中文维基百科第十八次动员令正在进行中，欢迎各位维基人踊跃参与！ [关闭]

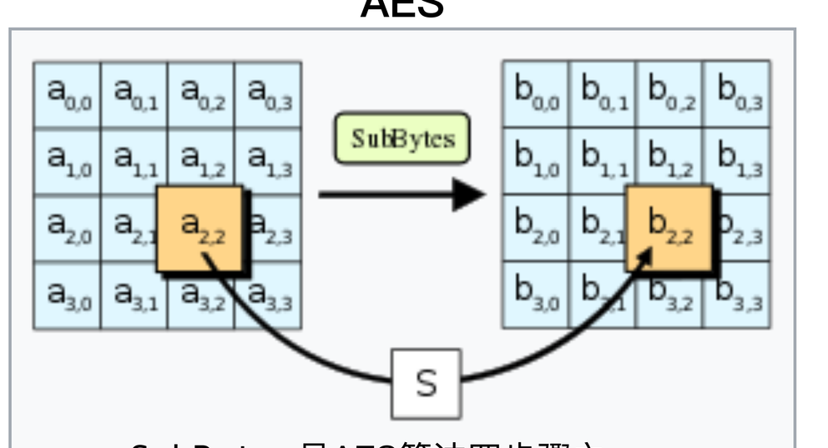
高级加密标准 [编辑]

维基百科，自由的百科全书

高级加密标准（英语：**A**dvanced **E**ncryption **S**tandard，缩写：AES），在密码学中又称**Rijndael加密法**，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院（NIST）于2001年11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效的标准。现在，高级加密标准已然成为对称密钥加密中最流行的算法之一。

该算法为比利时密码学家Joan Daemen和Vincent Rijmen所设计，结合两位作者的名字，以Rijndael为名投稿高级加密标准的甄选流程。（Rijndael的发音近于"Rhine doll"）

AES



SubBytes是AES算法四步骤之一。

概述	
设计者	Vincent Rijmen、Joan Daemen
首次发布	1998年
派生自	Square
继承算法	Anubis、Grand Cru、Kalyna
密码细节	
密钥长度	128、192或者256比特[a]
分组长度	128位[b]
结构	置换排列网络
重复回数	10, 12或14（视密钥长度而定）
最佳公开破解	
关系密码攻击可以破解9个加密循环/256比特（密钥）的AES。另外选择性明文攻击可以破解8个加密循环，192或256比特（密钥）的AES，或7个加密循环、128位（密钥）的AES。（Ferguson *et al.*, 2000）	

目录 [隐藏]

沿革 [编辑]

Rijndael是由Daemen和Rijmen早期所设计的Square改良而来；而Square则是由SHARK发展而来。

不同于它的前任标准DES，Rijndael使用的是代换–置换网络，而非Feistel架构。

密码说明 [编辑]

严格地说，AES和Rijndael加密法并不完全一样（虽然在实际应用中两者可以互换），因为Rijndael加密法可以支持更大范围的区块和密钥长度：AES的区块长度固定为128比特，密钥长度则可以是128，192或256比特；而Rijndael使用的密钥和区块长度均可以是128，192或256比特。加密过程中使用的密钥是由Rijndael密钥生成方案产生。

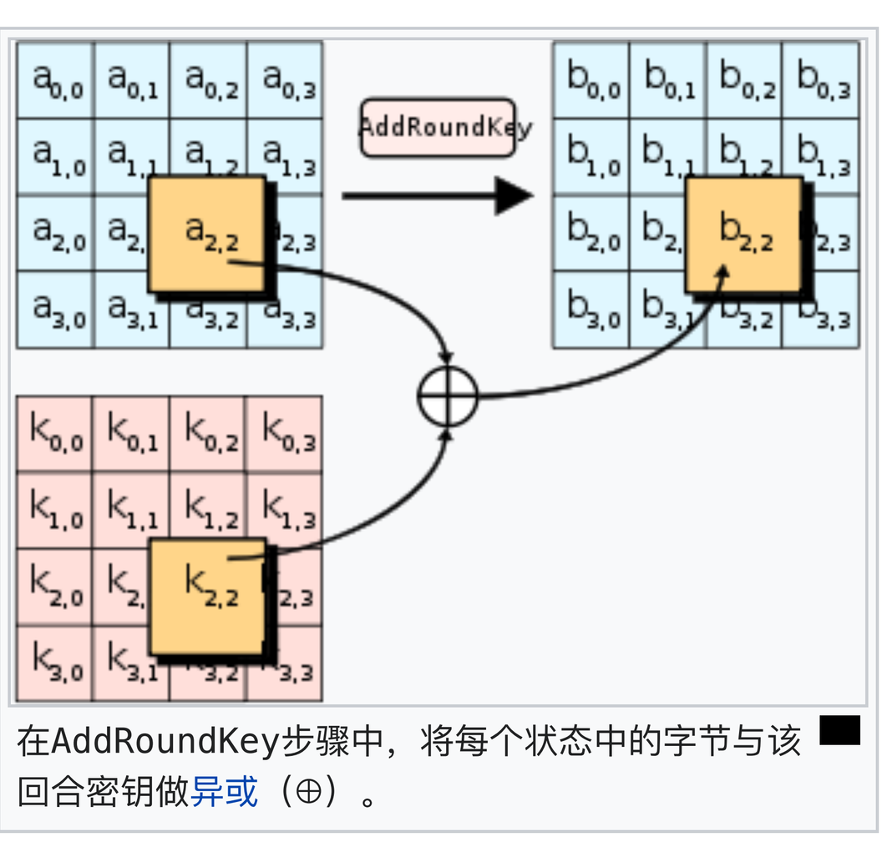
大多数AES计算是在一个特别的有限域完成的。

AES加密过程是在一个4×4的字节矩阵上运作，这个矩阵又称为"体（state）"，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个Byte）。（Rijndael加密法因支持更大的区块，其矩阵的"列数（Row number）"可视情况增加）加密时，各轮AES加密循环（除最后一轮外）均包含4个步骤：

1. AddRoundKey—矩阵中的每一个字节都与该次回合密钥（round key）做XOR运算；每个子密钥由密钥生成方案产生。
2. SubBytes—透过一个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。
3. ShiftRows—将矩阵中的每个横列进行循环式移位。
4. MixColumns—为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每内联的四个字节。最后一个加密循环中省略MixColumns步骤，而以另一个AddRoundKey取代。

AddRoundKey步骤 [编辑]

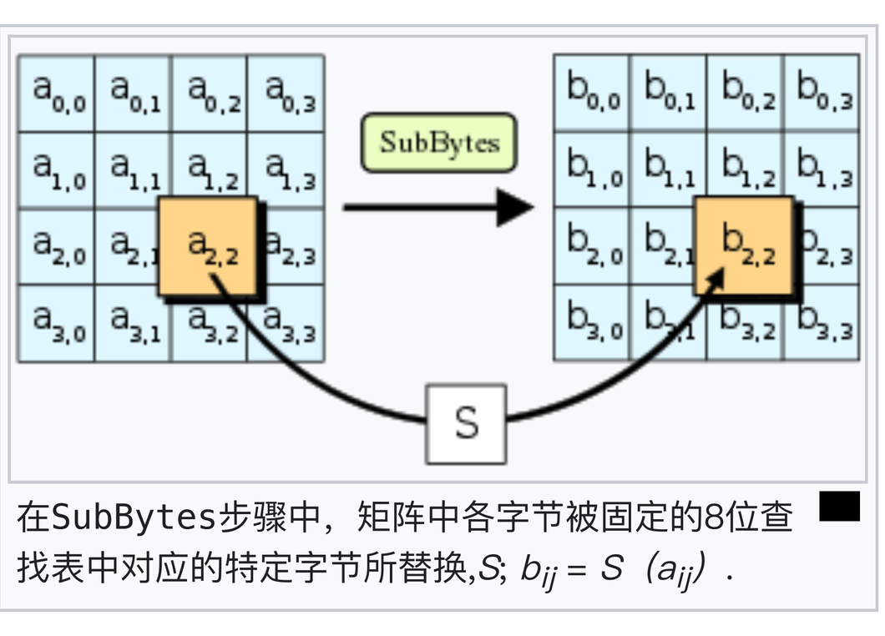
AddRoundKey步骤，回合密钥将会与原矩阵合并。在每次的加密循环中，都会由主密钥产生一把回合密钥（透过Rijndael密钥生成方案产生），这把密钥大小会跟原矩阵一样，以与原矩阵中每个对应的字节作异或（⊕）加法。



在AddRoundKey步骤中，将每个状态中的字节与该回合密钥做异或（⊕）。

SubBytes步骤 [编辑]

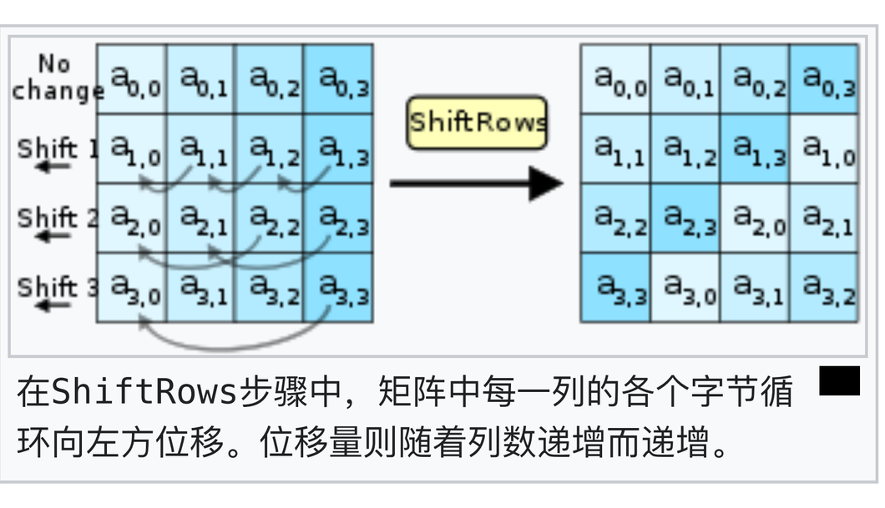
在SubBytes步骤中，矩阵中的各字节透过一个8位的S-box进行转换。这个步骤提供了加密法非线性的变换能力。S-box与$GF(2^8)$上的乘法反元素有关，已知具有良好的非线性特性。为了避免简单代数性质的攻击，S-box结合了乘法反元素及一个可逆的仿射变换矩阵建构而成。此外在建构S-box时，刻意避开了固定点与反固定点，即以S-box替换字节的结果会相当于错排的结果。此条目有针对S-box的详细描述：Rijndael S-box



在SubBytes步骤中，矩阵中各字节被固定的8位查找表中对应的特定字节所替换，S; $b_{ij} = S(a_{ij})$.

ShiftRows步骤 [编辑]

ShiftRows描述矩阵的列操作。在此步骤中，每一列都向左循环位移某个偏移量。在AES中（区块大小128位），第一列维持不变，第二列里的每个字节都向左循环移动一格。同理，第三列及第四列向左循环位移的偏移量就分别是2和3。128位和192比特的区块在此步骤的循环位移的模式相同。经过ShiftRows之后，矩阵中每一竖行，都是由输入矩阵中的每个不同行中的元素组成。Rijndael算法的版本中，偏移量和AES有少许不同；对于长度256比特的区块，第一列仍然维持不变，第二列、第三列、第四列的偏移量分别是1字节、2字节、3字节。除此之外，ShiftRows操作步骤在Rijndael和AES中完全相同。

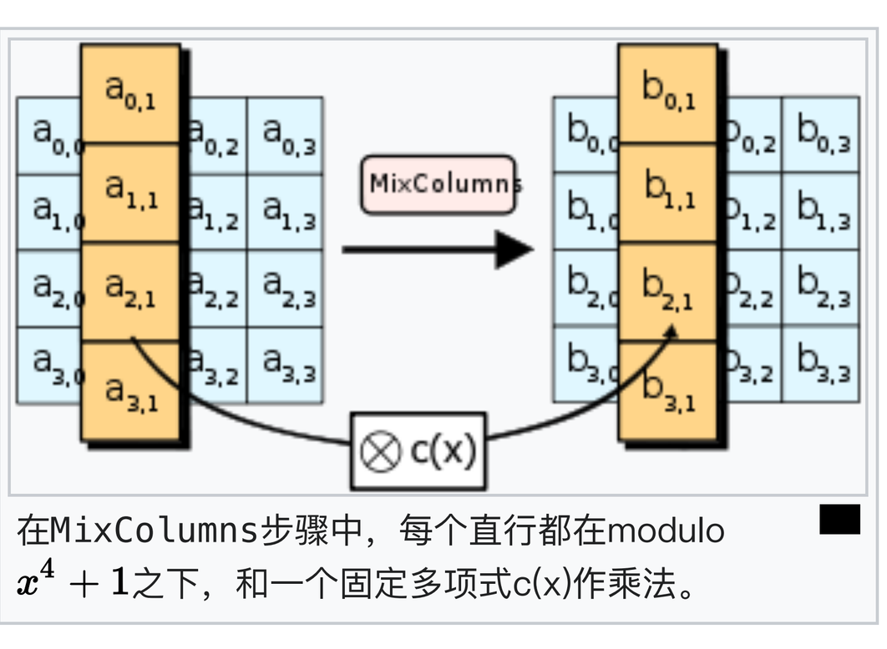


在ShiftRows步骤中，矩阵中每一列的各个字节循环向左方位移。位移量则随着列数递增而递增。

MixColumns步骤 [编辑]

在MixColumns步骤，每一行的四个字节透过线性变换互相结合。每一行的四个元素分别当作$1, x, x^2, x^3$的系数，合并即为$GF(2^8)$中的一个多项式，接着将此多项式和一个固定的多项式$c(x) = 3x^3 + x^2 + x + 2$在模$x^4 + 1$下相乘。此步骤亦可视为Rijndael有限域之下的矩阵乘法。MixColumns函数接受4个字节的输入，输出4个字节，每一个输入的字节都会对输出的四个字节造成影响。因此ShiftRows和MixColumns两步骤为这个密码系统提供了扩散性。

以下条目有对MixColumns更加详细的描述：Rijndael mix columns



在MixColumns步骤中，每个直行都在modulo $x^4 + 1$之下，和一个固定多项式c(x)作乘法。

加密算法优化 [编辑]

使用32或更多比特定址的系统，可以事先对所有可能的输入创建对应表，利用查表来实现SubBytes，ShiftRows和MixColumns步骤以达到加速的效果。这么作需要产生4个表，每个表都有256个格子，一个格子记载32位的输出；约占去4KB（4096字节）存储器空间，即每个表占去1KB的存储器空间。如此一来，在每个加密循环中，只需要查16次表，作12次32位的XOR运算，以及AddRoundKey步骤中4次32位XOR运算。若使用的平台存储器空间不足4KB，也可以利用循环交换的方式一次查一个256格32位的表。

然而，实际实现中应避免使用这样的对应表，否则可能因为产生缓存命中与否的差别而使旁道攻击成为可能。

安全性 [编辑]

截至2006年，针对AES唯一的成功攻击是旁道攻击或社会工程学攻击。美国国家安全局审核了所有的参与竞选AES的最终入围者（包括Rijndael），认为他们均能够满足美国政府传递非机密文件的安全需要。2003年6月，美国政府宣布AES可以用于加密机密文件：

> The design and strength of all key lengths of the AES algorithm（i.e., 128, 192 and 256）are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.[1]

（译：AES加密算法（使用128，192，和256比特密钥的版本）的安全性，在设计结构及密钥的长度上俱已到达保护机密信息的标准。最高机密信息的传递，则至少需要192或256比特的密钥长度。用以传递国家安全信息的AES实现产品，必须先由国家安全局审核认证，方能被发放使用。）

这标志着，由美国国家安全局NSA批准在最高机密信息上使用的加密系统首次可以被公开使用。许多大众化产品只使用128位密钥当作默认值；由于最高机密文件的加密系统必须保证数十年以上的安全性，故推测NSA可能认为128位太短，才以更长的密钥长度为最高机密的加密保留了安全空间。

通常破解一个区块加密系统最常见的方式，是先对其较弱版本（加密循环次数较少）尝试各种攻击。AES中128位密钥版本有10个加密循环，192比特密钥版本有12个加密循环，256比特密钥版本则有14个加密循环。至2006年为止，最著名的攻击是针对AES 7次加密循环的128位密钥版本，8次加密循环的192比特密钥版本，和9次加密循环的256比特密钥版本所作的攻击。[2]

由于已遭破解的弱版的AES，其加密循环数和原本的加密循环数相差无几，有些密码学家开始担心AES的安全性：要是有人能将该著名的攻击加以改进，这个区块加密系统就会被破解。在密码学的意义上，只要存在一个方法，比穷举法还要更有效率，就能被视为一种"破解"。故一个针对AES 128位密钥的攻击若"只"需要2^{120}计算复杂度（少于穷举法 2^{128}），128位密钥的AES就算被破解了；即便该方法在目前还不实用。从应用的角度来看，这种程度的破解依然太不切实际。最著名的暴力攻击法是distributed.net针对64位密钥RC5所作的攻击。

其他的争议则着重于AES的数学结构。不像其他区块加密系统，AES具有相当井然有序的代数结构。[3]虽然相关的代数攻击尚未出现，但有许多学者认为，把安全性创建于未经透彻研究过的结构上是有风险的。Ferguson，Schroeppel和Whiting因此写道："...我们很担心Rijndael [AES]算法应用在机密系统上的安全性。"[4]

2002年，Nicolas Courtois和Josef Pieprzyk发表名为XSL攻击的理论性攻击，试图展示AES一个潜在的弱点。但该攻击的数学分析有点问题，推测应是作者的计算有误。因此，这种攻击法是否对AES奏效，仍是未解之谜。就现阶段而言，XSL攻击AES的效果不十分显著，故将之应用于实际情况的可能性并不高。

旁道攻击 [编辑]

旁道攻击，又称旁路攻击、侧信道攻击，是一种基于从密码系统的物理实现中获取的信息的攻击方式。它不攻击加密算法本身，而是攻击那些基于不安全系统（会在不经意间泄漏信息）上的加密系统。

2005年4月，D.J. Bernstein公布了一种缓存时序攻击法，他以此破解了一个装载OpenSSL AES加密系统的客户服务器[5]。为了设计使该服务器公布所有的时序信息，攻击算法使用了2亿多条筛选过的明码。对于需要多个跳跃的国际互联网而言，这样的攻击方法并不实用[6]。Bruce Schneier称此攻击为"好的时序攻击法"[7]。

2005年10月，Eran Tromer和另外两个研究员发表了一篇论文，展示了数种针对AES的缓存时序攻击法[8]。

注释 [编辑]

a. ^ 密码长度128, 160, 192, 224,与256比特为Rijndael算法所支持，然而只有128, 192,与256比特长度密码为AES标准所明定。
b. ^ 区块长度128, 160, 192, 224,与256比特为Rijndael算法所支持，不过只有128位区块长度为AES标准所明定。

参考文献 [编辑]

引用 [编辑]

1. ^ 存档副本 (PDF). [2006-12-25]. （原始内容 (PDF)存档于2007-09-27）.
2. ^ Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, *Improved Cryptanalysis of Rijndael*, Fast Software Encryption, 2000 pp213—230 [1]
3. ^ [2]
4. ^ Niels Ferguson, Richard Schroeppel, Doug Whiting. A simple algebraic representation of Rijndael. Proceedings of Selected Areas in Cryptography, 2001, Lecture Notes in Computer Science. Springer Verlag: pp. 103—111. 2001 [2006-10-06]. （原始内容 (PDF/PostScript)存档于2006-11-04）.
5. ^ Daniel J. Bernstei. Cache-timing attacks on AES (PDF). Citeseer. 2005年4月.
6. ^ Lou Scheffer. Successful remote AES key extraction. 2005-04-17 [2011-05-16].
7. ^ Bruce Schneier. AES Timing Attack. 2005-05-17 [2011-05-16].
8. ^ Eran Tromer , Dag Arne Osvik and Adi Shamir. Efficient Cache Attacks on AES, and Countermeasures (PDF). Journal of cryptology. 2010, **23** (1): 37—71.

书目 [编辑]

- Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267—287, ASIACRYPT 2002.
- Joan Daemen, Steve Borg and Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer-Verlag, 2002. ISBN 3-540-42580-2.

外部链接 [编辑]

- The Rijndael Page（Forwards automatically to the AES Lounge; use old version link to browse）
- The Rijndael Page (old version)
- Literature survey on AES
- Recordings of the pronunciation of "Rijndael"（85 KB wav file）
- The archive of the old official AES website
- FIPS PUB 197: the official AES standard（PDF file）
- John Savard's description of the AES algorithm

实现 [编辑]

- 参考代码
- 65+种AES硬件实施方案
- A Javascript AES calculator showing intermediate values
- Brian Gladman's BSD licensed implementations of AES
- [永久失效链接] Paulo Barreto公布的AES的C语言算法[永久失效链接]
- D.J. Bernstein所写的开放著作权AES实施代码
- The GPL-licensed Nettle library also includes an AES implementation
- Compact AES implementation in hardware by IP Cores
- AES加密在Windows系统的实现（自由公开源码）
- LGPL授权的AES实现的C语言源代码
- 广泛的AES硬件实施方案，Helion Technology
- FPGA Based AES Implementation using Nios-II Processor

参见 [编辑]

- 高级加密系统甄选流程

查·论·编	分组密码 [隐藏]
常见加密算法	AES · Blowfish · DES（内部细节 · 3DES） · Serpent · Twofish
次常见加密算法	Camellia · CAST-128 · IDEA · RC2 · RC5 · SEED · Skipjack · TEA · XTEA
其他加密算法	3-Way · ABC · Akelarre · Anubis · ARIA · BaseKing · BassOmatic · BATON · BEAR and LION · CAST-256 · CIKS-1 · CIPHERUNICORN-A · CIPHERUNICORN-E · CLEFIA · CMEA · Cobra · COCONUT98 · Crab · Cryptomeria/C2 · CRYPTON · CS-Cipher · DEAL · DES-X · DFC · E2 · FEAL · FEA-M · FROG · G-DES · GOST · Grand Cru · Hasty Pudding cipher · Hierocrypt · ICE · IDEA NXT · Intel Cascade Cipher · Iraqi · KASUMI · KeeLoq · KHAZAD · Khufu and Khafre · KN-Cipher · Ladder-DES · Libelle · LOKI97 · LOKI89/91 · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · Q · RC6 · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · SM4 · Speck · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · Xenon · xmx · XXTEA · Zodiac
密码设计	Feistel网络 · 密钥调度 · 乘积密码 · S盒 · P盒 · 代换-置换网络 · 混淆与扩散 · 雪崩效应 · 密钥白化 · 密钥长度 · 块大小
攻击（密码分析）	穷举攻击/蛮力攻击（EFF DES破解机） · 中途相遇攻击（Biclique攻击 · 三子集中途相遇攻击） · 线性密码分析（堆积引理） · 差分密码分析（不可能差分密码分析） · 截断差分分析 · 高阶差分分析 · 差分-线性攻击 · 区分攻击（已知密钥区分攻击） · 积分密码分析 · 回力镖攻击 · 模*n*密码分析 · 相关密钥攻击 · 滑动攻击 · 回旋密码分析 · 时序攻击 · XSL攻击 · 插值攻击 · Partitioning · 戴维斯攻击 · 回弹攻击 · 弱密钥 · 肯德尔等级相关系数 · 卡方检验 · 时间、内存、数据取舍攻击
密码标准	高级加密标准（AES）评选过程 · CRYPTREC · NESSIE
工作方式	初始向量 · 工作模式 · 填充

分类：分组密码 | 高级加密标准

本页面最后修订于2020年7月11日 (星期六) 11:24。

本站的全部文字在知识共享 署名-相同方式共享 3.0协议之条款下提供，附加条款亦可能应用。（请参阅使用条款）
Wikipedia®和维基百科标志是维基媒体基金会的注册商标；维基™是维基媒体基金会的商标。
维基媒体基金会是按美国国内税收法501(c)(3)登记的非营利慈善机构。

隐私政策 关于维基百科 免责声明 手机版视图 开发者 统计 Cookie声明