

《古今密码学趣谈》

图书基本信息

书名：《古今密码学趣谈》

13位ISBN编号：9787121185595

10位ISBN编号：7121185598

出版时间：2012-10-1

出版社：电子工业出版社

作者：王善平

页数：175

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《古今密码学趣谈》

前言

人类历史有记录就有密码使用的记载。随着社会信息化的迅猛发展，人们越来越认识到密码在保障信息安全中发挥着不可替代的作用，世界各国均非常重视和支持密码学研究，并得到了社会力量的积极响应，这些因素推动着密码产业迅速发展。目前，密码和密码产品已经被越来越多的人认识，并得到了越来越广泛的应用。为积极落实《全民科学素质行动计划纲要》，大力普及密码学知识，提升我国公民的信息安全保护和防范意识，以及提高公民的科学素养，特别是激发广大青少年对密码学的兴趣，吸引他们投身于我国密码事业，中国密码学会组织编写了这本科普图书《古今密码学趣谈》。今年，在北京市科协科普创作出版专项计划的大力支持下，本书得以公开出版。本书由华东师范大学王善平教授编写，书中依据详实的资料，通俗的语言描绘了古今密码学发展的概貌，对所涉及的密码学基本原理和关键知识给予准确而清晰的阐述，同时介绍了密码在信息时代发挥的巨大作用，并展望了密码学的未来发展。在本书的编写过程中，西南交通大学何大可教授与中国地质大学（武汉）任伟副教授分别对初稿进行了审读，并提出了很好的修改意见，武汉大学张焕国教授与上海交通大学来学嘉教授、华中科技大学胡汉平教授等完成了本书第七章的撰写。

《古今密码学趣谈》

内容概要

本书是中国密码学会组织编写的密码学科普读物。书中依据翔实的资料，梳理了密码学发展脉络，回顾了密码史上的诸多重大事件，着重讲述两次世界大战时期惊心动魄的密码战，介绍了现代密码学及其在信息时代的广泛应用，展望了密码学的未来发展。同时，深入浅出地解释了古代和现代密码学的基本原理，并结合生活中的事例说明什么是密码和密码学。

本书适合中学及以上文化程度的密码爱好者阅读，还可作为密码工作者和密码专业学生的参考书。

《古今密码学趣谈》

作者简介

中国密码学会是中国科协领导下的国家一级学会，是由密码学及相关领域的科技工作者和单位自愿结成并依法登记的全国性、学术性、非营利性的法人社会团体，成立于2007年3月25日。

目前学会已成立了学术工作委员会、组织工作委员会、教育工作委员会，量子密码专业委员会、密码数学理论专业委员会、密码算法专业委员会、密码芯片专业委员会等七个分支机构。

《古今密码学趣谈》

书籍目录

写在前面的话——什么是密码学.....	1
第1章 密码学前史——古代保密通信和身份认证方法.....	9
1.1 最古老的密码学.....	9
1.2 古代中国军队的保密通信和身份认证方法.....	11
1.3 古代西方军队的保密通信.....	17
1.4 古代阿拉伯人开创密码分析学.....	19
1.5 中世纪后西方传统密码学的发展.....	20
第2章 第一次世界大战中的密码故事——密码学进入电子通信时代.....	27
2.1 英国海军部的“40号房间”.....	28
2.2 破解齐默尔曼密电.....	30
2.3 “美国黑室”——传奇密码专家雅德利的故事.....	31
第3章 传统密码学的基本知识.....	39
3.1 换位加密法.....	39
3.2 替换加密法.....	41
3.3 形形色色的隐写技术.....	43
第4章 第二次世界大战中的密码故事——机器密码时代.....	47
4.1 “超级情报”扭转战争局面.....	48
4.2 德国“隐谜”密码机的出现.....	52
4.3 波兰数学家首次破解“隐谜”密码机.....	57
4.4 英国布雷契莱庄园的故事.....	68
4.5 美国的密码战故事.....	84
4.6 中国抗日战争时期的密码战.....	93
第5章 信息时代的密码学.....	103
5.1 DES和AES数据加密方法.....	104
5.2 密码学的新方向.....	115
5.3 RSA和ECC公钥密码方案.....	121
5.4 现代密码学的若干基本知识.....	128
第6章 密码学在信息时代的应用.....	139
6.1 数字证书——可信的“网络身份证”.....	139
6.2 第二代居民身份证中的密码技术.....	143
6.3 密码在金融社保卡中的应用.....	144
6.4 网上银行与密码.....	147
6.5 金税工程防伪税控系统.....	152
6.6 密码技术在用户用电信息采集系统中的应用.....	154
6.7 云计算中的密码应用.....	159
第7章 展望未来的密码学.....	163
7.1 量子计算机对现代密码学的挑战.....	164
7.2 量子密码.....	168
7.3 生物密码.....	170
7.4 混沌密码.....	172
7.5 结束语.....	175
参考文献.....	177

3.与英印合作侦译日本空军情报 第二次世界大战时期的日本空军是隶属于海军和陆军的一个军种，所以其使用的密码也是日本三军中最简单的。而且由于他们轻视中国的技术能力，在这里甚至仅使用换位密码，不加任何随机数覆盖，从而给中国的军委技术研究室带来了破解的便利。 相比之下，日本陆军和海军使用的密码要复杂得多，几乎没有被中国人破解过。 1939年，重庆国民党当局曾得到八路军所缴获并送来日本陆军的三本密码手册，体现了当时的国共合作精神，遗憾的是依然无法破解日本陆军密码。 但是对于日本空军，中国的密码战士不仅能破解其密码，而且能熟练地进行通信分析：通过监听并分析其通信方向、流量、发报地点和手法等，获得了宝贵的军事情报。这些情报不仅为中国城市的防空做出了重要贡献，而且为中国空军和美国援华航空队（即飞虎队）的作战提供了很大的帮助。《中日航空大决战》的作者罗纳德·海华斯在书中说道：“这种情报的价值太大了。陈纳德（Claire Lee Chennault，美飞虎队队长）知道日军飞机朝哪个方向飞去以及它们的目标。因而能够以弱小的兵力与日军周旋。虽然飞虎队只是一个不足100架飞机的小部队，却与超过500架飞机的日军战斗数月。” 以下是对日空军密码战的一些资料。 1941年10月下旬，蒋介石“技研室”新成立的成都侦译工作队，监听发现日本空军通信突然十分繁忙，结合其他情况判断，侵华空军在大调动，纷纷飞离中国。一周后，通信趋于沉寂，大部分监听对象已消失，遂扩大监听范围，终于在日本空军偷袭美国珍珠港的第二天，监听到原来在中国的那些日本飞机参与攻击行动的信号。从而在第一时间，获悉珍珠港事件。 ……

精彩短评

- 1、可惜我不是很懂。
- 2、还没仔细看，大致浏览一下，还可以。
- 3、我喜欢的内容
- 4、内容非常好！！！！！！
- 5、没有提到playfair密码
- 6、外行人入门读物学到不少的知识 不错的科普文
- 7、很好的一本书。把很枯燥的知识写的很有趣，连我儿子都喜欢看。
- 8、一共买了2本书，还分开2个订单，一个北京发货，一个广州发货~慢慢学习看吧，就想增加一点关于密码方面的知识
- 9、我觉得看起来有些深奥，因该更适合专业人士阅读！
- 10、孩子正在看，说还蛮好看的
- 11、前面还成 虽然我一贯可以从垃圾堆里检出东西 但是实在忍不住要吐槽应用那章 尤其是二代身份证的那个文章 实在太标题党了 成功地做到了 写满文本却无任何信息传递
- 12、不错，值得一读。开眼界了。
- 13、有趣味，可以科普一下
- 14、首先看来了一下目录，蛮感兴趣的，没看完，具体内容就不给评价，但是现阶段还是觉得不错
- 15、通过一个个故事让我了解了密码的小故事，不错！
- 16、感觉挺好玩的，能够了解这方面的知识
- 17、内容非常吸引人，爱不释手。普及了密码学的一些知识，个人感觉要是现代密码学方面介绍的更详细一点就好了。当然有兴趣的可以去看更详细的专著。
- 18、不是很有趣，有点像教科书。
- 19、平时不怎么接触这个范畴，除需要设置密码，真是不看不知道
- 20、看了《暗算》，再看这书，挺有意思的
- 21、当闲书看了，还能学知识
- 22、密码初步认识，开发智力的好书
- 23、介绍密码学的书，还不错
- 24、书的质量红啊，内容也是很吸引人
- 25、好多小知识你不知道的
- 26、我是一口气看完的，虽然对其中设计数学的术语和定理不懂，但完全不影响我的阅读，很有趣，读完能了解许多密码的知识和小故事。
- 27、这本是儿子给我开的书单里的书，老实话，小学生看前面的还挺有意思，后面涉及的数学应该就看不懂了，不过慢慢研究着看吧，或许可以燃起对数学的热情呢。
- 28、和我想象中的差远了，不是我想要的那种类型.....
- 29、喜欢很好看，中央4台的读书节目介绍的主持人是绍刚，就买来看看挺好看的
- 30、适合入门级密码学者阅读，是一本基础书。
- 31、非常喜欢这本书，内容丰富，容易理解。很棒！
- 32、二战密码机攻防战一段很精彩 费曼在自传里提到过
- 33、数学不好，有些专业的部分看不懂。。。
- 34、昨天傍晚定的，今天中午就收到书，非常及时，非常满意。书很好，要很好研读一番。
- 35、通过故事的形式了解、学习密码。
- 36、这是一本由中国密码学会组编的书，内容通俗易懂。
- 37、胶装不好，书页都好掉了.....
- 38、密码学历史，从古代到密码学鼎盛时期，也就是战争时期的密码发展史。
- 39、专业性比较强的讲古书籍。
- 40、硬度有点大，不少内容就是跟着演算也弄不懂。
- 41、这是一本科普好书。深入浅出。
- 42、努力做个杂家，读书增长见识。

《古今密码学趣谈》

- 43、从古到今带你了解密码学的历史，由浅入深领你进入密码学的世界。
- 44、内容很有趣，也很系统，适合密码学入门
- 45、儿子和他的同学都很喜欢这本书。
- 46、正在学习中，开头的小插曲很有意思。。。。。

章节试读

1、《古今密码学趣谈》的笔记-

key

《古今密码学趣谈》

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：www.tushu111.com