迎广大读者指正。

裴定一

（中国密码学会理事长）

2008 年 11 月

# 前　言

密码技术是信息安全的核心技术，密码标准化是信息安全标准化的重要组成部分。密码和密码标准化在国家信息安全保障体系建设中的基础性、关键性和规范性作用日益明显。为适应密码及密码标准化发展的实际需要，在国家密码管理局的支持下，编写了“密码术语”这本小册子。

本书编入了当前密码标准化领域需要规范的密码基础术语181条，分为一般概念、技术机制和密码设备三类。这些基础术语的选择和定义的表述均遵照有关术语标准编写，力求做到预定受众明确、专业领域清晰、术语概念体系完整、定义表述准确、编写流程规范。但囿于密码及标准化方面的知识和经验，书中内容定有不妥之处，欢迎读者批评指正。

本书在编写过程中，得到了密码领域和标准化领域很多专家学者的指导帮助，在此，向他们表示衷心的感谢。同时，向支持本书出版的中国密码学会以及为此付出辛勤劳动的所有同志表示由衷的感谢。

龚奇敏

# 目　录

# 1 范围

本标准给出了密码领域的基础术语及其定义。

本标准适用于密码技术和产品的论证、设计、生产、认证、使用和维护等，也可作为密码有关标准的参照。

# 2 术语

## 2.1 一般概念

### 2.1.1 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。

### 2.1.2 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。

### 2.1.3 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。

### 2.1.4 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。

### 2.1.5 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。

### 2.1.6 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。

### 2.1.7 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。

### 2.1.8 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。

### 2.1.9 密文 ciphertext

加密后的数据。

### 2.1.10 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。

### 2.1.11 密文空间 ciphertext space

所有可能的密文组成的集合。

### 2.1.12 完备性 completeness

密码变换的一种性质，每一输出比特都依赖于所有输入比特。

### 2.1.13 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。

### 2.1.14 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合理的计算资源，则称该密码体制是计算安全的。

### 2.1.15 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。

### 2.1.16 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。

### 2.1.17 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。

### 2.1.18 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。

### 2.1.19 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。

### 2.1.20 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。

### 2.1.21 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。

### 2.1.22 密码校验值 cryptographic check value

密码校验函数的输出。

### 2.1.23 密码杂凑函数 cryptographic hash function

又称密码散列函数或密码哈希函数，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。

### 2.1.24 密码协议 cryptographic protocol

应用密码算法实现特定安全功能的协议。

### 2.1.25 密码同步 cryptography synchronization

使密码系统正确处理而进行的协作机制。

### 2.1.26 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。

### 2.1.27 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）。

### 2.1.28 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。

### 2.1.29 解密 decipherment/decryption

加密过程对应的逆过程。

### 2.1.30 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。

### 2.1.31 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。

### 2.1.32 有限域离散对数问题 discrete logarithm problem over finite field

给定一个有限域 $F_q$ 和 $F_q^*$ 的一个生成元 $g$，对于 $F_q^*$ 的任意一个元素 $h$，求整数 $a<q$，使得 $h=g^a$。

### 2.1.33 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 $Q=mP$。

### 2.1.34 椭圆曲线 elliptic curve

数域上的韦尔斯特拉斯方程：$y^2+a_1xy+a_2y=x^3+a_3x^2+a_4x+a_5$ 所确定的平面曲线。

### 2.1.35 加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

### 2.1.36 有限域 finite field

由有限个元素组成的域。

### 2.1.37 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。