

《图解密码技术（第3版）》

图书基本信息

书名：《图解密码技术（第3版）》

13位ISBN编号：9787115424918

出版时间：2016-6

作者：[日] 结城浩

页数：424

译者：周自恒

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.tushu000.com

《图解密码技术（第3版）》

内容概要

本书以图配文的形式，详细讲解了6种最重要的密码技术：对称密码、公钥密码、单向散列函数、消息认证码、数字签名和伪随机数生成器。

第1部分讲述了密码技术的历史沿革、对称密码、分组密码模式（包括ECB、CBC、CFB、OFB、CTR）、公钥、混合密码系统。第2部分重点介绍了认证方面的内容，涉及单向散列函数、消息认证码、数字签名、证书等。第3部分讲述了密钥、随机数、PGP、SSL/TLS 以及密码技术在现实生活中的应用。

《图解密码技术（第3版）》

作者简介

作者简介：

结城浩（Hiroshi Yuki）

生于1963年，日本资深技术作家和程序员。在编程语言、设计模式、数学、加密技术等领域，编写了很多深受欢迎的入门书。代表作有《数学女孩》系列、《程序员的数学》等。

作者网站：<http://www.hyuki.com/>

译者简介：

周自恒

IT、编程爱好者，初中时曾在NOI（国家信息学奥赛）天津赛区获一等奖，现就职于某管理咨询公司，任咨询顾问兼战略技术总监。译著有《图解CIO工作指南（第4版）》《大数据的冲击》《代码的未来》《30天自制操作系统》《家用游戏机简史》《有趣的二进制》等。

书籍目录

第1部分 密码	1
第1章 环游密码世界	3
1.1 本章学习的内容	4
1.2 密码	4
1.2.1 Alice与Bob	4
1.2.2 发送者、接收者和窃听者	4
1.2.3 加密与解密	6
1.2.4 密码保证了消息的机密性	7
1.2.5 破译	7
1.3 对称密码与公钥密码	8
1.3.1 密码算法	8
1.3.2 密钥	8
1.3.3 对称密码与公钥密码	9
1.3.4 混合密码系统	10
1.4 其他密码技术	10
1.4.1 单向散列函数	10
1.4.2 消息认证码	10
1.4.3 数字签名	11
1.4.4 伪随机数生成器	11
1.5 密码学家的工具箱	12
1.6 隐写术与数字水印	13
1.7 密码与信息安全常识	14
1.7.1 不要使用保密的密码算法	14
1.7.2 使用低强度的密码比不进行任何加密更危险	15
1.7.3 任何密码总有一天都会被破解	15
1.7.4 密码只是信息安全的一部分	16
1.8 本章小结	16
1.9 小测验的答案	17
第2章 历史上的密码——写一篇别人看不懂的文章	19
2.1 本章学习的内容	20
2.2 恺撒密码	20
2.2.1 什么是恺撒密码	21
2.2.2 恺撒密码的加密	21
2.2.3 恺撒密码的解密	22
2.2.4 用暴力破解来破译密码	23
2.3 简单替换密码	24
2.3.1 什么是简单替换密码	24
2.3.2 简单替换密码的加密	25
2.3.3 简单替换密码的解密	26
2.3.4 简单替换密码的密钥空间	26
2.3.5 用频率分析来破译密码	26
2.4 Enigma	31
2.4.1 什么是Enigma	31
2.4.2 用Enigma进行加密通信	31
2.4.3 Enigma的构造	32
2.4.4 Enigma的加密	34
2.4.5 每日密码与通信密码	36

2.4.6	避免通信错误	36
2.4.7	Enigma的解密	36
2.4.8	Enigma的弱点	38
2.4.9	Enigma的破译	38
2.5	思考	40
2.6	本章小结	41
2.7	小测验的答案	42
第3章 对称密码（共享密钥密码）——用相同的密钥进行加密和解密		45
3.1	炒鸡蛋与对称密码	46
3.2	本章学习的内容	46
3.3	从文字密码到比特序列密码	46
3.3.1	编码	46
3.3.2	XOR	47
3.4	一次性密码本——绝对不会被破译的密码	50
3.4.1	什么是一次性密码本	50
3.4.2	一次性密码本的加密	50
3.4.3	一次性密码本的解密	51
3.4.4	一次性密码本是无法破译的	51
3.4.5	一次性密码本为什么没有被使用	52
3.5	DES	53
3.5.1	什么是DES	53
3.5.2	加密和解密	54
3.5.3	DES的结构（Feistel网络）	54
3.5.4	差分分析与线性分析	60
3.6	三重DES	61
3.6.1	什么是三重DES	61
3.6.2	三重DES的加密	61
3.6.3	三重DES的解密	63
3.6.4	三重DES的现状	64
3.7	AES的选定过程	65
3.7.1	什么是AES	65
3.7.2	AES的选拔过程	65
3.7.3	AES最终候选算法的确定与AES的最终确定	66
3.8	Rijndael	66
3.8.1	什么是Rijndael	66
3.8.2	Rijndael的加密和解密	67
3.8.3	Rijndael的破译	71
3.8.4	应该使用哪种对称密码呢	71
3.9	本章小结	72
3.10	小测验的答案	73
第4章 分组密码的模式——分组密码是如何迭代的		75
4.1	本章学习的内容	76
4.2	分组密码的模式	77
4.2.1	分组密码与流密码	77
4.2.2	什么是模式	77
4.2.3	明文分组与密文分组	78
4.2.4	主动攻击者Mallory	78
4.3	ECB模式	79
4.3.1	什么是ECB模式	79

4.3.2	ECB模式的特点	80
4.3.3	对ECB模式的攻击	80
4.4	CBC模式	82
4.4.1	什么是CBC模式	82
4.4.2	初始化向量	83
4.4.3	CBC模式的特点	84
4.4.4	对CBC模式的攻击	84
4.4.5	填充提示攻击	86
4.4.6	对初始化向量（IV）进行攻击	86
4.4.7	CBC模式的应用实例	86
4.5	CFB模式	88
4.5.1	什么是CFB模式	88
4.5.2	初始化向量	89
4.5.3	CFB模式与流密码	89
4.5.4	CFB模式的解密	90
4.5.5	对CFB模式的攻击	90
4.6	OFB模式	91
4.6.1	什么是OFB模式	91
4.6.2	初始化向量	92
4.6.3	CFB模式与OFB模式的对比	92
4.7	CTR模式	93
4.7.1	计数器的生成方法	95
4.7.2	OFB模式与CTR模式的对比	95
4.7.3	CTR模式的特点	95
4.7.4	错误与机密性	96
4.8	应该使用哪种模式呢	96
4.9	本章小结	97
4.10	小测验的答案	98
第5章	公钥密码——用公钥加密，用私钥解密	101
5.1	投币寄物柜的使用方法	102
5.2	本章学习的内容	102
5.3	密钥配送问题	102
5.3.1	什么是密钥配送问题	102
5.3.2	通过事先共享密钥来解决	104
5.3.3	通过密钥分配中心来解决	105
5.3.4	通过Diffie-Hellman密钥交换来解决密钥配送问题	106
5.3.5	通过公钥密码来解决密钥配送问题	106
5.4	公钥密码	107
5.4.1	什么是公钥密码	107
5.4.2	公钥密码的历史	108
5.4.3	公钥通信的流程	108
5.4.4	各种术语	110
5.4.5	公钥密码无法解决的问题	110
5.5	时钟运算	110
5.5.1	加法	111
5.5.2	减法	113
5.5.3	乘法	114
5.5.4	除法	114
5.5.5	乘方	118

5.5.6	对数	118	
5.5.7	从时钟指针到RSA	119	
5.6	RSA	120	
5.6.1	什么是RSA	120	
5.6.2	RSA加密	120	
5.6.3	RSA解密	121	
5.6.4	生成密钥对	122	
5.6.5	具体实践一下吧	125	
5.7	对RSA的攻击	128	
5.7.1	通过密文来求得明文	128	
5.7.2	通过暴力破解来找出D	128	
5.7.3	通过E和N求出D	129	
5.7.4	中间人攻击	130	
5.7.5	选择密文攻击	132	
5.8	其他公钥密码	133	
5.8.1	ElGamal方式	133	
5.8.2	Rabin方式	133	
5.8.3	椭圆曲线密码	133	
5.9	关于公钥密码的Q&A	133	
5.9.1	公钥密码的机密性	134	
5.9.2	公钥密码与对称密码的密钥长度	134	
5.9.3	对称密码的未来	135	
5.9.4	RSA与质数	135	
5.9.5	RSA与质因数分解	136	
5.9.6	RSA的长度	136	
5.10	本章小结	138	
5.11	小测验的答案	139	
第6章	混合密码系统——用对称密码提高速度，用公钥密码保护会话密钥	141	
6.1	混合动力汽车	142	
6.2	本章学习的内容	142	
6.3	混合密码系统	142	
6.3.1	对称密码与公钥密码	142	
6.3.2	混合密码系统	143	
6.3.3	加密	144	
6.3.4	解密	146	
6.3.5	混合密码系统的具体例子	147	
6.4	怎样才是高强度的混合密码系统	147	
6.4.1	伪随机数生成器	147	
6.4.2	对称密码	148	
6.4.3	公钥密码	148	
6.4.4	密钥长度的平衡	148	
6.5	密码技术的组合	148	
6.6	本章小结	149	
6.7	小测验的答案	150	
第2部分	认证	151	
第7章	单向散列函数——获取消息的“指纹”	153	
7.1	本章学习的内容	154	
7.2	什么是单向散列函数	154	
7.2.1	这个文件是不是真的呢	154	

7.2.2	什么是单向散列函数	157
7.2.3	单向散列函数的性质	159
7.2.4	关于术语	162
7.3	单向散列函数的实际应用	163
7.3.1	检测软件是否被篡改	163
7.3.2	基于口令的加密	165
7.3.3	消息认证码	165
7.3.4	数字签名	165
7.3.5	伪随机数生成器	165
7.3.6	一次性口令	165
7.4	单向散列函数的具体例子	166
7.4.1	MD4、MD5	166
7.4.2	SHA-1、SHA-256、SHA-384、SHA-512	166
7.4.3	RIPMD-160	167
7.4.4	SHA-3	167
7.5	SHA-3的选拔过程	168
7.5.1	什么是SHA-3	168
7.5.2	SHA-3的选拔过程	168
7.5.3	SHA-3最终候选名单的确定与SHA-3的最终确定	168
7.6	Keccak	169
7.6.1	什么是Keccak	169
7.6.2	海绵结构	170
7.6.3	双工结构	171
7.6.4	Keccak的内部状态	172
7.6.5	函数Keccak-f [b]	174
7.6.6	对Keccak的攻击	177
7.6.7	对缩水版Keccak的攻击竞赛	177
7.7	应该使用哪种单向散列函数呢	178
7.8	对单向散列函数的攻击	178
7.8.1	暴力破解（攻击故事1）	178
7.8.2	生日攻击（攻击故事2）	180
7.9	单向散列函数无法解决的问题	182
7.10	本章小结	183
7.11	小测验的答案	184
第8章	消息认证码——消息被正确传送了吗	187
8.1	本章学习的内容	188
8.2	消息认证码	188
8.2.1	汇款请求是正确的吗	188
8.2.2	什么是消息认证码	189
8.2.3	消息认证码的使用步骤	190
8.2.4	消息认证码的密钥配送问题	190
8.3	消息认证码的应用实例	191
8.3.1	SWIFT	191
8.3.2	IPsec	191
8.3.3	SSL/TLS	192
8.4	消息认证码的实现方法	192
8.4.1	使用单向散列函数实现	192
8.4.2	使用分组密码实现	192
8.4.3	其他实现方法	192

8.5	认证加密	192
8.6	HMAC的详细介绍	193
8.6.1	什么是HMAC	193
8.6.2	HMAC的步骤	194
8.7	对消息认证码的攻击	196
8.7.1	重放攻击	196
8.7.2	密钥推测攻击	198
8.8	消息认证码无法解决的问题	199
8.8.1	对第三方证明	199
8.8.2	防止否认	199
8.9	本章小结	200
8.10	小测验的答案	200
第9章	数字签名——消息到底是谁写的	203
9.1	羊妈妈的认证	204
9.2	本章学习的内容	204
9.3	数字签名	204
9.3.1	Alice的借条	204
9.3.2	从消息认证码到数字签名	205
9.3.3	签名的生成和验证	206
9.3.4	公钥密码与数字签名	207
9.4	数字签名的方法	209
9.4.1	直接对消息签名的方法	209
9.4.2	对消息的散列值签名的方法	211
9.5	对数字签名的疑问	214
9.5.1	密文为什么能作为签名使用	214
9.5.2	数字签名不能保证机密性吗	214
9.5.3	这种签名可以随意复制吗	215
9.5.4	消息内容会不会被任意修改	215
9.5.5	签名会不会被重复使用	216
9.5.6	删除签名也无法“作废合同”吗	216
9.5.7	如何防止否认	217
9.5.8	数字签名真的能够代替签名吗	217
9.6	数字签名的应用实例	218
9.6.1	安全信息公告	218
9.6.2	软件下载	219
9.6.3	公钥证书	220
9.6.4	SSL/TLS	220
9.7	通过RSA实现数字签名	220
9.7.1	用RSA生成签名	220
9.7.2	用RSA验证签名	221
9.7.3	具体实践一下吧	221
9.8	其他的数字签名	222
9.8.1	ElGamal方式	222
9.8.2	DSA	223
9.8.3	ECDSA	223
9.8.4	Rabin方式	223
9.9	对数字签名的攻击	223
9.9.1	中间人攻击	223
9.9.2	对单向散列函数的攻击	224

9.9.3	利用数字签名攻击公钥密码	224
9.9.4	潜在伪造	225
9.9.5	其他攻击	226
9.10	各种密码技术的对比	226
9.10.1	消息认证码与数字签名	226
9.10.2	混合密码系统与对散列值签名	227
9.11	数字签名无法解决的问题	227
9.12	本章小结	227
9.13	小测验的答案	228
第10章	证书——为公钥加上数字签名	229
10.1	本章学习的内容	230
10.2	证书	230
10.2.1	什么是证书	230
10.2.2	证书的应用场景	230
10.3	实际生成一张证书	233
10.3.1	赛门铁克的Digital ID免费试用服务	233
10.3.2	生成证书	233
10.3.3	显示证书	234
10.3.4	证书标准规范	236
10.4	公钥基础设施（PKI）	237
10.4.1	什么是公钥基础设施	237
10.4.2	PKI的组成要素	238
10.4.3	认证机构的工作	240
10.4.4	证书的层级结构	241
10.4.5	各种各样的PKI	242
10.5	对证书的攻击	243
10.5.1	在公钥注册之前进行攻击	244
10.5.2	注册相似人名进行攻击	245
10.5.3	窃取认证机构的私钥进行攻击	245
10.5.4	攻击者伪装成认证机构进行攻击	246
10.5.5	钻CRL的空子进行攻击(1)	246
10.5.6	钻CRL的空子进行攻击(2)	247
10.5.7	Superfish	248
10.6	关于证书的Q&A	249
10.6.1	为什么需要证书	249
10.6.2	通过自己的方法进行认证是不是更安全	250
10.6.3	为什么要相信认证机构	251
10.7	本章小结	252
10.8	小测验的答案	253
第3部分	密钥、随机数与应用技术	255
第11章	密钥——秘密的精华	257
11.1	本章学习的内容	258
11.2	什么是密钥	258
11.2.1	密钥就是一个巨大的数字	258
11.2.2	密钥与明文是等价的	260
11.2.3	密码算法与密钥	260
11.3	各种不同的密钥	260
11.3.1	对称密码的密钥与公钥密码的密钥	260
11.3.2	消息认证码的密钥与数字签名的密钥	261

11.3.3	用于确保机密性的密钥与用于认证的密钥	262
11.3.4	会话密钥与主密钥	263
11.3.5	用于加密内容的密钥与用于加密密钥的密钥	264
11.4	密钥的管理	264
11.4.1	生成密钥	264
11.4.2	配送密钥	265
11.4.3	更新密钥	265
11.4.4	保存密钥	266
11.4.5	作废密钥	267
11.5	Diffie-Hellman密钥交换	268
11.5.1	什么是Diffie-Hellman密钥交换	268
11.5.2	Diffie-Hellman密钥交换的步骤	268
11.5.3	Eve能计算出密钥吗	270
11.5.4	生成元的意义	271
11.5.5	具体实践一下	272
11.5.6	椭圆曲线Diffie-Hellman密钥交换	273
11.6	基于口令的密码（PBE）	274
11.6.1	什么是基于口令的密码	274
11.6.2	PBE加密	275
11.6.3	PBE解密	276
11.6.4	盐的作用	277
11.6.5	口令的作用	279
11.6.6	通过拉伸来改良PBE	279
11.7	如何生成安全的口令	279
11.7.1	使用只有自己才能知道的信息	280
11.7.2	将多个不同的口令分开使用	280
11.7.3	有效利用笔记	281
11.7.4	理解口令的局限性	281
11.7.5	使用口令生成和管理工具	282
11.8	本章小结	282
11.9	小测验的答案	283
第12章	随机数——不可预测性的源泉	285
12.1	骡子的锁匠铺	286
12.2	本章学习的内容	286
12.3	使用随机数的密码技术	286
12.4	随机数的性质	287
12.4.1	对随机数的性质进行分类	287
12.4.2	随机性	288
12.4.3	不可预测性	289
12.4.4	不可重现性	289
12.5	伪随机数生成器	291
12.6	具体的伪随机数生成器	292
12.6.1	杂乱的方法	293
12.6.2	线性同余法	293
12.6.3	单向散列函数法	296
12.6.4	密码法	298
12.6.5	ANSI X9.17	300
12.6.6	其他算法	302
12.7	对伪随机数生成器的攻击	303

12.7.1	对种子进行攻击	303
12.7.2	对随机数池进行攻击	303
12.8	本章小结	304
12.9	小测验的答案	304
第13章	PGP——密码技术的完美组合	307
13.1	本章学习的内容	308
13.2	PGP 简介	308
13.2.1	什么是PGP	308
13.2.2	关于OpenPGP	309
13.2.3	关于GNU Privacy Guard	309
13.2.4	PGP的功能	310
13.3	生成密钥对	311
13.4	加密与解密	314
13.4.1	加密	314
13.4.2	解密	316
13.5	生成和验证数字签名	319
13.5.1	生成数字签名	319
13.5.2	验证数字签名	321
13.6	生成数字签名并加密以及解密并验证数字签名	324
13.6.1	生成数字签名并加密	324
13.6.2	解密并验证数字签名	324
13.7	信任网	328
13.7.1	公钥合法性	328
13.7.2	场景1：通过自己的数字签名进行确认	328
13.7.3	场景2：通过自己完全信任的人的数字签名进行确认	329
13.7.4	场景3：通过自己有限信任的多个人的数字签名进行确认	330
13.7.5	公钥合法性与所有者信任是不同的	331
13.7.6	所有者信任级别是因人而异的	331
13.8	本章小结	333
13.9	小测验的答案	333
第14章	SSL/TLS——为了更安全的通信	335
14.1	本章学习的内容	336
14.2	什么是SSL/TLS	336
14.2.1	Alice在Bob书店买书	336
14.2.2	客户端与服务端	337
14.2.3	用SSL/TLS承载HTTP	338
14.2.4	SSL/TLS的工作	339
14.2.5	SSL/TLS也可以保护其他的协议	340
14.2.6	密码套件	340
14.2.7	SSL与TLS的区别	341
14.3	使用SSL/TLS进行通信	341
14.3.1	层次化的协议	341
14.3.2	1 TLS记录协议	343
14.3.3	2-1握手协议	344
14.3.4	2-2密码规格变更协议	350
14.3.5	2-3警告协议	351
14.3.6	2-4应用数据协议	351
14.3.7	主密码	351
14.3.8	TLS中使用的密码技术小结	353

14.4	对SSL/TLS的攻击	353
14.4.1	对各个密码技术的攻击	353
14.4.2	OpenSSL的心脏出血漏洞	353
14.4.3	SSL 3.0的漏洞与POODLE攻击	354
14.4.4	FREAK攻击与密码产品出口管制	354
14.4.5	对伪随机数生成器的攻击	355
14.4.6	利用证书的时间差进行攻击	355
14.5	SSL/TLS用户的注意事项	356
14.5.1	不要误解证书的含义	356
14.5.2	密码通信之前的数据是不受保护的	356
14.5.3	密码通信之后的数据是不受保护的	356
14.6	本章小结	357
14.7	小测验的答案	357
第15章	密码技术与现实社会——我们生活在不完美的安全中	359
15.1	本章学习的内容	360
15.2	密码技术小结	360
15.2.1	密码学家的工具箱	360
15.2.2	密码与认证	362
15.2.3	密码技术的框架化	362
15.2.4	密码技术与压缩技术	362
15.3	虚拟货币——比特币	365
15.3.1	什么是比特币	365
15.3.2	P2P网络	366
15.3.3	地址	366
15.3.4	钱包	367
15.3.5	区块链	367
15.3.6	区块的添加	368
15.3.7	交易	369
15.3.8	挖矿	369
15.3.9	确认	370
15.3.10	匿名性	371
15.3.11	信任的意义	371
15.3.12	比特币小结	372
15.4	追寻完美的密码技术	372
15.4.1	量子密码	373
15.4.2	量子计算机	374
15.4.3	哪一种技术会率先进入实用领域	374
15.5	只有完美的密码，没有完美的人	375
15.5.1	理论是完美的，现实是残酷的	375
15.5.2	防御必须天衣无缝，攻击只需突破一点	375
15.5.3	攻击实例1：经过PGP加密的电子邮件	376
15.5.4	攻击实例2：用SSL/TLS加密的信用卡号	377
15.6	本章小结	379
附录	椭圆曲线密码	
	密码技术综合测验	381
附录A	椭圆曲线密码	382
附录B	密码技术综合测验	392
	参考文献	401

精彩短评

- 1、科普密码技术的好书，正好工作中用到了，作者写的很有条理，不错的书
- 2、好棒的书！收获最大的部分是每章后面的Q&A，小测验其次。然后框图也很易懂，所以虽然书很厚，但是好多都是在解释框图，而框图直接能看懂的话就不用看文字解释啦，所以可以看得很快。消息认证码之前没有怎么注意过，证书原来是公钥的签名。也了解了下比特币的区块链，不过还是不明白挖矿的具体原理。总体来说，学到了好多密码学的思想！
- 3、非常专业的入门级读物，读起来也是非常愉悦，很能带动思维，强推，选择性的省去了一些纯数学层面的东西，所以门槛也不高，逻辑上理清就可以了
- 4、对于密码技术做了全面的综述，非常适合入门。为了达到“史上最好懂”这一目标，全书几乎没有复杂的数学与编程知识，用图+伪代码的方式对密码，认证，随机数的原理予以说明。在全书的最后作者感慨“即便真有完美的密码技术，也不可能实现完美的安全性。这是因为必然会有人类，即不完美的我们参与其中。”
- 5、相当不错的科普书，花了4天读的差不多，因为时间关系读的有点仓促，有些地方还没捋顺，看完斯坦福的密码学再来把整体给梳理一下
- 6、近期读的收获最深的一本书，主要是因为之前的工作中频繁地涉及到了密码学的技术，但是却一直一知半解，读过此书终有一种恍然大悟的感觉。和其他图解系列书籍一样，这本书同样以通俗易懂的语言和结构清晰的叙述来讲解复杂的密码学，是一本很不错的密码学入门或者科普读物，能让我们对于常用的密码技术有一个宏观的认知，对技术应用有一定程度的指导意义，当然如果想深入学习其中的数学原理，这本书还是远远不够的。
- 7、很好的密码技术的科普读本，作为半懂不懂的我，有了全面概念的了解
- 8、还不错哦够科普
- 9、不错的入门书

《图解密码技术（第3版）》

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.tushu000.com