

现代密码分析学

—— 破译高级密码的技术

MODERN CRYPTANALYSIS
TECHNIQUES FOR
ADVANCED
CODE BREAKING

(美) Christopher Swenson 著
黄月江 祝世雄 等 译
张文政 校



国防工业出版社
National Defense Industry Press

 WILEY

装备科技译著出版基金资助

现代密码分析学 ——破译高级密码的技术

Modern Cryptanalysis
Techniques for Advanced Code Breaking

(美) Christopher Swenson 著

黄月江 祝世雄 等译

张西政 校

WILEY

Wiley Publishing, Inc.



国防工业出版社·北京·

National Defense Industry Press

著作权合同登记 图字：军-2012-010 号

图书在版编目(CIP)数据

现代密码分析学：破译高级密码的技术 / (美)斯文森(Swenson, C.)著；黄月江，祝世雄译. —北京：国防工业出版社，2012.11

书名原文：Modern Cryptanalysis: Techniques for Advanced Code Breaking

ISBN 978-7-118-08132-9

I. ①现... II. ①斯... ②黄... ③祝... III. ①密码术
IV. ①TN918.3

中国版本图书馆 CIP 数据核字(2012)第 231314 号

Translation from the English Language edition:

MODERN CRYPTANALYSIS: TECHNIQUES FOR ADVANCED CODE
BREAKING by Christopher Swenson

ISBN 978-0-470-13593-8

© 2008 Wiley Publishing, Inc.

10475 Crosspoint Boulevard

Indianapolis, IN 46256

All rights reserved. This translation published under License.

本书简体中文版由 Wiley Publishing, Inc. 授权国防工业出版社独家出版发行。
版权所有，侵权必究。

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×960 1/16 印张 14 1/4 字数 243 千字

2012 年 11 月第 1 版第 1 次印刷 印数 1—2000 册 定价 60.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777

发行邮购：(010)88540776

发行传真：(010)88540755

发行业务：(010)88540717

现代密码分析学

——破译高级密码的技术

威利出版公司出版

印第安纳波利斯, IN46256,

克拉斯颇因特大街 10475 号

版权 2008, 由克里斯托弗·斯文森拥有

由美国印第安纳州印第安纳波利斯市威利出版公司与加拿大联合发行

ISBN: 978 - 0 - 470 - 13593 - 8

于美国印刷(制作)

10 9 8 7 6 5 4 3 2 1

没有出版者提前的书面允许,或者,没有向丹弗斯城(MA01923)罗斯物德大道 222 号的版权许可中心((978)750 - 8400, 传真(978)646 - 8600)支付适当的每册复制费而得到授权,本书的任何部分都不能以任意形式、任何手段(包括电子的,机械的,照相复制的,录音的,扫描的手段或其他手段)复制,存储在检索系统或传输,除非得到 1976 美国版权条例第 107 款或 108 款的许可。要出版同意的请求应送给印第安纳波利斯市(IN46256)克拉斯颇因特大街 10475 号的威利出版公司法律部((317)572 - 3447, (317)572 - 4355)或联线 <http://www.wiley.com/go/permissions>.

责任限定/放弃保证:就本书内容的准确性和完整性,出版者与作者不作任何描述或保证,特别放弃所有保证,包括不(限定)保证本书对特殊目的适应性。不能通过销售材料或促销材料作保证。这里包含的忠告和策略不会对每一种情况都适合。卖本书的前提条件是出版者不提供法律的、财务的或其他的专业服务。如果需要专业帮助,应寻求有能力的专业人员。出版者和作者都不会对由

此引起的损失负责。在本书中,将一个组织或网站作为进一步信息的引用和/或进一步信息的潜在来源这一事实并不意味着作者或出版者对组织或网站可能提供的信息作保证或者对它(们)可能作的推荐作保证。另外,读者应当意识到在写本书和读本书的时候,本书中列出的互联网网站可能已经变化或消失。

为了得到有关我们其他作品和服务的一般信息或为了得到技术支持,请在美国国内通过(800)762-2974 和我们的顾客管理部联系,在美国之外通过(317)572-3993 或传真(317)572-4002 和我们的顾客管理部联系。

从出版者那里可得国会图书馆出版目录分类数据。

商标: 威利(Wiley), 威利标志及相关的(商业)形式是约翰·威利与桑斯公司(John Wiley & Sons Inc.) 和/或它在美国和其他国家的分支机构的商标或注册商标,没有书面允许,不能使用它们。所有其他商标分别是它们拥有者的财产。威利出版公司不与本书提到的任何作品或卖主发生联系。

威利还以各种电子形式出版书籍。不许以电子版的形式获取某些印出来的内容。

本书表达的观点和意见并不反映美国国防部的观点与意见。

译者序

在信息社会里,无论国家、单位还是个人都越来越认识到信息安全的重要性,而密码学是信息安全的基础,几乎所有的信息系统都使用了密码技术。对一个使用了密码技术的系统来说,首先要保证系统的安全性,即所使用的密码体制是安全的;其次,对一个加了密的“敌对”系统,应想方设法地去破译该系统,破译该系统的核心最终都归结到密码体制的破译,所以掌握常见的密码体制的破译方法,对设计和破译密码算法是非常必要的。目前国内、外已有很多介绍密码学的书籍,但密码破译分析学方面的专著甚少。本书的作者 Christopher Swenson 博士在密码分析方面做出了出色的研究成果,曾获得由国际密码研究协会(IACR)和美国数学学会(AMS)共同颁发的信息安全学术成就奖。Christopher Swenson 博士在本书中全面、系统地介绍了密码分析学,有助于我们学习国外最新的密码分析技术,了解我们与国际先进水平之间的差距,推动我国密码分析技术的发展。

本书有如下特点:

1. 内容丰富。全面地介绍了古典密码、公钥密钥和分组密码的分析方法,并将这些方法应用于当前流行的密码算法的分析。
2. 自成体系。给出了学习这些分析方法所必需的数学知识,并用有趣的例子去帮助读者进行理解。习题的良好设计也能使读者更深入地体会所讲述的方法。
3. 理论前沿。不仅总结了通用的分析方法,而且还介绍了许多最新的分析技术,如差分分析及其变型、线性分析和飞去来器攻击等。

本书还系统、全面地介绍了密码分析学领域的重要参考文献,是一本可读性强和详细描述当代密码分析学现状的著作。本书的出版,希望能对国内从事信息安全和密码分析的同行们提供借鉴和帮助,也可作为信息安全专业的研究生以及相关专业的大学高年级本科生全面学习密码分析理论的基础性书籍,可供从事密码设计和破译工作的科研人员参考。

全书由中国电子科技集团公司第三十研究所和保密通信重点实验室共同翻译完成,国防工业出版社王晓光编审为本书的顺利出版给予了悉心指导和辛苦努力。以下人员参与了出版、翻译和审校工作:黄月江、祝世雄、张文政、曾兵、霍家佳、譙通旭、赵伟、王林、于飞、张李军、周宇、董新锋、范佳、周文、张雅念、张晓玉等,在此对他们辛勤的工作表示衷心的感谢!

由于译者水平有限,书中难免会有一些错误和不当之处,欢迎读者批评指正!

译者
2012年4月

作者简介

克里斯托弗·斯文森(邮箱: www.caswenson.com) 现正在塔尔萨大学攻读计算机科学博士学位,而且他还在该校协助并教授信息安全课程、电信学课程和密码分析课程。他是积极的研究者并已发表了多篇安全领域的论文。他获得了信息保障奖学金,该项目即国防部赛博部队项目。

原书编辑人员

执行编辑

卡罗尔·朗

副社长兼执行集团出版者

理查德·斯瓦德利

开发编辑

约翰·斯里维尔

副社长兼执行出版者

约瑟夫 B. 维克特

制作编辑

迪部尔·班利杰尔

设计协调人,封面

林瑟·斯坦福

复制编辑

卡特·卡夫瑞

校对人员

南希·卡南斯科

编辑经理

玛丽·贝斯·瓦克菲尔德

编索引人员

莫兰尼·贝尔金

制作经理

蒂姆·塔特

封面图像

©雅玛达·塔罗/数字影像/

盖特图像

致 谢

我感谢帮助我出版本书的许多人士。首先,感谢我的未婚妻瑟斯德·布拉姆,她在本书的写作过程中一直支持我。我要感谢苏吉特·舍诺依和塔尔萨大学,他们为我提供场地以便教授原创性课程(还要感谢学习该课程的所有学生)。当然,我要感谢我的母亲格冷达和我的父亲罗杰,以及我的姐妹瑞克和杰西,还有我的继父理查德,他们这么多年来一直支持我。

没有威利出版公司的卡罗尔·朗和约翰·斯里维尔的支持我不可能写出本书。还要非常感谢唐纳德·克鲁斯,莱斯利·南颇特和约翰·霍比,以及数以百计的人员,他们在 TeX、LaTeX、MetaPost 和相关的排字项目上付出了努力。

目 录

引言	1
参考文献	8
第1章 古典密码	9
1.1 单表密码	9
1.2 使用密钥	11
1.2.1 密钥表	12
1.2.2 ROT13	12
1.2.3 Klingon	13
1.3 多表密码	13
1.3.1 维吉尼亚表	14
1.4 变换密码	15
1.4.1 列变换	16
1.4.2 双列变换	16
1.5 密码分析学	17
1.5.1 单表密码的破解	17
1.5.2 多表密码的破译	21
1.5.3 列变换密码的破译	23
1.5.4 双列变换密码的破译	26
1.6 小结	27
练习	27
参考文献	28
第2章 数论密码	29
2.1 概率论	29
2.1.1 排列和组合选择	30
2.1.2 相关性	31
2.1.3 生日悖论	36
2.1.4 密码学上的哈希算法	39

2.2	数论基础复习	41
2.2.1	整除和素数	41
2.2.2	同余	42
2.3	代数基础复习	44
2.3.1	一些定义	45
2.3.2	有限域上的求逆	47
2.4	基于因子分解的密码学	49
2.4.1	RSA 算法	49
2.5	基于离散对数的密码学	51
2.5.1	Diffie Hellman 算法	51
2.6	椭圆曲线	52
2.6.1	点加	53
2.6.2	椭圆曲线密码学	57
2.6.3	椭圆曲线版本的 Diffie - Hellman 协议	58
2.7	小结	58
	习题	58
	参考文献	59
第 3 章	整数分解和离散对数	60
3.1	整数分解	60
3.2	算法理论	61
3.2.1	记号	62
3.2.2	Python 速成课程	63
3.3	指数级分解方法	65
3.3.1	穷举攻击算法	66
3.3.2	Fermat 平方差	68
3.3.3	Pollard 的 ρ 方法	70
3.3.4	Pollard 的 $p-1$ 方法	72
3.3.5	二次型分解算法	73
3.3.6	椭圆曲线分解方法	74
3.4	亚指数分解方法	75
3.4.1	连分数分解算法	75
3.4.2	筛法	77
3.5	离散对数	77
3.5.1	穷举攻击方法	78

3.5.2	大步小步法	79
3.5.3	离散对数的 Pollard p 算法	80
3.5.4	离散对数的 Pollard λ 算法	81
3.5.5	指示演算法	82
3.6	小结	83
练习		83
参考文献		84
第4章	分组密码	86
4.1	基于比特、字节、字的运算	86
4.1.1	运算	88
4.1.2	代码	89
4.2	乘积密码	90
4.3	替换和置换	90
4.3.1	S 盒	90
4.3.2	P 盒	92
4.3.3	移位寄存器	93
4.4	替换—置换网络	94
4.4.1	EASY1 密码	95
4.5	Feistel 结构	100
4.6	DES	102
4.6.1	DES 密钥编制	103
4.6.2	DES 轮函数	104
4.6.3	三重 DES	105
4.6.4	DESX	105
4.7	FEAL	106
4.7.1	S 函数	107
4.7.2	密钥生成函数 f_K	108
4.7.3	轮函数 f	109
4.7.4	密钥编制	111
4.8	Blowfish	112
4.8.1	Blowfish 的密钥编制算法	112
4.8.2	Blowfish 算法	113
4.8.3	轮函数	114
4.8.4	注释	114

4.9	AES/Rijndael	114
4.9.1	Rijndael 加密算法	115
4.9.2	Rijndael 解密算法	119
4.9.3	密钥扩展	120
4.9.4	对 Rijndael 的注记	121
4.10	分组密码模式	121
4.10.1	电子密码本	121
4.10.2	密文分组链接	122
4.10.3	密文反馈	123
4.10.4	输出反馈	124
4.10.5	计数模式	125
4.11	Skipjack	125
4.11.1	Skipjack 加密算法	125
4.11.2	Skipjack 解密算法	126
4.11.3	置换	127
4.12	消息摘要和哈希	128
4.12.1	校验和	129
4.12.2	循环冗余码校验	129
4.12.3	MD5	130
4.12.4	SHA-1	131
4.13	随机数生成器	132
4.13.1	偏差	133
4.13.2	线性同余随机数生成器	133
4.14	一次一密码本	134
4.15	小结	135
	练习	136
	参考文献	136
第5章	通用的分析方法	138
5.1	穷举攻击	138
5.2	时间—空间折中攻击	139
5.2.1	中间相遇攻击	140
5.2.2	Hellman 时间—空间折中	141
5.2.3	时间—空间折中的成效	142
5.2.4	缺点	143

5.2.5 多表折中	143
5.2.6 Rivest 的特异终点	144
5.3 彩虹链表	144
5.3.1 彩虹链表的优点	145
5.3.2 微软局域网管理器口令哈希	145
5.4 滑动攻击	146
5.4.1 Feistel 密码的滑动攻击	147
5.4.2 高级滑动攻击	148
5.5 哈希函数分析	149
5.6 随机数生成器分析	150
5.7 小结	151
练习	152
参考文献	152
第 6 章 线性分析	154
6.1 概述	154
6.2 Matsui 算法	156
6.3 S 盒的线性逼近	157
6.4 Matsui 堆积引理	161
6.5 EASY1 密码	162
6.6 线性逼近和密钥恢复	165
6.7 DES 的线性分析	168
6.8 多重线性逼近	169
6.9 寻找线性逼近	170
6.10 线性分析程序代码	172
6.11 小结	177
练习	177
参考文献	178
第 7 章 差分密码分析	179
7.1 概述	179
7.2 记号	179
7.3 S 盒的差分	180
7.4 组合 S 盒的特征	183
7.5 获得密钥	184
7.6 差分密码分析的程序代码	185

7.7 Feistel 密码的差分密码分析	189
7.7.1 FEAL 的差分密码分析	190
7.7.2 DES 的差分密码分析	190
7.8 分析	193
7.9 差分—线性密码分析	193
7.10 条件特征	195
7.11 高阶差分	196
7.12 截断差分	197
7.13 不可能差分	199
7.14 飞去来器攻击	201
7.15 插值攻击	203
7.16 相关密钥攻击	204
7.16.1 GOST 的相关密钥攻击	205
7.16.2 3DES 的相关密钥攻击	205
7.17 小结	206
练习	207
参考文献	207

引 言

正如许多事情一样,在密码分析学领域没有一本教科书介绍现代密码学的进展,本书对这个问题给出了回答。密码分析学在最近的数百年中已经得到了长足的发展,人们对密码分析学进行了广泛的研究并得到了大量成果。

然而,当我们进入 20 世纪后,这些密码分析学的书籍和资料变得相对滞后。每一本“密码分析学”方面的书几乎都是 100 年以前的,按今天的标准,这些书主要关注某些最简单密码的破译。

相反,这个领域本身并没有停止发展,特别是在刚刚过去的 30 年里,随着日益强大的计算机的出现,它得到了难以置信的快速研究。在世界范围内,在密码分析学方面举办了各种会议和出版了许多论文,但没有人去考虑借助一种简单的方式来让人们去从头开始学习密码分析学。Bruce Schneier 在文献[5]中已经指出这种方式是不值得的,因为这个领域变化得太快了,他的话极有道理。但是,当前密码分析学上的方法都是建立在相同的基础上的,并且大多数背景资料都需要懂得当前的研究情况或者参与到其中,这些将使学习变得越来越庞大和复杂。更重要的是,一些重要的论文都是由不同的人群和出于不同的个人目的而写的,这些使得人们理解起来更困难。

但我必须重申 Schneier 在文献[5]中说过的话:仅仅有一种方式能使得人们成为一个好的密码分析专家——练习破译密码。然而,我希望这本书能使新的或熟练的密码分析学家全面了解许多密码分析方面的成果。

当我在塔尔萨大学教学时,许多同学对密码分析学表现出了极大的兴趣,他们知道我喜欢该领域。我开始准备这门课,尽管我使用的是参考文献[7],但是我还是发现没有一本我真正想要的教科书。

为此我开始从各种会议和出版物中收集各种材料,而且为学生整理上课中的各种笔记和摘要。同时我意识到也许有其他几个人与我有同样的问题:在较少的理论基础上想自学这个学科,甚至教学和上课。我们希望有这些人,否则将使我的出版商对推销这本书非常失望。

为了适当地讲现在密码分析学,我们不得不先做一些其他的事:最重要的是商定要做的和为什么要去做,这些就是引言中要介绍的。尽管我会把更有力的