

## <<网络信息安全与 PGP 加密>>

### 图书基本信息

书名：<<网络信息安全与 PGP 加密>>

13位ISBN编号：9787302030065

10位ISBN编号：7302030065

出版时间：1998-07

出版时间：清华大学出版社

作者：林东

页数：340

字数：550

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<网络信息安全与 PGP 加密>>

### 内容概要

本书以因特网用户为对象，深入浅出地介绍了密码学初步知识，包括现代加密技术前沿——公开密钥加密系统在内的一些高强度信息加密技术发展演变历程，详述了新的而可靠、用户易于实践又颇受欧美网络界人士喜爱的PGP加密系统的操作环境和使用方法；在分析因特网安全隐患的基础上，向网络用户推荐了应该掌握的一些信息保护措施，并为进一步拓展这方面的知识，提供了可资跟踪方向的重要站点网址。

本书适用于因特网广大用户、计算机专业科生、网络管理人员、信息安全技术专业人员。

# <<网络信息安全与PGP加密>>

## 书籍目录

序引言第一部分 加密技术与PGP系统概论第一章 国际互联网与数据加密技术1.1 国际互联网的历史、现状及其不安全性1.1.1 历史与现状1.1.2 电子邮件与万维网1.1.3 国际互联网的不安全性1.2 解决国际互联网的安全问题1.3 用PGP加密系统保护通信安全第二章 密码学初步与公开密钥加密系统2.1 加密方法2.1.1 代码加密2.1.2 替换加密2.1.3 变位加密2.1.4 一次性密码簿加密2.2 密钥与密码破译方法2.2.1 密钥的穷尽搜索2.2.2 密码分析2.2.3 其它密码破译方法2.3 对传统加密方法的分析2.3.1 传统密码加密举例2.3.2 传统加密方法存在的问题2.4 公开密钥加密系统2.4.1 什么是公开密钥加密系统2.4.2 公开密钥加密系统的优点2.4.3 使用公开密钥加密系统的数字签字技术2.4.4 与传统加密方法的结合2.5 PGP加密系统的流程和基本术语2.6 加密方法的可靠性第三章 现代加密技术与PGP的历史回顾3.1 官方和民间对加密技术的研究3.2 加密技术标准化——DES的诞生3.3 DES的破译和安全使用3.4 公开密钥加密技术的兴起3.4.1 Ralph Merkle 猜谜法3.4.2 Diffie-Hellman的指数密钥交换加密3.4.3 RSA加密算法3.4.4 背包加密算法及其教训3.5 把公开密钥加密技术推广向市场3.6 PGP加密系统的诞生3.6.1 PGP的作者——菲尔·齐默尔曼3.6.2 齐默尔曼的自拟算法和PGP 2.0版的3.6.3 PGP1.0版的发行3.7 PGP的成长壮大3.7.1 摈弃齐默尔曼的自拟算法和PGP 2.0版的发行3.7.2 PGP发行走向金化的道路3.7.3 PGP商业版与金的菲商业版3.7.4 PGP系统在世界上的迅速传播3.7.5 美国政府对齐默尔曼的调查3.8 PGP的未来3.8.1 破译129位RS密码3.8.2 向RSA算法提出挑战第四章 PGP加密技术面对的社会和法律问题4.1 联邦政府与窃听4.2 联邦调查局的数字电话计划4.3 美国国家安全局的Clipper世片4.4 美国加密技术的出口管理制作4.5 专利法对公开密钥加密技术发展的影响第二部分 PGP加密系统的操作与应用第五章 准备工作5.1 PGP的主要版本和辅助软件5.1.1 PGP的主要版本5.1.2 PGP的辅助软件5.2 运行前的准备工作5.2.1 用户界面5.2.2 联机帮助5.2.3 命令格式5.2.4 输出文件格式5.2.5 文件名后缀约定5.2.6 环境变量5.2.7 配置文件和变量5.2.8 语种文件第六章 用PGP保护文件6.1 对文件加密6.1.1 文件加密示例6.1.2 文件加密的内部过程6.2 销毁原文件6.3 对文件解密6.4 加密生成ASCII文件6.5 单独使用文本文件转换开关符6.6 破译PGP文件加密的方法小结 第七章 配制PGP的钥匙对7.1 配制PGP公开秘密钥匙对示例7.2 含金量配制的内部过程7.2.1 选择钥匙长度7.2.2 供用户标识信息7.2.3 选择口令7.2.4 制造伪随机数7.3 用户可能会遇到的问题小结 第八章 用PGP保护电子通信8.1 加密通信内容示例8.1.1 起草信件内容8.1.2 用收件人的公开钥匙加密信件内容8.1.3 发出加密后的信件8.1.4 使用文本格式转换8.1.5 销毁原文件8.1.6 阅读后即销毁8.2 加密通信的内部过程8.3 一次完成发送加密电子邮件8.3.1 起草和加密同时完成8.3.2 加密与发送一次完成8.3.3 起草、加密和发送一次完成8.4 接收加密的邮件8.4.1 解密电子邮件示例8.4.2 解密的内部过程8.4.3 改变解密输出文件8.4.4 只阅读不存盘8.5 发送大文件8.5.1 发送大文件示例8.5.2 改变子文件大小的缺省值8.6 发送多个收件人的电子邮件8.6.1 多个收件人的邮件示例8.6.2 让发信人也能阅读密文8.7 破译PGP通信加密的方法小结 第九章 用PGP作数字签字9.1 数字签字示例9.1.1 为文件作数字签字9.1.2 鉴别数字签字9.2 MD5报文分解函数9.3 PGP系统数字签字的内部过程9.4 PGP系统数字签字的操作9.4.1 发送既加密又签字的邮件9.4.2 接收带数字签字的邮件9.4.3 生成单独的签字文件9.4.4 选择特定的钥匙签字小结 第十章 管理PGP密钥10.1 公开和秘密钥环文件10.2 显示钥匙环上的钥匙10.3 修改钥匙证书内容10.3.1 改变用户口令10.3.2 增加用户标识信息10.3.3 删除用户标识信息10.3.4 修改用户标识信息10.4 公开钥匙的分发10.4.1 直接拷贝公开钥匙环文件10.4.2 提取公开钥匙输出到文件10.4.3 提取公开钥匙用电子邮件发送10.4.4 提取多把公开?匙10.5 往钥匙环上加入钥匙10.6 从钥匙环上删除钥匙10.7 PGP软件包自带的钥匙文件小结 第十一章 PGP证明和分发钥匙11.1 伪造的RSA钥匙11.2 社会中建立信任关系的方式11.3 PGP的信任网11.4 加入无签字的钥匙11.5 加入经签字的钥匙11.6 修改信任度11.7 为钥匙签字11.8 删除钥匙上的签字小结 第十二章 PGP吊销、停用和备份钥匙12.1 吊销公开钥匙12.2 停用公开钥匙12.3 备份钥匙12.3.1 简单的钥匙备份方法12.3.2 拆分口令的钥匙备份方法12.3.3 通用的钥匙备份方法小结 第十三章 PGP的配置文件13.1 什么是配置文件13.2 修改配置文件13.3 在命令行上临时修改配置变量的取值13.4 缺省配置文件13.5 配置变量一览第十四章 PGP公开钥匙服务器14.1 PGP公开钥匙服务器14.2 通过万维网使

## <<网络信息安全与PGP加密>>

用PGP服务器14.3 通过电子邮件使用PGP服务器14.4 通过匿名文件传输协议(FTP)使用服务器14.5  
常见问题第三部分 网络用户的信息保护第十五章 国际互联网用户信息的安全问题15.1 用户识别系统15.1.1 UNIX口令系统15.1.2 PGP的口令系统15.1.3 基于时间的一次性口令系统15.1.4 挑战-回答式的一次性口令系统15.1.5 其它识别系统15.2 数据备份15.3 软件系统中的“机关”15.4 网络系统中的个人计算机15.4.1 个人计算机的可信性15.4.2 计算机硬件的可信性15.5 国际互联网上的付款系统15.5.1 Netscape浏览器15.5.2 Cybercash信用卡付款系统15.5.3 DigiCash的电子钞票系统15.6 国际互联网上的证书签发机构第十六章 国际互联网上的匿名的转发系统16.1 匿名电子邮件转发系统的原理16.2 选择匿名转发系统的考虑因素16.2.1 系统实现匿名的方法16.2.2 系统的信息加密功能16.2.3 系统及管理人士的声誉16.2.4 系统可靠性及性能指标16.3 有关匿名转发系统的争议16.4 网上的主要匿名转发系统16.5 Penet转发系统16.5.1 申请匿名帐号16.5.2 设定和改变口令16.5.3 选择别名16.5.4 发匿名信16.5.5 匿名红贴网络新闻16.5.6 公开和匿名回信16.5.7 正式使用前的试用16.5.8 取消匿名帐号16.5.9 改变地址、求助和保密16.6 Cypherpunks转发系统16.6.1 匿名电子邮件和网络新闻16.6.2 加密发信内容16.6.3 回复匿名信16.6.4 回信内容的保密16.6.5 保护回信人身份16.6.6 其它辅助功能16.6.7 多次转发16.6.8 求助16.6.9 第二代Cypherpunks匿名转发系统16.7 Alpha转发系统16.7.1 建立匿名帐号16.7.2 发匿名和刊登网络新闻16.7.3 正式使用前的试用16.7.4 回复匿名信16.7.5 改变匿名帐号口令和回信地址16.7.6 关闭匿名帐号16.7.7 多次转发16.7.8 巧用带加密转发系统16.7.9 求助16.8 关于建立和使用多次转发的建议16.9 通过万维网发送匿名电子邮件小结 附录 附录A 如何获取PGP软件A.1 PGP各版本与其合性A.2 PGP各版本比较A.3 PGP的发行机构A.4 通过文件传输协议服务器获取PGP A.5 通过万维网获得PGP附录B 如何安装PGP DOS版B.1 展开软件包B.2 安装PGPB.3 校验软件B.4 设置时区变量TZ附录C 如何安装PGP UNIX版C.1 展开软件包C.2 编译PGPC.3 安装PGPC.4 清除编译生成文件C.5 修改PGP目录读写权限C.6 校验软件附录D PGP命令及使用参考附录E 参考网址信息

## <<网络信息安全与PGP加密>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>