

<<经典密码学与现代密码学>>

图书基本信息

书名：<<经典密码学与现代密码学>>

13位ISBN编号：9787302107408

10位ISBN编号：7302107408

出版时间：2005-7

出版时间：清华大学出版社

作者：(美)斯皮尔曼

译者：叶阮健 曹英 张长富

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>

<<经典密码学与现代密码学>>

内容概要

《经典密码学与现代密码学》主要从三个方面来介绍密码学的知识：第一部分介绍了经典密码学的经典问题，包括单码加密法、仿射加密法、多码加密法、多图加密法和换位加密法；第二部分介绍了现代密码学，包括流加密法、块加密法和公钥加密法；第三部分介绍了密码学的未来，并对量子加密法进行了简单介绍。

《经典密码学与现代密码学》一个突出的特点是，对密码破解进行了详细描述，使读者既掌握加密的内部算法，又能了解各种加密法的弱点。

与《经典密码学与现代密码学》配套的CAP软件实现了各种加密法，读者可以利用该软件进行加密和解密，从而增强了《经典密码学与现代密码学》的科学性和适用性。

每章末尾还给出了一些复习题，给读者以很大的启发和想象力。

《经典密码学与现代密码学》不仅是一本很好的密码学教材，对密码学研究人员和广大密码学爱好者也都是一本不可多得的参考用书。

<<经典密码学与现代密码学>>

书籍目录

第1章 密码学概论

- 1.0 概述
- 1.1 密码学
- 1.2 重要术语
- 1.3 加密法的评价
- 1.4 密码分析法
- 1.5 编码与加密法的历史简介
- 1.6 经典加密法与现代加密法
- 1.7 CAP软件介绍
- 1.8 本章小结
- 1.9 重要术语

习题

第一部 分经典加密法

第2章 经典单码加密法

- 2.0 概述
- 2.1 关键词加密法
 - 2.1.1 关键词加密法的分析法
 - 2.1.2 频率信息
 - 2.1.3 使用CAP软件破解多关键词加密法
- 2.2 仿射加密法
 - 2.2.1 仿射加密法的加密分析
- 2.3 多文字加密法
 - 2.3.1 多文字加密法的分析
- 2.4 单码加密法的历史简介
- 2.5 本章小结
- 2.6 重要术语

第3章 经典多码加密法

- 3.0 概述
- 3.1 Vigenere加密法
 - 3.1.1 Vigenere加密法分析
 - 3.1.2 用CAP分析Vigenere加密法
- 3.2 自动密钥加密法
 - 3.2.1 自动密钥加密法的分析
- 3.3 Nihilist加密法
- 3.4 圆柱面加密法
 - 3.4.1 Bazeriers圆柱面加密法的分析
- 3.5 回转轮加密法
 - 3.5.1 Enigma加密法的破解
 - 3.5.2 使用CAP软件破解回转轮加密法
- 3.6 加密机的历史简介
- 3.7 本章小结
- 3.8 重要术语

习题

第4章 经典多图密法

- 4.0 概述

<<经典密码学与现代密码学>>

4.1 Playfair加密法

4.1.1 Playfair加密法分析

4.1.2 用CAP软件分析Playfair加密法

4.2 Hill加密法

4.2.1 在CAP软件中实现Hill加密法

4.2.2 Hill加密法分析

4.3 Beale加密法的历史简介

4.4 本章小结

4.5 重要术语

习题

第5章 经典换位加密法

5.0 概述

5.1 置换加密法

5.1.1 置换加密法分析

5.2 列置换加密法

5.2.1 列换位加密法分析

5.2.2 使用CAP软件来破解列换位加密法

5.3 双重换位加密法

5.3.1 双重换位加密法分析

5.3.2 使用CAP软件破解双重换位加密法

5.4 换位加密法的历史简介

5.5 本章小结

5.6 重要术语

习题

第二部分 现代加密法

第6章 流加密法

第7章 块加密法

第8章 公钥加密法

第9章 密钥管理、数字签名、散列函数与证书

第三部 分密码学的未来

第10章 量子密码学

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>