云南大学学报（自然科学版）
JOURNAL OF YUNNAN UNIVERSITY(NATURAL SCIENCES)
中文核心期刊
中国科技核心期刊

云南大学学报(自然科学版) » 2004, Vol. 26 » Issue (3): 212-215 DOI:

RSA加密体制的安全隐患

杨维忠[1], 李彤[2], 郝林[1]
1. 云南大学, 计算机科学系, 云南, 昆明, 650091;
2. 云南大学, 软件学院, 云南, 昆明, 650091

Hidden security flaws of RSA encryption system

YANG Wei-zhong[1], LI Tong[2], HAO Lin[1]
1. Department of Computer Science, Yunnan University, Kunming 650091, China;
2. School of Software, Yunnan University, Kunming 650091, China

- 摘要
- 参考文献
- 相关文章

全文: PDF (803 KB) HTML (KB) 输出: BibTeX | EndNote (RIS) 背景资料

摘要 详述了RSA算法,给出了RSA加解密的算法以及它的抗攻击能力分析表,而且总结了常见的攻击方式,最后分析了在实际应用中存在的一些弊端.

关键词： RSA 公钥密码体制 安全性

Abstract： It is explicated the theory of RSA,and presented the RSA algorithms.Also,it is analysed RSA’s ability against attack,and summarized the ordinary ways of attack.Finally,it is explored the flaws of RSA system in practical use.

Key words： RSA public key cryptography security

收稿日期: 2003-09-09;

基金资助:云南省自然科学基金资助项目(2002F0010M);云南省科技攻关项目(2001I710);云南省省校省院合作项目(2001AABLA002)

服务
- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- E-mail Alert
- RSS

作者相关文章
- 杨维忠
- 李彤
- 郝林

引用本文:

杨维忠,李彤,郝林. RSA加密体制的安全隐患[J]. 云南大学学报(自然科学版), 2004, 26(3): 212-215.

YANG Wei-zhong,LI Tong,HAO Lin. Hidden security flaws of RSA encryption system[J]. , 2004, 26(3): 212-215.

没有本文参考文献

没有找到本文相关文献

编辑出版：云南大学学报编辑部 (昆明市翠湖北路2号, 650091)
电话：0871-5033829(传真) 5031498 5031662 E-mail: yndxxb@ynu.edu.cn yndxxb@163.com