doi :10.3969/j.issn.1671-1122.2011.05.012

AES 加密算法分析及其在信息安全中的应用

张金辉[1]，郭晓彪[2]，符鑫[2]

（1. 解放军总医院，北京 100853 ；2. 后勤指挥学院，北京 100858）

摘 要 ：随着现代密码分析水平、芯片处理能力的不断提高，高级加密标准 AES 算法将在各行业广泛应用。该文章介绍了 AES 加密算法的发展以及实现过程，并探讨其在信息安全方面的应用。

关键词 ：AES ；加密算法 ；信息安全

中图分类号 ：TP393.08 文献标识码 ：A 文章编号 ：1671-1122（2011）05-0031-03

AES Encryption Algorithm Analysis and the Application in Information Security

ZHANG Jin-hui[1], GUO Xiao-biao[2], FU Xin[2]

(1.*General Hospital of PLA, Beijing* 100853*, China;* 2.*Logistics Command Academy, Beijing* 100858*, China*)

Abstract: With modern password analysis level, chip processing power unceasing enhancement, the advanced encryption standard AES algorithm can be widely used in various fields. This paper introduces the development of AES encryption algorithm and realization process, and discusses its application in information security.

Key words: AES; encryption algorithms; information security

0 引言

20 世纪末，当差分密码分析及线性密码分析出现以后，由美国人开创的 DES（Data Encryption Standard，即数据加密标准）逐渐由繁荣走向衰落。1997 年 1 月 2 日，美国国家和标准技术研究所（NIST）发布高级加密标准 (AES-FIPS) 研发计划，9 月 12 日发布征集候选算法公告，NIST 计划确定一种可以保护敏感信息的公开、全球通用并且免费的算法作为 AES（Advanced Encryption Standard，即高级加密标准），用以取代 DES。对该标准的基本要求是 ：支持 128 比特分组长度和 128、192、256 比特密钥长度，并且算法必须是私钥体制的分组密码。经过 3 年多时间的反复较量，对首轮入选的 15 种不同算法进行了广泛的评估和测试，筛选出 5 种算法进入决赛。由比利时的密码专家 Joan Daemen 及 Vincent Rijmen 所提出的 Rijndeal 加密算法，最终胜出。2000 年 10 月 2 日，Rijndael 算法被 NIST 确定为新一代高级加密标准。

1 AES 算法介绍

1.1 概述

密码算法的理论与实现研究是信息安全研究的基础。对各类电子信息进行加密，在其存储、处理、传送以及交换过程中实施保护，是保证信息安全的有效措施。数据加密标准 DES 于 1977 年 1 月向社会公布，它是第一个世界公认的实用分组密码算法标准。但在经过 20 年的应用后，DES 已被认为不可靠。3DES 作为 DES 的替代，密钥长度为 168bits，可克服穷举攻击问题。同时，3DES 的底层加密算法对密码分析攻击有很强的免疫力。但由于用软件实现该算法的速度慢，使得 3DES 不能成为长期使用的加密算法标准，需要一种新的高级加密标准来替代。

AES 具有密钥灵活性及较高的可实现性，具有较高的安全性能及实现效率，其密钥建立时间极短，且灵敏性良好。Rijndeal 算法给出了最佳查分特征概率，进行了算法抵抗差分密码分析以及线性密码分析。无论 Rijndeal 使用反馈模式或无反馈模式，其硬件和软件实现性能都表现优秀。此外，Rijndeal 对内存的极低需求使其适合于在存储器受限环境下使用，并能够表现出极好的性能。

收稿时间 ：2011-04-15

作者简介 ：张金辉（1973-），男，河南，高级工程师，硕士，主要研究方向 ：通信网络技术 ；郭晓彪（1982-），男，内蒙古，助理工程师，硕士，主要研究方向 ：后勤信息化 ；符鑫（1984-），男，河北，助理工程师，硕士，主要研究方向 ：后勤信息化。

1.2 AES算法结构介绍

AES 使用 128、192 和 256 位密钥，用 128bits 分组加密和解密数据。对称密钥密码使用相同的密钥加密和解密数据，通过分组密码返回的加密数据位数与输入数据相同。使用循环结构迭代加密，在该循环中重复置换（Permutations）和替换（Substitutions）输入数据。

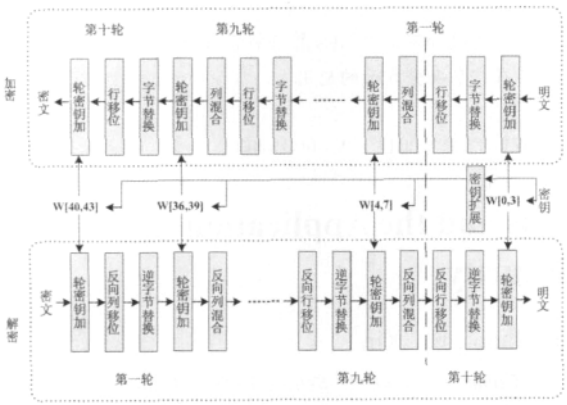

图1 AES加密和解密

图 1 给出了AES 算法的总体结构。加密和解密算法的输入是一个 128 比特的分组，分组是一个字节方阵，被复制到状态数组，这个数组在加密或解密过程中的每一步都会被更改。直到最后一步结束后，状态数组将被复制到输出矩阵。类似地，128 比特的密钥也被描述为一个字节方阵。然后，密钥被扩展成为一个子密钥的数组。每个字是 4 字节，而对于 128 比特的密钥，子密钥总共有 44 个字，矩阵中字节的顺序是按列排序的。比如，128 比特的明文输入的前 4 个字节占输入矩阵的第 1 列，接下来 4 个字节占第 2 列，以此类推 [1]。

1.3 AES算法步骤介绍

AES 算法主要包括：字节替换、行移位、列混合和轮密钥加四个步骤 [2]。

1）字节替换（Substitute Byte）。使用一个表（被称为 S- 盒）对分组进行逐一字节替换。S- 盒是 AES 定义的矩阵，把 State 中每个字节的高 4 位作为行值，低 4 位作为列值，然后取出 S- 盒中对应行列的元素作为输出。这个步骤提供了AES 加密的非线性变换能力。S- 盒与有限域乘法逆元有关，具有良好的非线性特性。为了避免简单代数攻击，S- 盒结合了乘法逆元及可逆的仿射变换矩阵建构而成。

2）行移位（Shift Row）。每一行都向左循环位移某个偏移量。在 AES 中（区块大小 128 位），State 的第一行维持不变，State 的第二行循环左移 1 个字节。同理，State 的第三行及第四行分别循环左移 2 个字节和 3 个字节。经过 Shift Row 之后，矩阵中每一列，都是由输入矩阵中的每个不同列中的元素组成。行移位就是将某个字节从一列移到另一列中，它的线性距离是 4 字节的倍数。

3）列混合（Mix Column）。每列的四个字节通过线性变换互相结合，对每列独立进行操作。每列的四个元素分别当作系数，合并后即为有限域中的一个多项式，接着将此多项式和一个固定的多项式相乘。此步骤亦可视为有限域之下的矩阵加法和乘法。矩阵的系数是基于在码字间有最大距离的线性编码，也是基于算法执行效率的考虑。Mix Column 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，Shift Row 和 Mix Column 两步骤为这个密码系统提供了扩散性。经过几轮列混和变换和行移位变换后，所有的输出位均与所有的输入位相关。

4）轮密钥加（Add Round Key）。在每次的加密循环中，都会由主密钥扩展产生一组轮密钥（通过 Rijndael 密钥生成方案产生），这个轮密钥大小会跟原矩阵一样，该步骤就是轮密钥与原矩阵中每个对应的字节做异或运算。轮密钥加变换非常简单，却能影响 State 中的每一位。密钥扩展的复杂性和 AES 的其他阶段的复杂性，确保了该算法的安全性。

1.4 AES算法模块介绍

AES 算法主要分为三大模块，即密钥扩展，数据加密和数据解密 [3]。

1）密钥扩展。使用 Rotword() 函数将数组中左端第一个数字移至数组的末端，而原来在它之后的数字依次前移一位，即对数组中的数字实现循环左移一位的运算。由于数组中的 4 个数字已合并为一个数字，在程序的实际执行过程中是进行数字的循环移位运算，而不是做数组的循环左移运算，这样可以大大简化运算过程，很大程度提高了运算效率。

2）数据加密。依据 S 置换表，使用 SubByte() 函数对状态矩阵 State[4][4] 中的数字进行置换。使用 ShiftRow() 函数对状态矩阵 State[4][4] 中的各行数据进行循环移位运算。循环移位遵循以下规则，状态矩阵 State[4][4] 中的第一行数据位置不变，第二行数据循环左移一位数字，第三行数据循环左移两位数字，第四行数据循环左移三位数字。

3）数据解密。依据 S 置换表的逆表，使用 InvSubByte() 函数对状态矩阵 State[4][4] 中的数字进行置换，置换方法与 SubByte() 函数相同。使用 InvShiftRow() 函数对状态矩阵 State[4][4] 中的各行数据进行循环移位运算。AES 的解密算法和加密算法不同。尽管密钥扩展的形式一样，但在解密中每轮交换步骤的顺序与加密中的顺序不同。其缺点在于对同时需要加密和解密的应用，需要两个不同的软件或固件模块。

2 AES 在信息安全中的应用

2.1 相关应用简介

随着信息安全要求的不断提高，数据加密作为保护信息安全的重要手段，其应用不再局限于军事、国防等有限领域，

而是迅速走进千家万户。AES 将加密密钥的位数提高到 128bit 以上，极大地增加了破解密文的难度。Rijndael 被选为 AES 是经过多个国家的密码专家广泛讨论的结果。Rijndael 算法具有灵活、简便、抗击多种密码分析的优点，它的目标是发展成能够安全用于商业、政治和军事的加密算法。

AES（Rijndael）算法汇聚了安全性、效率高、易实现性和灵活性等优点，是一种较 DES 更好的算法，通常被认为是 DES 算法的取代者。目前 AES 算法主要用于基于私钥数据加密算法（对称密钥加密算法）的各种信息安全技术和安全产品，为原有的数据加密应用提供更强的数据安全保障。此外，AES 算法硬件实现的速度大约是软件实现的 3 倍，这就给用硬件实现加密提供了很好的机会。随着网络技术发展迅猛，网络数据加密要求日益提高，AES 的应用首先体现在网络信息安全领域中。

2.2 无线网络应用

由于无线网络的通信信道较有线网络更为开放，安全性的要求更高。目前，无线网络主要有两个国际标准：一是用于 WLAN 的 IEEE803.11 协议（Wi-Fi）；二是用于 WMAN 的 IEEE803.16 协议（WiMAX）。这两个协议在制定初期所采用的安全机制分别为 RC4 和 DES，后来这两个协议也都将 AES 加入到协议的安全机制中。此外，为了保障数据传输安全性，其他的一些无线网络技术也都使用了AES。例如 ZigBee 技术，为确保 MAC 帧的完整性、机密性、真实性和一致性，其 MAC 层使用 AES 算法进行加密，并且生成一系列的安全机制。ZigBee 技术是一种近距离、低复杂度、低功耗、低数据速率，低成本的双向无线通信技术，主要适用于自动控制和远程控制领域，可以嵌入到各种设备中。

2.3 电子商务应用

在电子商务方面，主要是 AES 在电子商务基础平台中的密码协议和交易安全协议中的应用。例如，将 AES 应用在 SSL（Secure Sockets Layer 安全套接层）协议中。在实施数据传输前，发送方通过身份认证后，用 SSL 安全通道发送 AES 密钥到接收方的同时，使用 AES 算法对实时数据加密，然后基于 UDP 协议通过互联网发送加密的实时数据到接收方。这样接收方可以用接收到的 AES 密钥得到具体的实时数据。此外，还可以研究将 AES 与其他一些公钥加密算法（非对称加密算法）相结合，设计出新的密码。目前比较典型的研究包括：AES 与 RSA 相结合的混合加密体系；利用 NTRU 公钥密码体系分配 AES 密钥；AES 与 ECC（椭圆曲线加密算法）相结合的加密体系；AES 在数据签名中的应用；AES 在公钥加密体系 PKI 中的应用等等。

2.4 AES软件应用

在 AES 软件实现方面，其应用领域包含语音、视频信息的加密，数据库中的数据加密等。随着计算机对多媒体信息处理能力的增强，多媒体信息加密的问题日渐凸显。由于多媒体信息的数据量很大，直接对其加密效率较低。所以，不仅要考虑数据加密算法 AES 的使用方法，还要设计相应的对多媒体信息进行加密的过程。关于 AES 在数据库方面的应用，主要在于如何在数据输入、输出中生成、分配和管理所用的密钥以及安全的数据加密策略。

2.5 AES硬件应用

在 AES 硬件实现方面，主要方向有射频 IC 卡中的数据安全、智能安全卡和对硬盘数据的加密等方面。目前射频 IC 卡的应用范围很广，如公交 IC 卡、校园一卡通、门禁卡和新一代的居民身份证中都嵌入了 IC 芯片。其中所存储的数据通常都含有持卡人的私人信息，这些信息如果不经过加密处理，很可能泄露出去。因此，如何在射频 IC 卡中加入数据加密功能是 AES 硬件应用的一个研究方向。

3 结束语

AES 的研究从理论到应用，已经深入到了信息安全技术的各个领域，深入研究与开发新的 AES 实现和应用具有重要的理论和实践意义。随着密码技术的高速发展，高级加密标准 AES（Rijndael）算法将逐渐取代 DES 在 IPSec、SSL 和 ATM 中的使用，并广泛应用于虚拟专用网、远程访问服务器（RAS）、SONET（同步光网络）、高速 ATM/Ethernet 路由器、卫星通信、移动通信、电子金融业务等领域。此外，网络保密系统、财政保密、电子游戏保密等方面也将采用 AES 加密算法，将现有的关于 AES 研究成果与其他领域的相关技术与应用相结合，从应用的角度拓展数据加密技术，从而获得新的应用，是 AES（Rijndeal）的发展方向。（责编 杨晨）

参考文献：
[1] William Stallings. 网络安全基础 [M]. 白国强，王海欣，陈弘毅 . 北京：清华大学出版社，2007：31-33.
[2] 卡哈特 . 密码学与网络安全 [M]. 金名等 . 北京：清华大学出版社，2005：9.
[3] 刘天华，孙阳，朱宏峰 . 网络安全 [M]. 北京：科学出版社，2010.4.

资讯

第十二届中国信息安全大会在北京召开

4 月 21 日，第十二届中国信息安全大会在北京召开。本次大会是由中国电子信息产业发展研究院主办、中国计算机报社承办，并得到中国计算机学会计算机安全专业委员会、公安部第一研究所、中国信息安全测评中心、中国信息安全认证中心、国家计算机病毒处理中心等单位的大力支持和指导。同时，还得到了中国信息主管网，网易科技频道、中国计算机行业网，中国计算机安全网等网络媒体的特别支持。会上，来自政府主管部门、行业应用部门和企业的代表共计 500 余人围绕当前信息安全领域的热点话题展开了讨论。（记者 杨晨）