AES原理与仪器

制作人：PPT制作者
时间：2024年X月

目录

01

第1章 AES概述

AES的定义

AES，即高级加密标准，是一种用于电子数据加密的对称加密算法。

AES的用途

加密电子数据

保护信息安全

国际标准

全球范围内被广泛采用

广泛应用

电子政务、电子商务等领域

AES的制定机构

美国国家标准与技术研究院（NIST）负责制定和推广AES算法。

02

第2章 AES的算法原理

AES的优点

强大的安全性

128位、192位、256位三种密钥长度

良好的兼容性和灵活性

硬件和软件均适用

高效的资源占用

资源消耗低

高速的加密和解密速度

适用于各种场景

AES的缺点

密钥管理困难

密钥生成、分发、存储和废弃都需要严格管理

算法复杂性

实现AES需要较高的编程技术

对硬件要求较高

加密和解密速度受到硬件性能的限制

AES的加密流程

AES加密流程包括初始轮、轮加密、轮密钥生成和输出轮。

AES的解密流程

AES解密流程包括初始轮、轮解密、轮密钥生成和输出轮。

● 03

第3章 AES的密钥生成

AES密钥的构成

AES密钥由主密钥和轮密钥组成，分别用于初始化轮密钥和加密解密过程。密钥长度有128位、192位、256位三种。

AES密钥的生成过程

主密钥生成

随机生成或基于密码散列函数

轮密钥生成

通过密钥扩展算法，从主密钥派生出多个轮密钥