计算机工程 2009 35 (23): 130-132,135 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

RC4流密码与微软Office文档安全分析

何克晶

(华南理工大学计算机科学与工程学院，广州 510641)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 根据微软官方文档、OpenOffice文档及wvWare实现等完全公开的信息，对RC4流密码及其在微软Office系列中的实现进行分析，认为Office 97~2003所默认使用的40 bit加密方式较不安全，通过结合Rainbow预计算攻击方法，证实其脆弱性。通过研究，建议不使用默认的“Office 97/2000兼容”40 bit加密，而采用更安全的“Microsoft Enhanced Cryptographic Provider”128 bit加密，或者使用压缩软件进行二次加密，从而进一步提高安全性。

关键词 RC4流密码；预计算攻击；微软Office；文档安全

分类号 TP309

DOI:

通讯作者:

作者个人主页: 何克晶