<<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

出版时间：电子工业出版社

作者：王善平

页数：178

字数：258000

<<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。

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

章节摘录

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附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。
相比较之下，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。
……

版权说明