一种 AES 算法的网络通信信息加密传输系统设计

赵莉莉，张继琛
（潍坊科技学院　山东　潍坊　262700）

【摘要】为解决传统信息传输方式安全性差的问题，本文设计了一种基于高级加密标准（advanced encryption standard，AES）算法的网络通信信息加密传输系统，通过 AES 算法对数据进行加密处理，确保信息在传输过程中的机密性和完整性。本文详细介绍了 AES 算法原理、系统各模块设计以及实际应用，旨在为网络通信安全提供有效的解决方案。

【关键词】高级加密标准（AES）算法；信息加密；网络通信；安全性；加密传输系统
【中图分类号】TN918　　【文献标识码】A　　【文章编号】1009-5624（2024）12-0095-03
DOI:10.16009/j.cnki.cn13-1295/tq.2024.12.031

0　引言

信息化时代，数据传输的安全性至关重要。传统的明文传输方式容易受到各种攻击，导致信息泄露和篡改，随着信息技术的不断发展，网络通信安全成为重要的研究课题。为解决这一问题，本文提出了一种基于高级加密标准（advanced encryption standard，AES）算法的网络通信信息加密传输系统设计方案，通过对数据进行加密，保障信息在传输过程中的安全。

1　AES 算法原理

1.1 基本原理

AES 算法是一种对称加密算法，即加密和解密使用相同的密钥[1-2]。AES 算法以其高效性和安全性广泛应用于各类数据加密场景。AES 支持 128 位、192 位和 256 位密钥长度，其中 128 位密钥使用最为普遍。AES 算法主要包括多轮字节替换、行移位、列混淆和轮密钥加等操作。

1.2 AES 算法加密过程

AES 算法加密过程分为多个步骤。①将明文数据与初始轮密钥进行异或操作；②进行多轮变换，每轮包括字节替换（使用 S 盒进行非线性替换）、行移位（对数据行进行循环移位）、列混淆（对数据列进行混淆操作，除最后一轮外）和轮密钥加（与轮密钥进行异或操作）；③通过轮变换（包括字节替换、行移位和轮密钥加）生成最终的密文。

基于 AES 算法的网络通信信息加密传输系统由数据发送端、密钥管理模块和数据接收端组成。数据发送端通过初始轮密钥加、多轮变换和最终轮变换对原始数据进行 AES 算法加密，并通过网络传输模块将加密后的数据发送到接收端。数据接收端通过相应的逆变换过程进行解密，恢复原始数据。密钥管理模块生成、分发和管理 AES 加密所需的密钥，确保发送端和接收端使用相同的密钥进行加密和解密操作。完整的系统设计保障了网络通信信息的安全传输，整体的系统设计架构如图 1 所示。

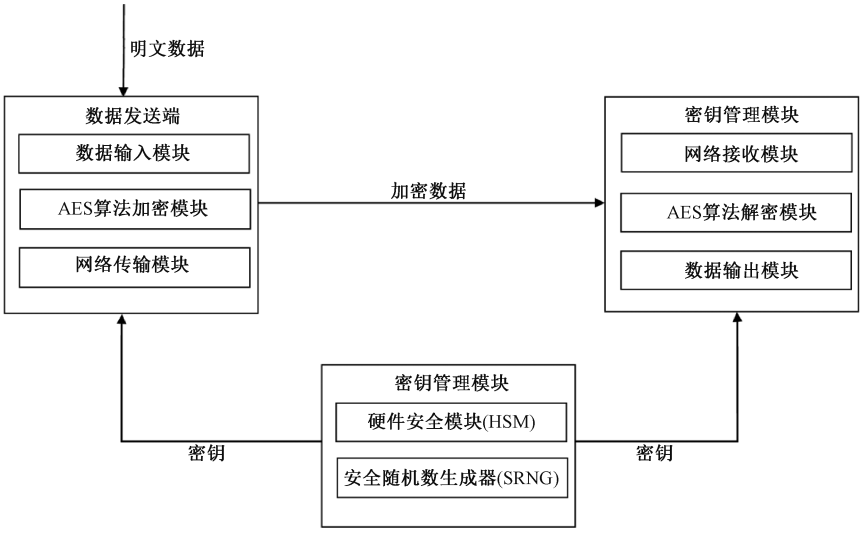

图 1　基于 AES 算法的网络通信信息加密传输系统设计架构

1.2.1 数据发送端

数据发送端主要包括数据输入模块、AES 算法加密模块和网络传输模块。

首先，通过数据输入模块获取待加密的原始数据（明文数据）P，随后使用 AES 算法加密模块对数据进行加密，加密过程如下。

（1）将明文数据 P 与初始轮密钥 K_0 进行异或操作，如

作者简介：赵莉莉（1993—），女，山东菏泽，硕士，助教，研究方向：信号与信息处理。

式(1)所示[3]。

$$\boldsymbol{S}_0 = P \oplus K_0 \tag{1}$$

式中：$\boldsymbol{S}_0$ 为初始轮密钥加后的数据状态矩阵；⊕ 为按位异或操作。

(2)使用 128 位密钥进行十轮变换。使用 S 盒对每个字节进行非线性替换，如式(2)所示。

$$\boldsymbol{S}_i' = \mathrm{SubBytes}(\boldsymbol{S}_i) \tag{2}$$

式中：$\boldsymbol{S}_i'$ 表示字节替换后的数据状态矩阵；SubBytes 为 S 盒替换操作；$\boldsymbol{S}_i$ 为当前轮的数据状态矩阵。$\boldsymbol{S}_i'$ 对状态矩阵中的每一行进行循环移位操作，如式(3)所示。

$$\boldsymbol{S}_i'' = \mathrm{ShiftRows}(\boldsymbol{S}_i') \tag{3}$$

式中：$\boldsymbol{S}_i''$ 为行移位后的数据状态矩阵；ShiftRows 为行移位操作。对状态矩阵中的每一列进行混淆操作(除最后一轮外)，如式(4)所示。

$$\boldsymbol{S}_i''' = \mathrm{MixColumns}(\boldsymbol{S}_i'') \tag{4}$$

式中：$\boldsymbol{S}_i'''$ 为列混淆后的数据状态矩阵；MixColumns 为列混淆操作。将变换后的状态矩阵与当前轮密钥进行异或操作，如式(5)所示。

$$\boldsymbol{S}_{i+1} = \boldsymbol{S}_i''' \oplus K_{i+1} \tag{5}$$

式中：$\boldsymbol{S}_{i+1}$ 为当前轮密钥加后的数据状态矩阵；⊕ 表示按位异或操作；K_{i+1} 为第 $i+1$ 轮的轮密钥。

(3)进行最终轮变换。最后一轮不进行列混淆，仅包括字节替换、行移位和轮密钥加，如式(6)所示。

$$C = \mathrm{ShiftRows}(\mathrm{SubBytes}(\boldsymbol{S}_9)) \oplus K_{10} \tag{6}$$

式中：C 为最终生成的密文；ShiftRows 为行移位操作；SubBytes 为字节替换操作；$\boldsymbol{S}_9$ 为第 9 轮的数据状态矩阵；⊕ 表示按位异或操作；K_{10} 为第 10 轮的轮密钥。

(4)通过网络传输模块将加密后的数据 C 发送到接收端。

1.2.2 数据接收端

数据接收端主要包括网络接收模块、AES 算法解密模块和数据输出模块。

接收端通过网络接收模块获取加密数据 C，随后使用相同的密钥 K 和相同的 AES 算法对加密数据 C 进行解密。解密过程如下。

(1)将接收到的加密数据 C 与初始轮密钥 K_{10} 进行异或操作，如式(7)所示。

$$\boldsymbol{S}_9 = C \oplus K_{10} \tag{7}$$

式中：$\boldsymbol{S}_9$ 为中间状态矩阵，用于下一步的解密过程；⊕ 为按位异或操作。

(2)使用 128 位密钥进行十轮变换，变化过程为：

①将变换后的状态矩阵与当前轮密钥进行逆向异或操作，如式(8)所示。

$$\boldsymbol{S}_i''' = \boldsymbol{S}_{i+1} \oplus K_{i+1} \tag{8}$$

式中：$\boldsymbol{S}_i'''$ 为通过逆向异或操作生成的前一轮状态矩阵，用于接下来的解密过程；$\boldsymbol{S}_{i+1}$ 为当前轮的状态矩阵，是上一步处理后的结果；⊕ 为按位异或操作；K_{i+1} 为当前轮的密钥，用于本轮解密。

②对状态矩阵中的每一列进行逆向混淆操作(除第一轮外)。

③对状态矩阵中的每一行进行逆向移位操作。

④使用逆 S 盒对每个字节进行非线性替换。

⑤最后一轮不进行逆列混淆，仅包括逆行移位、逆字节替换和逆轮密钥加。得到解密后的数据状态矩阵 $\boldsymbol{S}_0$。

(3)将解密后的原始数据 $\boldsymbol{S}_0$ 输出至数据输出端，得到明文 P。

接收端的解密过程与发送端的加密过程相对应，通过逆向的 AES 算法和相同的密钥 K 实现了对加密数据的解密，确保了数据在传输过程中的安全性和完整性。

1.2.3 密钥管理模块

密钥管理模块负责生成、分发和管理 AES 算法加密所需的密钥。密钥的安全性至关重要，因此，采用安全的密钥分发机制，确保发送端和接收端使用相同的密钥进行加密和解密操作。常见的密钥分发方法包括预共享密钥和基于公钥加密的密钥交换协议。密钥管理的实现过程如下。

(1)使用一个安全随机数生成器(secure random number generator，SRNG)生成 AES 算法加密所需的密钥 K[4]。本文设计的基于 AES 算法的网络通信信息加密传输系统使用 128 位密钥。如式(9)所示。

$$K = \mathrm{SRNG}(128\,\mathrm{bits}) \tag{9}$$

式中：K 为生成的 AES 密钥；SRNG 为安全随机数生成器。

(2)密钥分发，过程为如下。

①预共享密钥。在发送端和接收端预先共享同一个密钥 K。该方法适用于双方在安全环境下直接交换密钥的场景。如式(10)所示。

$$K \rightarrow \mathrm{SE\ and\ RE} \tag{10}$$

式中：SE 为发送端；RE 为接收端。

②基于公钥加密的密钥交换协议：使用公钥加密算法(如 RSA 或 Diffie-Hellman 密钥交换协议)进行密钥分发。本文使用 RSA 算法实现密钥分发，过程为[5]：

首先，生成一对公钥和私钥 $(K_{\mathrm{pub}}, K_{\mathrm{pri}})$。

随后，发送端用接收端的公钥 K_{pub} 加密生成的密钥 K，如式(11)所示。

$$C_K = \mathrm{Encrypt}(K_{\mathrm{pub}}, K) \tag{11}$$

式中：Encrypt 为加密操作。

最后，接收端接收到加密的密钥 C_K，用自己的私钥 K_{pri} 解密获取密钥 K，如式(12)所示。

$$K = \mathrm{Decrypt}(K_{\mathrm{pri}}, C_K) \tag{12}$$

式中：Decrypt 为解密操作。

(3)密钥管理。在整个通信过程中，密钥管理模块还负责密钥的定期更新和存储安全。为确保密钥不被泄露，采用硬件安全模块进行密钥管理[6]。硬件安全模块是一

种专用的硬件设备,专门用于生成、存储和管理加密密钥,并提供高安全性的加密处理。硬件安全模块通过硬件加密技术保护密钥,确保密钥不被泄露或篡改。

密钥管理模块通过安全的密钥管理机制,确保发送端和接收端能够使用相同的密钥 K 进行加密和解密操作,保证了网络通信信息的安全性和完整性[7]。

2 AES 算法的网络通信信息加密传输系统的应用

在实际应用中,基于 AES 算法的加密传输系统广泛应用于电子商务、政府通信等领域。

2.1 电子商务领域的应用

在电子商务领域,保护用户支付信息和订单数据的安全性至关重要。通过使用基于 AES 算法的网络通信信息加密传输系统,电子商务平台能够有效防止支付信息的泄露和欺诈行为。未加密的传输系统和基于 AES 算法加密的传输系统在电子商务领域中的应用效果对比如表 1 所示。

表 1 加密前后的系统在电子商务领域中的应用效果对比

系统	每年支付信息泄露事件数量	每年支付欺诈事件数量	每年用户投诉数量	数据传输加密覆盖率/%	用户满意度(1~10)
未加密的传输系统	200	150	500	0	3
基于 AES 加密的传输系统	8	5	15	99.98	8

表 1 结果显示,基于 AES 算法加密的传输系统应用于电子商务领域,大幅减少了支付信息泄露和欺诈事件,用户投诉数量显著下降,用户满意度大幅提升。数据传输的加密覆盖率达到 99.98%,确保支付信息在传输过程中的安全性,增强了用户对电子商务平台的信任。

2.2 应用于政府通信

在政府通信中,保护机密信息的安全性和完整性至关重要。使用基于 AES 算法的网络通信信息加密传输系统,可以有效防止机密信息泄露和篡改,确保政府通信的安全。表 2 展示了未加密的传输系统和基于 AES 算法加密的传输系统在政府通信中的应用效果对比。

表 2 结果显示,基于 AES 加密的传输系统应用于政府通信,显著降低了机密信息泄露和篡改事件的数量,安全事故响应次数大幅减少,信息安全评分显著提升。数据传输的加密覆盖率达到 99.99%,确保机密信息在传输过程中的安全性,极大地增强了政府通信的保密性和安全性。

表 2 加密前后的系统在政府通信中的应用效果对比

系统	每年机密信息泄露事件数量	每年信息篡改事件数量	每年安全事故响应次数	数据传输加密覆盖率/%	信息安全评分(1~10)
未加密的传输系统	30	15	20	0	3.5
基于 AES 加密的传输系统	1	1	2	99.99	9.5

3 结语

本文设计了一种基于 AES 算法的网络通信信息加密传输系统,通过对数据进行加密处理,提升了信息传输的安全性和可靠性。具体应用中,在电子商务领域,支付信息泄露和欺诈事件大幅减少,用户满意度显著提升;在政府通信中,机密信息泄露和篡改事件显著减少,信息安全评分显著提高。未来,随着网络通信技术的不断发展和信息安全需求的不断提高,AES 算法将在更多领域中得到应用和优化。

【参考文献】

[1] 李文迪. 基于改进 AES 算法的通信信息加密安全传输方法研究[J]. 中国新技术新产品, 2024(7): 143-145.
[2] 姚旭影. 基于 AES 算法和混沌映射的嵌入式终端数据传输并行加密方法[J]. 安阳工学院学报, 2024, 23(2): 54-59.
[3] 邱建兵, 胡勇. 一种基于异或运算的属性撤销 CP-ABE 方案[J]. 四川大学学报(自然科学版), 2024, 61(1): 95-101.
[4] 王永, 龚建, 王明月, 等. 一种整数混沌映射的伪随机数生成器[J]. 北京邮电大学学报, 2022, 45(1): 58-62.
[5] 刘晓峻. 基于 RSA 算法的电力通信信息安全保护方法[J]. 信息与电脑(理论版), 2023, 35(22): 57-59.
[6] 于少军. 商用密码应用中基于硬件安全模块的密钥管理研究[J]. 信息与电脑(理论版), 2024, 36(5): 207-209.
[7] 周力. 基于 AES 算法的网络通信信息加密传输技术研究[J]. 长江信息通信, 2023, 36(1):70-72.