An English-Chinese Dictionary of Cryptography and Cybersecurity

英汉密码学与网络安全词典

◆ 主编　郎永清

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

英汉密码学与网络安全词典

An English-Chinese Dictionary of Cryptography and Cybersecurity

主编　郎永清

主审　封化民

编者　解献芬　张武江　巴雪静　王　玮

刘伟伟　刘　妍　张艳硕

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本词典收录密码学与网络安全领域研究、开发、应用和管理等方面的词语5000多条，涵盖密码学、网络安全、代数与数论等学科，以及相应的基础理论体系、技术体系和应用体系方面的常用基本英语词汇、最新术语、缩略语及其汉译，力求做到术语或相关词条概念体系完整、定义表述准确。所有词条均按字母顺序排列，并进行规范与审定。

本词典适合高等院校密码学专业与网络安全相关专业的师生，网络安全、计算机、通信、电子工程等领域的从业人员，以及翻译工作者使用。

图书在版编目（CIP）数据

英汉密码学与网络安全词典/郎永清主编. —北京：电子工业出版社，2017.8
ISBN 978-7-121-31866-5

Ⅰ. ①英… Ⅱ. ①郎… Ⅲ. ①密码学－词典－英、汉 ②计算机网络－网络安全－词典－英、汉 Ⅳ. ①TN918.1－61 ②TP393.08－61

中国版本图书馆CIP数据核字（2017）第131019号

责任编辑：富 军 特约编辑：刘汉斌
印 刷：涿州市京南印刷厂
装 订：涿州市京南印刷厂
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：880×1 230 1/32 印张：7.5 字数：295千字
版 次：2017年8月第1版
印 次：2017年8月第1次印刷
定 价：68.00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)88254888，88258888。

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。

本书咨询联系方式：fujun@phei.com.cn。

前　言

当今世界，随着互联网技术的不断更新，网络信息安全日益成为全球关注的一个重要议题，也是摆在世界各国面前的紧迫任务。信息安全是国家安全的重要组成部分。密码理论和加密技术是网络安全技术的核心。可以说，没有密码技术就没有网络安全。随着密码学与网络安全学科的迅速发展，有关的新技术、新名词和缩略语等层出不穷，给学习者和研究者带来极大的不便。

本词典收录当前密码学与网络安全领域常用词语5000多条，涵盖密码学、网络安全、代数与数论等学科，以及相应的基础理论体系、技术体系和应用体系方面的常用基本英语词汇、最新术语、缩略语及其汉译，突出现代性、实用性和简明性，力求选词实用精练，体现时代特征，例证典型地道，释义简明准确，编排科学合理。

我们在编纂过程中尝试使用语料库辅助词典编纂技术，建成一个密码学英汉摘要平行语料库（Cryptography English-Chinese Parallel Abstract Corpus，CECPAC）。该库的建设目的就是构建一座语言桥梁，旨在通过定量和定性相结合的优势探讨英汉密码学专业词汇及相关术语的词频和翻译特征。英汉平行语料库为词条的翻译提供了良好的数据支撑，极大地提高了本词典编纂的效率。

《英汉密码及网络安全词典》是一本“专科”双语词典。英语术语翻译也不是“直译”，而是尽可能地从汉语的相同学科找出等价的术语。在词汇筛选及翻译过程中，我们采取密码学教师与外语教师合作编写的方式，保证词典的编纂质量。

本词典适合高等院校密码学专业与网络安全相关专业的师生，网络安全、计算机、通信、电子工程等领域的从业人员及翻译工作者使用。

本词典在编纂过程中得到北京电子科技学院领导、科研处、信息

安全系、人文社科部、图书馆的大力支持。教育部高等学校信息安全专业教学指导委员会秘书长封化民教授在百忙之中审定了全部书稿并提出了宝贵的修改意见。李晓明、李梦东、韩妍妍等同志参加了本词典的策划、选材、编译、审校及修改工作。在此一并表示衷心的感谢！

由于编者水平和学识有限，书中难免有不当之处，敬请读者批评指正。

编　者

2017 年 4 月

目　　录

A

A5	一种对称密码算法
AAA	Authentication，Authorization，Accounting 验证、授权和记账
AAC	Advanced Audio Coding 高级音频编码
ABA Digital Signature Guidelines	美国律师协会（American Bar Association）1996 年制定的数字签名指南
Abel	阿贝尔（挪威数学家）
Abelian	阿贝尔的，可交换的
Abelian Varieties	阿贝尔簇
Abreast Davies-Meyer	并列 DM 算法
Absence of Communication Attack	不存在通信攻击
Absolute Indicator	绝对指示器
Abundanceof Communication Attack	大量通信攻击
Abundant Number	过剩数
Abuse-Free Protocol	无滥用协议
Abwehr	（德国第二次世界大战期间）反间谍机关
AC0 Leakage	AC0 泄漏
Access	（使用权）访问
Access Authority	访问授权
Access Control	访问控制
Access Control List	访问控制表
Access Control Mechanism	访问控制机制
Access Control Model	访问控制模型

Access Control Policy	访问控制策略
Access Level	访问级别
Access List	访问列表
Access Management	访问管理
Access Matrix Model	访问矩阵模型
Access Point	访问点，接入点
Access Profile	访问配置文件
Access Right	访问权限
Access Structure	访问结构
Access Type	访问类型
Account	账户
Account Management	账户管理
Accountability	可说明性，责任性，问责制
Accounting Legend Code	记账识别码，计算代码，会计图例编码
Accounting Number	账号
Account Owner	账户拥有者
Accreditation	验证，认可
Accreditation Authority	认证机构
Accreditation Boundary	认证边界
Accreditation Package	认证包
Accrediting Authority	认证机构
Accumulator	累加器
ACE-KEM	NESSIE 选择的非对称密码机制
Acquirer	收单方，收购方
Acrostics	藏头诗，离合文，数行文字
ACS	Access Control Services 访问控制服务
Acting on a Set	作用于一个集合
Action of Group on a Set	一个集合上群的作用
Activation Data	激活数据

Active Adversary	活跃敌手
Active Attack	主动攻击
Active Content	动态内容，活动内容
Active Cryptanalysis	主动密码分析
Active Eavesdropper	主动窃听者
Active Penetration Test	主动渗透测试
Active Security	主动安全
Active Security Testing	动态安全测试
ActiveX	ActiveX 控件
Ad Hoc Network	自组网，自适应网络
Adaptive Adversary	适应性攻击
Adaptive Auxiliary Information (AAIMPC)	自适应辅助信息
Adaptive Chosen Ciphertext Attack	自适应选择密文攻击
Adaptive Chosen Plaintext Attack	自适应选择明文攻击
Adaptively Secure	自适应安全
Adaptively Secure Garbling	自适应安全置乱
Addition Rule	加法规则
Addition Chain	加法链
Addition Problem	加法问题
Addition Sequence	加入顺序
Additional Assumption	额外假设
Addition-Subtraction Chain	加减法链
Additive Group	加法群
Additive Inverse	加法逆元
Additive Knapsack	加法背包
Additive Noise	加性噪声

Additional Decryption Key	附加的解密密钥
Add-on Security	（计算机之外的）附加保护措施
Address Spoofing	地址欺骗
Adequate Security	足够的安全（保障）性
A-Distance	A 距离
Adjoint	共轭，伴随矩阵
Adjoint Matrix	伴随矩阵
Adleman-Pomerance-Rumely Primality	Adleman、Pomerance 和 Rumely 的素性测试
Administrator	管理员
Administrative Account	管理（员）账户
Administrative Safeguard	管理保障
Admissible Change of Variables	变量的容许变化
Advanced Encryption Standard	高级加密标准
Advanced Key Processor (AKP)	高级密钥处理程序
Advanced Persistent Threats (APT)	高级持续性威胁
Advantage	优势
Adversarial Challenge	敌手的挑战
Adversarially-Chosen Plaintext Distribution	敌手选择明文分布
Adversary	敌手
Adversary Structure	攻击结构
Adversary Simulator	咨询模拟器
AE	Authenticated Encryption 认证加密
AEAD	Authenticated Encryptionwith Associated Data 带关联数据的认证加密

AES	Advanced Encryption Standard 高级加密标准
Affine Equivalent	仿射等价
Affine Function	仿射函数
Affine Invariant	仿射不变量
Affine Scheme	仿射概形
AG-Code	Algebraic Geometry Code 代数几何码
Agency	代理
Agency of Certification Authority	数字证书授权机构
Agent	代理人
Aggressive Mode	积极（进攻）模式
AGM Method	基于代数几何的算法
AH	Authentication Header 身份验证报头
AKP	Advanced Key Processor 高级密钥处理程序
Alberti Encryption	Alberti 加密
Alberti Table	Alberti 表格
Alert	报警，警告
Alert Message	警报信息
Algebraic Attack	代数攻击
Algebraic Degree	代数次数
Algebraic Element	代数元
Algebraic Immunity	代数免疫性
Algebraic Independence	代数独立性
Algebraic Integer	代数整数
Algebraic Normal Form	代数范式，代数标准型
Algebraic Number	代数数
Algebraic Number Field	代数数域

Algebraic Reduction	代数归约
Algebraically Closed	代数封闭的
Algebraically Independent Element	代数无关的元素
Algebraic-Geometry Code	代数几何码
Algebra	代数
Algorithm	算法
Aliquot Cycle	循环圈，真因子圈
All-But-One Decryption	可重复性解密
All-But-One Simulation Technique	可重复性仿真技术
All Hazards Approach	全致灾因子方法
Allocation	配置
All-or-Nothing Encryption	全有全无加密术
Almost Bent Function	几乎 Bent 函数
Almost Perfect Nonlinear Function	几乎完全非线性函数
Almost Perfect Zero-Knowledge	几乎完全零知识
Alternate	交替，轮流
Alternate COMSEC Custodian	替补通信安全管理人员，备用 COMSEC 保管人
Alternate Site	备用站点，备用处理设施
Alternate Work Site	临时工作地点，交替工作站点
Alternating Group	交替群
Alternating Step Generator	一般步进生成器
American Bar Association	美国律师协会
American National Institute of Standards and Technology (NIST)	美国国家标准与技术研究所

Amicable Pair	亲和数对
Amitsur Levitzki Theorem	Amitsur Levitzki 定理
Application Recovery	应用程序恢复
Amortized Communication Complexity	消减通信复杂度
Amortized Cost	摊销成本
Amplified Boomerang Attack	放大 Boomerang 攻击
An Apriori Bounded Polynomial Number	一个先验界多项式数目
An Interval in a Modular Lattice	模格的一个间隔
Analogue	类似物
Analogue for Algebra	模拟代数
Analogue for Ring	模拟环
Analysis	分析
Analytic Number Theory	解析数论
AND Function	AND 函数
Anisotropic	各向异性
Anisotropic Kernel	各向异性核
Annihilator	零化子
Anomalous Binary Curve	异常二进制曲线
Anomaly	异常
Anomaly-Based Detection	异常检测
Anonym	匿名者
Anonymity	匿名
Anonymity Set	匿名集
Anonymous Broadcast	匿名广播
Anonymous Network	匿名网络
Anonymous Remailer	匿名（重游程序）转发器

Anonymous Signature	匿名签名
ANSI	American National Standards Institute 美国国家标准学会，ANSI 编码
Antihomomorphism	反同态，反同构
Anti-Jam	抗干扰
Anti-Linear	抗线性
Anti-Spoof	反欺骗
Antispyware Software	反间谍软件
Antivirus Software	防病毒软件
APN Function	APN 函数
APPEL	P3P 偏好交换语言
Applicant	申请人
Application	应用程序
Application Cryptogram	应用密文
Approval to Operate (ATO)	批准运行
Approved Modeof Operation	认可的操作模式
Approved Security Function	核准的安全功能
Approximate Common Divisor	近似公因子
Approximate Eigenvector	近似特征向量
Approximation	近似（算法）
APT	Advanced Persistent Threats 高级持续性威胁
Arbitrary Auxiliary Information	任意辅助信息
Arbitrary Communication Resource	任意通信资源
Arbitrary Cyclotomic	任意单位根
Arbitrary Key	任意密钥
Arbitrary Partial Information	任意部分信息

Arbitrary Permutation	任意置换
Archimedes	阿基米德
Archive	存档，档案文件
Arithmetic	算术
Arithmetic Fundamental Theorem	算术基本定理
Arity	参数数量
ARQC	Authorization Request Cryptogram 授权请求密文
Artin Chevalley Theorem	阿廷·谢瓦莱定理
Artin's Conjecture	阿廷猜想
ARX	Addition, Rotation and XOR 加、循环移位和异或结构
AS	AS 运算符
Ascending Chain	上升链条，上升链
Assessment	评价，评估
Assessment Finding	评估结果
Assessment Method	评估方法
Assessment Object	评估对象
Assessment Objective	评估目标
Assessment Procedure	评估程序
Assessor	鉴定器，评定器，评审员
Asset	资产
Asset Criticality	资产临界点
Asset Identification	资产鉴定
Asset Reporting Format (ARF)	资产报告格式
Associated Data	关联数据
Associative	联想的，组合的，联合的
Associative Law	结合律

Associativity	关联性
Associator	相伴，伙伴
Assumption	假设，设想
Assurance	确保，确信度，保障
Assurance Case	安全保证案例，保障案例
Assured Information Sharing	确保信息共享
Assured Software	有保证的软件
Asymmetric	非对称
Asymmetric Cryptography	非对称加密学
Asymmetric Cryptosystem	非对称密码系统
Asymmetric Functionality	非对称功能
Asymmetric Key	非对称密钥
Asymmetric Proxy Encryption	非对称代理加密
Asymmetric Proxy Signature Scheme	非对称代理签名方案
Asymmetric Watermarking	非对称水印
Asymptotic Complexity	渐近复杂度
Asymptotic Security	渐近安全性
Asymptotically	渐近性
Asymptotically Optimal	渐近最优
Asymptotically Square Root	渐近平方根
Asymptotically Tight Security Analysis	渐近紧致安全分析
Asynchronous Self-Synchronizing	异步式自同步
ATM	Asynchronous Transfer Mode 异步传输模式
ATO	Approval to Operate 批准运行
Attack	攻击
Attack Sensing and Warning (AS&W)	攻击监测和警告

Attack Signature	攻击签名
Attribute	属性
Attribute Authority	属性授权，属性权威
Attribute Certificate	属性证书
Attribute Management	属性管理
Attribute-Based Access Control	基于属性的访问控制
Attribute-Based Authorization	基于属性的授权
Attribute-Based Encryption	基于属性的加密
Attribute-Based Encryption Scheme	基于属性的加密方案
Auctioneer Role	拍卖者角色
Audit	审计，审核
Audit Data	审计数据
Audit Log	审计日志
Audit Protocol	审计协议
Audit Reduction Tool	审计工具还原，审计精选工具
Audit Review	审计复核
Audit Trail	审计跟踪
Authenticate	认证
Authenticated Data	认证数据
Authenticated Encryption	认证加密
Authenticated Encryption with Associated Data	带相关数据的认证加密
Authenticated Key Exchange	认证密钥交换
Authentication	认证
Authentication Authority	认证授权
Authentication Information	认证信息
Authentication Code	认证码