吉首大学学报自然科学版 » 2007, Vol. 28 » Issue (5): 34-37 DOI:

RSA算法中安全大素数生成方法及其改进

(湖南娄底职业技术学院，湖南 娄底 417000)

Study and Improvement of Generation Method of Safety Big Prime Number in RSA Algorithm

(Loudi Vocational & Technical College,Loudi 417000,Hunan China)

摘要 在介绍RSA算法的基本原理及加、解密过程的基础上，分析比较了各种检测素数的方法，综合各种方法的优缺点，提出了一种新的生成安全大素数的方法.

关键词： RSA公钥密码体制 安全大素数 素数检测

Abstract: This paper introduces the basic principle and the encryption and decryption process,and analyses and compares different prime testing algorithms.It gives a new algorithm of safety big prime generation by considering the good and bad points of each method.

Key words: RSA safety big prime number prime testing

基金资助：

湖南省教育厅科学研究项目（05D060）；娄底职业技术学院科研资助项目（05ZF001）

作者简介：游新娥(1968-)，女，湖南双峰人，湖南省娄底职业技术学院计算机副教授，高级程序员，硕士研究生，主要从事软件工程与信息安全研究.

引用本文:

游新娥. RSA算法中安全大素数生成方法及其改进[J]. 吉首大学学报自然科学版, 2007, 28(5): 34-37.

YOU Xin-E. Study and Improvement of Generation Method of Safety Big Prime Number in RSA Algorithm[J]. Journal of Jishou University(Natural Sciences Edit, 2007, 28(5): 34-37.

[1] DOUGLAS R STINSON(著).冯登国(译).密码学原理与实践 [M].北京：电子工业出版社，2003.

[2] WENBO MAO(著).王继红，伍前红(译).现代密码学理论与实践 [M].北京：电子工业出版社，2004.

[3] 胡志远.口令破解与加密技术 [M].北京：机械工业出版社，2003.

没有找到本文相关文献

通讯地址：湖南省吉首市人民南路120号《吉首大学学报》编辑部 邮编：416000
电话传真：0743-8563684 E-mail：xb8563684@163.com 办公QQ：1944107525