

Sumário

Agradecimentos	7
Sobre a autora	8
Prefácio.....	15
Capítulo 1 – Introdução.....	16
1.1 Uma história milenar	16
1.1.1 A criptologia na Antigüidade	17
1.1.2 Dos Gabinetes Negros aos Serviços de Inteligência.....	18
1.1.3 Na era dos computadores e da Internet	18
1.2 O vocabulário	20
1.2.1 As áreas principais	21
1.2.2 Mais alguns detalhes	22
1.3 Guloseimas adicionais	23
Capítulo 2 – O fascínio do segredo	24
2.1 O universo dos segredos	24
2.1.1 Mistério e poder	24
2.1.2 Sociedades e organizações secretas	25
2.1.3 Conflitos armados	27
2.1.4 Interesses comerciais	28
2.2 Formas e meios de comunicação	28
2.3 Os gestos como forma de comunicação	29
2.3.1 A linguagem dos surdos-mudos	30
2.3.2 Os movimentos labiais.....	30
2.3.3 A linguagem de gestos dos índios	31
2.3.4 A engenharia dos gestos.....	33
2.4 Os sons como forma de comunicação	33
2.4.1 O alfabeto fonético.....	34
2.4.2 O som dos idiomas.....	34
2.4.3 Os tambores que falam	35
2.4.4 Outras “conversas” sonoras e musicais	36
2.5 As imagens como forma de comunicação	37
2.5.1 Hieróglifos do terceiro milênio	37
2.5.2 Cores, cartuns e HQ	38
2.6 Os sinais como forma de comunicação	39
2.6.1 Sinalização com bandeiras.....	39
2.6.2 Telégrafos impressores.....	40
2.6.3 Sinais percebidos pelo tato	42
2.7 A escrita como forma de comunicação	44
2.7.1 As primeiras convenções	44
2.7.2 A escrita fonética.....	45
2.7.3 Os alfabetos.....	47

2.8 Os meios de comunicação mais comuns	48
2.8.1 As transmissões luminosas.....	48
2.8.2 Os serviços de correio.....	49
2.8.3 A imprensa	52
2.8.4 O transporte de sons.....	52
2.8.5 A primeira radiotransmissão	54
2.8.6 Da luz do fogo ao teletransporte	55
2.9 O básico da informação	56
2.9.1 Informação como fator de organização.....	56
2.9.2 Medindo informação.....	57
2.10 Formas de ocultação	58
2.11 Desvendando segredos.....	59
2.11.1 As interceptações.....	59
2.12 Exercícios para liberar os neurônios.....	63
2.12.1 Treinando a orientação.....	64
2.12.2 Neurônios apressadinhos	64
2.13 Desafios	66
2.13.1 Perguntinhas para neurônios bip-bip	66
2.13.2 Trocando de alfabeto.....	66
2.13.3 Usando silabários.....	67
2.14 Rala-cuca: Panoramix pagava imposto?.....	69
Capítulo 3 – Esteganografia, o jogo de esconde-esconde	72
3.1 Um pouco de história.....	72
3.2 As tintas “invisíveis”	75
3.2.1 Séculos de sucesso	75
3.2.2 Algumas aplicações modernas	76
3.2.3 Pequeno laboratório de tintas especiais	77
3.3 A autenticação de documentos.....	80
3.4 Objetos marcados	83
3.4.1 Camuflagens.....	84
3.4.2 Sósias	84
3.4.3 Semagramas	85
3.4.4 Esteganografia de código aberto	87
3.5 Imagens como cobertura.....	88
3.5.1 Anamorfose.....	89
3.5.2 Brincando com os sentidos	91
3.5.3 Um passeio pelo mundo da espionagem fotográfica	93
3.5.4 Micropontos e as fotografias ultraminiaturizadas	96
3.6 Som como cobertura.....	98
3.6.1 Conversas ininteligíveis.....	98
3.6.2 Características do som	100
3.6.3 Misturando sons.....	101
3.6.4 O sigilo nas comunicações telefônicas	103
3.6.5 Sons digitais	105
3.6.6 O sistema binário	106
3.6.7 Arquivos digitais como cobertura	108
3.7 Texto como cobertura	111
3.7.1 Frater Franciscus.....	111

3.7.2 Um servo leal.....	112
3.7.3 Notícias de uma terra distante.....	113
3.8 Trithemius, o abade brincalhão.....	114
3.8.1 A história de vida.....	114
3.8.2 A fama de ocultista.....	116
3.8.3 A verdadeira história do Livro III.....	117
3.8.4 As “Ave-Marias” de Trithemius.....	119
3.9 A grelha de Cardano.....	120
3.9.1 A vida de Cardano.....	120
3.9.2 Os métodos criptográficos de Cardano.....	121
3.10 A esteganografia na atualidade.....	121
3.10.1 Imagens digitais como cobertura.....	122
3.10.2 Watermarking.....	123
3.10.3 Material genético.....	124
3.11 Desafios.....	126
3.11.1 Elementos de segurança das cédulas do Real.....	126
3.11.2 Bronca do gerente.....	127
3.11.3 Alfabeto genético.....	127
Capítulo 4 – Os códigos.....	129
4.1 Os códigos na criptologia.....	129
4.1.1 Um código da Antiguidade – o telégrafo hidro-ótico.....	130
4.2 Os códigos abertos.....	131
4.2.1 Os telégrafos aéreos.....	131
4.2.2 Os códigos comerciais.....	133
4.3 Falando em código.....	135
4.3.1 Os <i>code talkers</i>	137
4.3.2 Falando sobre a bomba atômica.....	142
4.4 Nomenclaturas que ficaram famosas.....	144
4.4.1 Rainha Mary da Escócia.....	144
4.4.2 O telegrama de Zimmerman.....	147
4.5 Ética sem códigos x códigos sem ética.....	151
4.6 Amadorismo nos códigos.....	153
4.7 Alguns nomes em código.....	155
4.8 Desafios.....	156
4.8.1 O mais simples dos códigos.....	156
4.8.2 Um código em código.....	156
Capítulo 5 – Sopa de letrinhas.....	157
5.1 O bastão de Licurgo, lenda ou realidade?.....	157
5.2 Observações iniciais.....	158
5.3 As transposições regulares.....	159
5.3.1 Tipos de inserção.....	159
5.3.2 Tipos de retirada.....	161
5.3.3 Grades triangulares.....	162
5.3.4 A viagem do cavaleiro.....	163
5.3.5 A transposição colunar.....	164
5.3.6 Transposições simétricas duplas.....	165
5.3.7 A grade giratória de Fleissner.....	166

5.4	As transposições assimétricas.....	169
5.4.1	Transposição colunar assimétrica.....	170
5.4.2	Resgatando uma cifra fraca.....	171
5.4.3	A cifra do “Exército dos Estados Unidos”.....	173
5.4.4	A segurança das cifras de transposição.....	174
5.4.5	A cifra Rail Fence.....	175
5.5	As transposições como inspiração.....	175
5.6	As transposições na atualidade.....	177
5.7	Desafios.....	178
5.7.1	Princípio fundamental da transposição.....	178
5.8	Rala-cuca: esta é de lascar.....	178
5.9	Rala-cuca: o padrão é o padrão.....	178
Capítulo 6 – “Tocando as letlas”.....		180
6.1	Na época das Escrituras Sagradas.....	180
6.1.1	A cifra Atbash.....	180
6.1.2	A cifra Albam.....	181
6.1.3	A cifra Atbah.....	182
6.1.4	As cifras hebraicas no século XVIII.....	183
6.2	A segurança no Império Romano.....	184
6.2.1	O Código de César.....	184
6.3	Nem só de letras vive uma substituição.....	185
6.3.1	Os Templários.....	185
6.3.2	A cifra maçônica e rosacruz.....	186
6.3.3	Alguns cifrantes interessantes.....	187
6.4	Enigmas na literatura.....	188
6.4.1	Edgar Allan Poe.....	188
6.4.2	Sherlock Holmes se rende às cifras.....	189
6.5	Enigmas no mundo do crime.....	190
6.6	Um harém de letras.....	191
6.7	Um é bom, dois é melhor.....	193
6.7.1	O Disco de Alberti.....	194
6.7.2	Trithemius está de volta.....	196
6.7.3	Um personagem desconhecido e a idéia da senha.....	198
6.7.4	Um jovem prodígio mistura tudo.....	199
6.7.5	Para quem tem memória curta.....	202
6.7.6	E o Oscar vai para... Vigenère!.....	203
6.7.7	Variações sobre o tema.....	206
6.8	Na Grécia antiga.....	210
6.8.1	O código de Políbio.....	210
6.9	Pegando carona com Cleoxeno e Democleto.....	212
6.9.1	A cifra Playfair.....	212
6.9.2	Playfair de duas grades.....	215
6.9.3	Playfair de três grades.....	216
6.9.4	Playfair de quatro grades.....	217
6.9.5	Desconhecida, mas muito interessante.....	218
6.9.6	A cifra tomográfica de Delastelle.....	219
6.10	A segurança das cifras de substituição.....	220
6.10.1	A cifra inviolável – One-time pad.....	222
6.10.2	A cifra de Hill.....	225

6.11 Desafios.....	227
6.11.1 Araponga de meia-tigela	227
6.11.2 As celebridades	228
6.12 Rala-cuca: rasgando o verbo.....	228
6.13 Rala-cuca: orgulho nacional	229
Capítulo 7 – Associando métodos	230
7.1 Esteganografia e substituição.....	230
7.1.1 A cifra de Bacon.....	230
7.1.2 Lições dos dissidentes russos.....	232
7.2 Substituição e transposição.....	234
7.2.1 A cifra ADFGVX	234
7.2.2 Painvin e a cifra ADFGVX.....	236
7.3 As cifras modernas.....	238
7.3.1 DES, o algoritmo simétrico de bloco mais difundido.....	238
7.4 Desafio	242
7.5 Rala-cuca: palíndromos	242
Capítulo 8 – Dispositivos criptográficos	243
8.1 As eras da criptografia	243
8.2 Pequenos artefatos portáteis	244
8.2.1 A régua de Saint-Cyr.....	244
8.2.2 Cilindros cifrantes.....	244
8.3 Máquinas cifrantes.....	246
8.3.1 O projeto Enigma.....	246
8.3.2 A adoção da Enigma	247
8.3.3 Elementos básicos da Enigma.....	247
8.3.4 A segurança da Enigma	250
8.3.5 O susto causado pela Enigma	250
8.3.6 As primeiras informações	251
8.3.7 A logística da Enigma	252
8.3.8 Marian Rejewski versus Enigma	254
8.3.9 O mapa da mina	256
8.3.10 A Enigma como máquina de guerra.....	258
8.3.11 Bletchley Park versus Enigma	259
8.3.12 A Enigma Naval	262
8.4 Rala-cuca: bomba caseira	262
Capítulo 9 – Criptoanálise, a engenharia reversa da criptografia	264
9.1 Um criptoanalista de dar inveja.....	264
9.2 Considerações sobre a criptoanálise.....	266
9.3 O pioneirismo dos árabes	267
9.3.1 A personalidade das letras e dos idiomas.....	268
9.4 A frequência de ocorrência das letras	268
9.4.1 Português do Brasil.....	268
9.4.2 Espanhol, italiano, inglês, francês e alemão	271
9.5 Os métodos estatísticos.....	272
9.5.1 O teste kappa.....	273
9.5.2 O Índice de Coincidência (I.C.).....	275
9.5.3 O teste phi	275
9.6 Os princípios de Kerckhoff.....	277

9.7	Material de apoio	277
9.8	Quebrando transposições regulares (geométricas)	279
9.8.1	A transposição colunar simples	279
9.8.2	A transposição com a grade giratória de Fleissner	282
9.8.3	A transposição dupla	286
9.9	Quebrando transposições irregulares	289
9.9.1	O quarto bloco da escultura Kryptos	291
9.10	Considerações finais sobre as transposições	293
9.11	Quebrando substituições simples	294
9.11.1	Análise sem o auxílio de gráficos	295
9.11.2	Análise com o auxílio de gráficos	298
9.11.3	Mais um exemplo de substituição simples	300
9.11.4	Considerações sobre as substituições simples	302
9.12	Quebrando substituições homofônicas	302
9.13	Quebrando substituições polialfabéticas	306
9.14	A força bruta	310
9.15	Palavras finais	313
Apêndice A – Pequeno glossário		314
Apêndice B – Referências de protocolos		319
B.1	Códigos	319
B.1.1	LIBRAS – Língua Brasileira de Sinais	320
B.1.2	Caretinhas ou Caracteretas	320
B.1.3	Semáforo de bandeiras	322
B.1.4	Código Morse	324
B.2	Métodos de escrita	325
B.2.1	Hieróglifos	325
B.2.2	O silabário japonês, hiragana	326
B.3	Sistemas de transmissão	327
B.3.1	Tabela ASCII	327
Apêndice C – Soluções dos desafios		331
Desafio 2.13.1	– Perguntinhas para neurônios bip-bip	331
Desafio 2.13.2	– Trocando de alfabeto	332
Desafio 2.13.3	– Usando silabários	332
Desafio 3.11.1	– Elementos de segurança das cédulas do real	333
Desafio 3.11.2	– A bronca do gerente	336
Desafio 3.11.3	– Alfabeto genético	337
Desafio 4.8.1	– O mais simples dos códigos	340
Desafio 4.8.2	– Um código em código	341
Desafio 5.7.1	– Princípio fundamental da transposição	341
Desafio 6.11.1	– Araponga de meia-tigela	344
Desafio 6.11.2	– As celebridades	346
Desafio 7.4	– Decifre o criptograma	348
Apêndice D – Bibliografia		349
	Na Internet	350
Índice remissivo		352