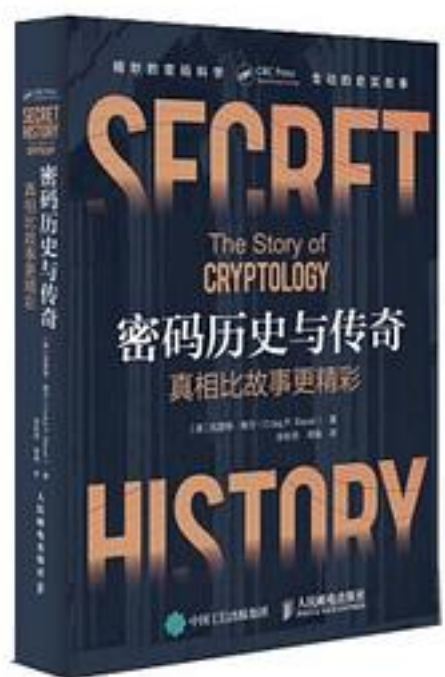


密码历史与传奇



[密码历史与传奇 下载链接1](#)

著者:[美] 克雷格·鲍尔 (Craig P.Bauer)

出版者:人民邮电出版社

出版时间:2019-4-1

装帧:精装

isbn:9787115493965

密码历史与传奇适合对密码学感兴趣的大众读者阅读，也适合大学相关专业将之作为课程教材使用，尤其适合大学教师将其作为教学参考书使用。

密码历史与传奇

以通俗易懂的方式讲述了密码学的历史和密码算法，并生动地介绍了密码学的一些应用实例。本书通过许多案例故事将原本非常专业的内容讲述得生动有趣，因此，即使你没有数学或密码学的知识基础，也可以阅读本书。同时，作者在写作本书时整理和引用了大量的首次公开发表的珍贵资料，使密码学专业人士也能够从书中获得新知识和新资料。

作者介绍:

译者, 徐秋亮, 教授, 博士, 博士生导师。1960年4月出生。现为山东大学计算机科学与技术学院副院长。长期从事信息安全、密码学等领域的理论研究工作, 研究领域涉及公钥密码、数字签名、密钥管理、访问控制、信息安全系统体系结构等信息安全核心理论与技术, 并在椭圆曲线密码学、门限密码学、数字签名等领域做出特色。

目录: 第一部分 古典密码学

第1章 古代根源 3

1. 1 穴居人密码 3

1. 2 希腊密码学 4

1. 2. 1 密码棒密码 4

1. 2. 2 波利比奥斯密码 5

1. 3 维京密码 6

1. 4 早期隐写术 7

参考文献和进阶阅读 8

第2章 单表代换密码或MASC: 消息的伪装 10

2. 1 凯撒密码 10

2. 2 其他单表代换密码系统 11

2. 3 埃德加·爱伦·坡 14

2. 4 亚瑟·柯南·道尔 18

2. 5 频数分析 21

2. 6 圣经密码学 22

2. 7 更多的频数和模式词 23

2. 8 元音识别算法 27

2. 8. 1 苏霍京方法 27

2. 9 更多的单表代换密码 30

2. 10 单表代换密码的密码分析 33

2. 11 杀手和作曲家的未被破译的密码 35

2. 12 仿射密码 37

2. 13 摩尔斯电码和霍夫曼编码 42

2. 14 单表代换密码杂记 46

2. 15 名字手册 47

2. 16 名字手册的密码分析 49

2. 17 图书密码 52

参考文献和进阶阅读 54

第3章 进展到一个不可破译的密码 61

3. 1 维吉尼亚密码 61

3. 2 维吉尼亚密码的发展史 63

3. 3 维吉尼亚密码分析 67

3. 4 克里普托斯 76

3. 5 自动密钥 80

3. 6 运动密钥密码系统及其分析 81

3. 7 一次一密或维尔南密码 93

3. 8 破解不可破译的密码 97

3. 9 伪随机性 99

3. 10 自1915年以来未解密的密码 101

3. 11 OTPs和SOE 102

3. 12 历史重写 102

参考文献和进阶阅读 104

第4章 换位密码 108

4. 1 简单的重排和列换位	108
4. 1. 1 栅栏换位	108
4. 1. 2 矩形换位	109
4. 1. 3 更多换位路径	111
4. 2 列换位密码的分析	112
4. 3 历史应用	117
4. 4 易位构词	118
4. 5 两重换位	120
4. 6 词换位	122
4. 6. 1 再会美国内战密文	124
4. 7 换位装置	124
参考文献和进阶阅读	128
第5章 莎士比亚、杰斐逊和约翰·F·肯尼迪	130
5. 1 莎士比亚V. S. 培根	130
5. 2 托马斯·杰斐逊：总统、密码学家	135
5. 3 密码轮密码的分析	137
5. 4 波雷费密码	148
5. 5 波雷费密码分析	153
5. 5. 1 计算机密码分析	157
5. 6 柯克霍夫原则	158
参考文献和进阶阅读	159
第6章 第一次世界大战和赫伯特·O·亚德里	164
6. 1 齐默尔曼电报	164
6. 2 ADFGX：一种新的密码	167
6. 3 ADFGX的密码分析	169
6. 4 赫伯特·O·亚德里	184
6. 5 和平时期的胜利和一本回忆录	187
6. 6 收缴手稿事件	189
6. 7 再次通过小说发财	190
6. 8 赫伯特·O·亚德里是叛徒吗	192
6. 9 审查制度	193
参考文献和进阶阅读	196
附录	200
第7章 矩阵加密	201
7. 1 莱文和希尔	201
7. 2 矩阵加密的工作过程	202
7. 3 莱文进行的攻击	204
7. 4 鲍尔和米尔华进行的攻击	208
7. 5 故事未完	212
参考文献和进阶阅读	212
第8章 二战：德军的恩尼格玛	216
8. 1 机器的崛起	216
8. 2 恩尼格玛的工作过程	219
8. 3 计算密钥空间	223
8. 4 密码分析第一部分：恢复转轮接线	225
8. 5 密码分析第二部分：恢复出日密钥	241
8. 6 攻破后的故事	245
8. 7 艾伦·图灵与布莱奇利庄园	245
8. 8 洛伦兹密码和巨人计算机	249
8. 9 如果恩尼格玛从未被破解会怎样？	251
8. 10 终点和新起点	252
参考文献和进阶阅读	254
第9章 对日本的密码战	258
9. 1 珍珠港预警	258

9. 2 弗里德曼的团队组建	259
9. 3 对日本外交密码——红密的密码分析	260
9. 3. 1 橙密	264
9. 4 紫密：怎么运行的	265
9. 5 紫密的密码分析	267
9. 6 魔术的实用性	271
9. 7 密码员	273
9. 8 好莱坞的密码员形象	279
9. 9 语言上口头代码的使用	281
参考文献和进阶阅读	281
第二部分 现代密码学	
第10章 克劳德·香农	289
10. 1 关于克劳德·香农	289
10. 2 熵	290
10. 3 进一步讨论	294
10. 4 唯一解	295
10. 5 茫然与困惑	296
参考文献和进阶阅读	297
第11章 美国国家安全局	299
11. 1 美国国家安全局的起源	300
11. 2 瞬变电磁脉冲辐射标准技术	301
11. 3 规模和预算	302
11. 4 自由号和普韦布洛号	304
11. 5 丘奇委员会的调查	306
11. 6 冷战后规模缩小	309
11. 7 一些猜测	310
11. 8 2000年及以后	312
11. 9 NSA面试	313
11. 10 BRUSA、UKUSA以及Echelon	314
参考文献和进阶阅读	316
第12章 数据加密标准	321
12. 1 DES是如何工作的	321
12. 2 对DES的反应和密码分析	330
12. 2. 1 异议1：和密钥大小相关	330
12. 2. 2 异议2：S盒的保密性	333
12. 2. 3 S盒被揭示	334
12. 3 电子前沿基金会和DES	334
12. 4 第二次机会	336
12. 5 有趣的特征	339
12. 5. 1 密码学幽默	340
12. 6 加密模式	341
12. 6. 1 莱文方法	341
12. 6. 2 现代加密模式	342
参考文献和进阶阅读	346
第13章 公钥密码体制的诞生	349
13. 1 美国独立战争时期的密码学家	349
13. 2 迪菲—赫尔曼密钥交换	350
13. 3 RSA：来自麻省理工学院的解决方案	353
13. 3. 1 费马小定理（1640）	354
13. 3. 2 欧几里德算法	356
13. 4 政府对密码学研究的控制	359
13. 5 RSA获得专利，Alice和Bob生而自由	366
参考文献和进阶阅读	368
第14章 攻击RSA	369

14.	1.11种非因数分解攻击	369
14.	1. 1 攻击1: 共模攻击	369
14.	1. 2 攻击2: 中间人攻击	370
14.	1. 3 攻击3: 小解密指数攻击	371
14.	1. 4 攻击4: p或q的部分信息泄露攻击	373
14.	1. 5 攻击5: d的部分信息泄露攻击	373
14.	1. 6 攻击6: 小加密指数攻击	374
14.	1. 7 攻击7: 同加密指数攻击	374
14.	1. 8 攻击8: 搜索消息空间	376
14.	1. 9 攻击9: 适应性选择密文攻击	376
14.	1. 10 攻击10: 时间攻击	377
14.	1. 11 攻击11: 罗纳德是错误的, 怀特是正确的	378
14.	2 因数分解挑战	380
14.	2. 1 古老的问题	381
14.	3 试除法和埃拉托色尼筛法 (约前284—前204)	381
14.	4 费马分解法	384
14.	5 欧拉分解法	385
14.	6 波拉德p-1算法	387
14.	7 狄克逊算法	388
14.	7. 1 二次筛法	393
14.	8 波拉德数域筛法	394
14.	8. 1 其他的方法	395
14.	8. 2 密码学幽默	395
	参考文献和进阶阅读	396
	第15章 素性检测与复杂性理论	399
15.	1 一些关于素数的事实	399
15.	2 费马检测	402
15.	3 米勒—拉宾检测	404
15.	3. 1 产生素数	406
15.	4 确定性素性检测	406
15.	4. 1 AKS 素性检测 (2002)	407
15.	4. 2 GIMPS	409
15.	5 复杂类P与NP、概率性与确定性	410
15.	6 瑞夫·墨克的公钥系统	413
15.	7 背包加密	416
15.	8 盖莫尔 (Elgamal) 加密	419
	参考文献和进阶阅读	421
	第16章 认证性	426
16.	1 来自于第二次世界大战的问题	426
16.	2 数字签名及一些攻击	428
16.	2. 1 攻击12: 选择密文攻击	428
16.	2. 2 攻击13: 针对共模问题的内部因子分解攻击	429
16.	2. 3 攻击14: 内部人员的非因式分解攻击	430
16.	2. 4 Elgamal签名	431
16.	3 散列函数: 提速	431
16.	3. 1 李维斯特的MD5和NIST的SHA-1	432
16.	4 数字签名算法	435
	参考文献和进阶阅读	437
	第17章 良好隐私	439
17.	1 两全其美	439
17.	2 良好隐私的诞生	440
17.	3 齐默尔曼的自述	444
17.	4 实施问题	448
	参考文献和进阶阅读	450

第18章 流密码	451
18. 1 同余发生器	451
18. 2 线性反馈移位寄存器	453
18. 3 LFSR攻击	455
18. 4 手机流密码A5/1	457
18. 5 RC4	458
参考文献和进阶阅读	460
第19章 Suite B全明星算法	464
19. 1 椭圆曲线密码	464
19. 1. 1 Elgamal, ECC版	470
19. 2 ECC的幕后人物	471
19. 3 高级加密标准	473
19. 3. 1 字节代换	475
19. 3. 2 行移位	479
19. 3. 3 列混淆	479
19. 3. 4 轮密钥加	481
19. 3. 5 融会贯通: AES-128如何工作	482
19. 4 AES攻击	482
19. 5 安全专家布鲁斯·施奈尔	483
参考文献和进阶阅读	484
第20章 可能的未来	489
20. 1 量子密码学: 工作原理	489
20. 2 量子密码学: 历史背景	491
20. 3 DNA计算	495
参考文献和进阶阅读	500
索引	505
• • • • •	(收起)

[密码历史与传奇 下载链接1](#)

标签

考据

科普

文化史

密码学

历史

网络生活

2019

文化

评论

[密码历史与传奇 下载链接1](#)

书评

[密码历史与传奇 下载链接1](#)