计算机工程　2006 32 (16): 118-119,124　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

RSA算法中几种可能泄密的参数选择

谢建全1,2,阳春华1

1. 中南大学信息科学与工程学院，长沙 410083；2. 湖南财经高等专科学校，长沙 410205

收稿日期　修回日期　网络版发布日期 2006-8-14　接受日期

摘要　RSA加密算法是目前使用较多、安全性高的一种非对称加密算法，在实际应用中要使该算法有较高的防破解强度，在大素数的选择上是有要求的。文章给出了选择高质量的大素数的有效方法，并对一些不当的选择可能造成的泄密给出了相应的证明。

关键词　大素数　RSA算法　安全性　攻击

分类号

DOI:

对应的英文版文章：2006-16-044

通讯作者:

作者个人主页: 谢建全1;2;阳春华1