吉首大学学报自然科学版 » 2013, **Vol. 34** » Issue (5): 42-44 DOI: 10.3969/j.issn.1007-2985.2013.05.010

计算机 最新目录 | 下期目录 | 过刊浏览 | 高级检索 Previous Articles | Next Articles

基于Visual Foxpro的ElGamal数字签名算法

李淑敬, 李林国

(阜阳师范学院信息工程学院，安徽 阜阳 236041)

Realization of EIGamal Digital Signature in VFP

LI Shu-Jing, LI Lin-Guo

(College of Information Engineering,Fuyang Teachers College,Fuyang 236041,Anhui China)

- 摘要
- 参考文献
- 相关文章

全文: PDF (348 KB) HTML (1 KB) **输出:** BibTeX | EndNote (RIS) **背景资料**

摘要 数字签名的使用越来越广泛，其主要的实现方法是公钥密码算法.ElGamal算法是一种比较常用的公钥密码算法，既可以用于加密又可以用于签名，具有生成速度快、签名验证简单的特点.VFP(Visual Foxpro)是一种使用比较广泛的面向对象的数据库设计系统，基于VFP的签名实现方法比较少.介绍ElGamal数字签名算法在VFP中的实现，阐述了ElGamal数字签名算法的原理，详细介绍了算法的实现过程，最后给出在VFP中ElGamal数字签名的实现界面.

关键词: EIGamal 数字签名 Visual Foxpro

Abstract: The digital signature is realized maily by the symmetric encryption algorithm.ElGamal algorithm,a commonly used symmetric encryption algorithm,is widly used in the digital signature and the encryption,with the advantages of fast generation and simple signature verification.Visual Foxpro is a widdely-applied targe-oriented databse designing system.In this paper the realization of ElGamal digital signature algorithm is detailedly introduced,and the course and interface of ElGamal digital signature in VFP is described.

Key words: ElGamal algorithm digital signature visual foxpro

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

- 李淑敬
- 李林国

基金资助:

阜阳师范学院科研资助项目（2009FSKJ16）；安徽省青年人才基金资助项目（2010SQTL196）；安徽省自然科学基金资助项目（KJ2012B138）

作者简介: 李淑敬（1981-），女，山东聊城人，阜阳师范学院讲师，硕士研究生，主要从事网络安全研究.

引用本文:

李淑敬,李林国. 基于Visual Foxpro的EIGamal数字签名算法[J]. 吉首大学学报自然科学版, 2013, 34(5): 42-44.

LI Shu-Jing,LI Lin-Guo. Realization of EIGamal Digital Signature in VFP[J]. Journal of Jishou University(Natural Sciences Edit, 2013, 34(5): 42-44.

[1] 李淑敬，李林国.基于PKI数字签名在校园网中的设计方案 [J].微计算机信息,2012,28(10)：369.

[2] 孙金青，孙艳蕊，袁喜凤，等.可转化的基于EIGamal环签名方案 [J].微计算机信息,2008,24(4-3)：49-50.

[3] 李滨.EIGamal签名方案的安全性分析及其改进 [J].西南民族大学学报：自然科学版，2006,32(2)：376-379.

[4] 何少芳.基于EIGamal 加密算法的非对称数字指纹体制 [J].现代电子技术，2010(3)：47-48.

[5] 许倩.代理盲签名理论及其在电子现金系统中的研究与应用[D].广州：华南理工大学电子与信息学院，2010.

[6] 邓从政.EIGamal数字签名系统的一种伪签名算法及其安全性分析 [J].成都大学学报：自然科学版，2006,25(4)：284-286.

[7] 余姜德，商林，于志平.EIGamal加密体制在软件保护技术中的应用 [J].计算机与现代化,2005(5)：86-88.

[8] 张勇.用VC程序求有限域的本原元及其应用 [J].河北北方学院学报：自然科学版,2009,25(5)：15-17.

[9] 尹少平.密钥交换协议中本原根的快速确定方法及其实现 [J].微计算机信息，2006,22(8-3):101-103.

[1] 曾岫, 彭宏, 左国威, 张为民. **SOAP安全工具包的设计与实现**[J]. 吉首大学学报自然科学版, 2009, 30(2): 38-40.