《密码编码和密码分析原理与方法》

图书基本信息

书名：《密码编码和密码分析原理与方法》

13位ISBN编号：9787111090847

10位ISBN编号：7111090845

出版时间：2001-9-1

出版社：机械工业出版社

作者：F.L.Bauer

页数：400

《密码编码和密码分析原理与方法》

内容概要

本书介绍密码编码学和密码分析方法，对破译密码的方法提出了许多建议。本书从密码学的历史中摘录了大量史料，内容丰富，叙述生动，不仅适合密码学研究人员和网络安全技术人员参考，也适合想了解密码学的普通读者阅读。

《密码编码和密码分析原理与方法》

书籍目录

《密码编码和密码分析原理与方法》

精彩短评

1、被拙劣翻译毁掉的一本好书
2、密码学还是古典的有意思，古典密码学中文版里还是这本最好
3、垃圾翻译……
4、译得很差
5、相当好的入门教材，我我我略懂，当然主要是看结构。看结合的事件与发展脉络。高数部分忽略，数理统计的部分了解逻辑而已。

《密码编码和密码分析原理与方法》

精彩书评

1、我是一个不喜欢在书本上写写画画的人；我很自豪，看过数遍的书，可以保持得像新书一样；但是，这本书里面，充满了我用红笔做出的批注……古典密码体系中，表格是极为常见的；在这个译本中，表格排版错误也不罕见；还好，对表格认真分析后，我用红笔改过来。加密、脱密往往是以字母为基础的；在这个译本中，写错字母是稀松平常的；还好，认真核对加密、脱密过程后，我用红笔改过来。欧洲数百年密码斗争中最重要的三种语言：英语、法语、德语；译者对后两者完全不懂，而原样照抄又错、漏连连；谢天谢地，德语、法语我都学过，用红笔一一改过来。但是，像我这样NB，既看得懂英、法、德三种语言，又能找出译文中技术性错误的人，有多少呢？其他买了这本书的读者，多么令人同情啊！！！x_x至于译者的英语功底么……来看看下面这段话：“ Enigma-D型商用密码机……，它可以通过波兰Biuro Szyfrow合法购买 ”。等等！这个Biuro Szyfrow是啥？波兰总参谋部密码处！Marian Rejewski的老东家，最先攻破Enigma的地方！Enigma的故事，对密码分析大凡有点儿了解的人，早已烂熟于胸了。但是本书的译者，即使是在他们译完整本书之后，估计仍旧是稀里糊涂的。这么一伙儿人翻译出来的东西，有没有其它类似的驴唇不对马嘴的错译，谁能知道？这一处问题被我发现了，让我如何相信，其它那些看上去颇为可疑的文字，是因为我的理解能力有问题，而不是译者在胡说八道？译者们自称来自“ 中国信息安全产品测评认证中心 ”，不过，恕我直言，从译文中的种种迹象判断，他们对于密码学、密码分析的原理和历史缺乏最基本的了解。能力决定成败，抑或态度决定一切？这个问题，咱们不去争论，俺只知道，当一群能力不足而态度又很不认真的人，动手翻译他们自己几乎不了解的一本书，对于读者来说，就是一场灾难。

《密码编码和密码分析原理与方法》

版权说明