计算机工程与应用 2006 42 (12期): ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

一种改进ECB模式的AES算法加解密优化方案

朱灵波, 戴冠中, 刘航

西北工业大学控制与网络研究所 信息安全中心

收稿日期 2006-1-12 修回日期 网络版发布日期 接受日期

摘要 分组对称加密算法的工作模式对于敏感信息的安全性至关重要。本文采用了工作于改进ECB模式（IECB）的AES算法实现了文件加解密，提高了数据存储的安全性。文中还提出一种文件尾端处理方法以适应分组加解密的要求，并对不同文件大小采用分类处理策略以达到优化时空消耗的目的。最后通过实验比较了IECB和ECB的性能差异，结果表明IECB能稳定工作，获得正确、可靠的结果。

关键词 AES算法,ECB模式,IECB模式,尾端处理,分类处理

分类号

An Optimized Data Stream Encryption and Decryption Implementation of AES Algorithm with improved-ECB(IECB) Mode

Ling-Bo Zhu,,

西北工业大学控制与网络研究所 信息安全中心

Abstract

The operation mode of block cipher algorithm is of vital importance for information security. In this paper, IECB:an improved data stream encryption and decryption implementation of AES algorithm,IECB is presented to encrypt\decrypt data stream and proved to be able to enhance the data storage security. Trial disposing is presented to satisfy block cipher and will achieve the optimal with space and time consumption by classification disposing according to different document sizes. Finally a comparison of the performance between IECB and ECB through experiment is made and it demonstrates that IECB mode can work steadily and obtain correct and reliable result.

Key words AES algorithm ECB mode IECB mode trail processing classification processing

DOI:

通讯作者 朱灵波 朱灵波 semitroy@sohu.com