

Índice

1	Introdução e motivações	15
1.1	Problemas de sigilo e autenticidade	16
1.2	Organização do texto	18
1.3	O que é criptografia?	18
1.3.1	Cifra de César	18
1.3.2	Criptografia e decriptografia	20
1.3.3	Quebra e ataque em criptografia	20
1.3.4	Criptografia aberta	21
1.3.5	Como provar que um algoritmo criptográfico é seguro? O caso AES	21
1.4	Criptanálise e seus tipos	22
1.4.1	Frequência de letras na língua – vulnerabilidade	25
1.5	Substituição simples	25
1.6	Cifra de Vigenère	26
1.7	Cifra de Vigenère-Vernam	27
1.8	Transposição (ou permutação)	28
1.9	Composição	28
2	Teoria da informação – Entropia	31
2.1	Difusão e confusão	31
2.2	Entropia	32
2.3	Segurança perfeita	33
2.3.1	Chaves igualmente prováveis	35
2.3.2	Condição necessária e suficiente para segurança perfeita	36
2.3.3	<i>One-time-pad</i>	38
2.4	Criptossistema aleatório	39
2.4.1	Redundância	40
2.4.2	Distância de unicidade	41

2.4.3	Exemplo de redundância e distância de unicidade . . .	41
3	Criptografia de chave secreta	43
3.1	<i>Data Encryption Standard</i> – DES	44
3.1.1	Esquema geral do DES	45
3.1.2	Uma iteração DES	47
3.1.3	A função de iteração $f_{K_j}(D_j)$	47
3.1.4	Geração de subchaves K_j	49
3.1.5	Descrição das S-boxes	50
3.1.6	Decriptografia DES	51
3.1.7	Tabelas DES	53
3.1.8	Quebrar o DES?	58
3.1.9	Exercício	59
3.2	<i>International Data Encryption Algorithm</i> – IDEA	59
3.2.1	As três operações básicas do IDEA	59
3.2.2	Geração das subchaves	60
3.2.3	Uma iteração (<i>round</i>) do IDEA	62
3.2.4	Decriptografia pelo algoritmo IDEA	67
3.2.5	Dados para teste	68
3.2.6	Exercício	68
3.3	<i>Secure And Fast Encryption Routine</i> – SAFER K-64	69
3.3.1	Descrição de uma iteração	69
3.3.2	Descrição da transformação final T	71
3.3.3	Descrição da geração das subchaves	71
3.3.4	Descrição do algoritmo inverso do SAFER	71
3.3.5	Ilustração do algoritmo SAFER	72
3.4	RC5	73
3.4.1	Parâmetros do RC5	73
3.4.2	Operações básicas do RC5	73
3.4.3	Algoritmo de geração de subchaves RC5	74
3.4.4	Algoritmo de criptografia RC5	76
3.4.5	Algoritmo de decriptografia RC5	76
3.4.6	Dados para testes do RC5	77
3.5	RC6	77
3.5.1	Parâmetros do RC6	77
3.5.2	Operações básicas do RC6	77
3.5.3	Algoritmo de criptografia RC6	78
3.5.4	Decriptografia RC6	79

3.5.5	Geração de subchaves RC6	80
3.5.6	Dados para teste do RC6	81
3.6	<i>Fast Encryption Algorithm</i> – FEAL	83
3.7	<i>Advanced Encryption Standard</i> - AES	87
3.7.1	Esquema geral do AES-Rijndael	89
3.7.2	<i>SubBytes(Bloco)</i>	92
3.7.3	<i>ShiftRows(Bloco)</i>	97
3.7.4	<i>MixColumns(Bloco)</i>	98
3.7.5	<i>AddRoundKey (Bloco, ExpandedKey)</i>	102
3.7.6	Geração de subchaves (<i>key schedule</i>)	102
3.7.7	Valores de teste da geração de subchaves	107
3.7.8	Valores de teste do AES	108
3.7.9	Inversa do AES-Rijndael	108
3.7.10	Criptanálise do Rijndael	110
3.7.11	AES simplificado	111
3.8	Criptanálise diferencial – CD	111
3.9	Criptanálise linear – CL	112
3.10	Fortalecimento contra CD e CL	112
3.11	Modos de operação	113
3.11.1	Modo ECB – <i>Electronic Code Book Mode</i>	114
3.11.2	Modo CBC – <i>Cipher Block Chaining Mode</i>	114
3.11.3	Modo CFB – <i>s-Cipher Feedback Mode</i>	115
3.11.4	Modo OFB – <i>s-Output Feedback Mode</i>	116
3.11.5	Modo Contador (<i>Counter Mode</i>)	116
4	Criptografia de chave pública	121
4.1	Problema do logaritmo discreto	124
4.2	Diffie-Hellman	125
4.2.1	Ataque ativo do tipo <i>man-in-the-middle</i>	126
4.2.2	Protocolo Diffie-Hellman modificado	127
4.2.3	Um exemplo do protocolo modificado	127
4.3	Algoritmo RSA	127
4.3.1	Cálculo de um par de chaves	128
4.3.2	Algoritmo de criptografia e deciptografia	128
4.3.3	Autenticação do receptor	129
4.3.4	Criptanálise do RSA – “calcanhar-de-aquiles”	129
4.3.5	Autenticação do remetente	131
4.3.6	Verificação de integridade – “Cheque” eletrônico	133

4.3.7	Exemplo numérico maior de RSA	133
4.3.8	Demonstração da inversa do algoritmo RSA	133
4.3.9	Algoritmo de exponenciação modular	134
4.3.10	Segurança do RSA – fatoração e outras formas de re- calcular a chave secreta do RSA	134
4.3.11	Como calcular primos longos	137
4.3.12	Exercícios	144
4.4	Algoritmo Rabin de criptografia	145
4.4.1	Cálculo de um par de chaves	146
4.4.2	Algoritmo de criptografia	146
4.4.3	Algoritmo de decryptografia	146
4.4.4	Autenticação do receptor	147
4.4.5	Criptanálise do algoritmo	147
4.4.6	Exemplo do algoritmo	147
4.5	O Algoritmo ElGamal de chave pública	148
4.5.1	Algoritmo de criptografia	148
4.5.2	Algoritmo de decryptografia	149
4.5.3	Um exemplo numérico	149
4.5.4	Segurança do Algoritmo ElGamal	149
4.5.5	Observações	150
4.5.6	Demonstração da função inversa	150
4.6	Problema do logaritmo discreto geral	150
4.7	O Algoritmo ElGamal geral	151
4.7.1	Algoritmo de criptografia	151
4.7.2	Algoritmo de decryptografia	152
4.7.3	Exemplos de grupos G para ElGamal	152
4.7.4	Corpo finito de Galois	152
4.8	Curvas elípticas	158
4.8.1	Problema do logaritmo discreto sobre curvas elípticas – PLD-CE	165
4.8.2	Criptossistema ElGamal sobre curva elíptica	166
4.8.3	Criptossistema Menezes-Vanstone	167
4.8.4	Curvas elípticas sobre $GF(2^m)$	169
4.8.5	Algoritmo ElGamal sobre curvas elípticas em Corpo Finito de Galois	170
4.8.6	Curvas elípticas na web	171
4.9	Algoritmo MH	171
4.9.1	Cálculo de um par de chaves MH	172

4.9.2	Algoritmo de criptografia MH	172
4.9.3	Algoritmo de decriptografia MH	172
4.9.4	Algoritmo auxiliar para a decriptografia MH	174
4.9.5	Autenticação do receptor	174
4.9.6	Criptanálise do Algoritmo MH	174
4.9.7	Exemplo do Algoritmo MH	175
4.9.8	Algoritmo MH iterado	176
4.10	Certificado digital - X.509	176
4.11	<i>Smart-card</i>	177
4.12	Exercícios	178
5	Autenticação e identificação	181
5.1	Jogo de cara-e-coroa por telefone	182
5.2	Protocolo de identificação Feige, Fiat e Shamir	183
5.2.1	Se não houvesse desafio	184
5.2.2	Primeira forma de personificar Alice	184
5.2.3	Segunda forma de personificar Alice	185
5.2.4	Informação secreta revelada por Alice	185
5.2.5	Como generalizar para mais de um segredo para Alice .	185
5.2.6	<i>Smartcards</i>	186
5.3	Protocolo de identificação GQ	186
5.3.1	Escolha dos parâmetros	186
5.3.2	Escolha dos parâmetros para cada usuário	186
5.3.3	Protocolo de identificação	187
5.3.4	Personificação	188
5.3.5	Exemplo	188
5.4	Protocolo de identificação Schnorr	189
5.4.1	Escolha dos parâmetros	190
5.4.2	Escolha dos parâmetros para cada usuário	190
5.4.3	Protocolo de identificação	190
5.4.4	Um exemplo numérico	191
5.4.5	Personificação	192
6	Assinatura criptográfica	193
6.1	Assinatura RSA	194
6.2	Algoritmo Rabin de assinatura	195
6.2.1	Propriedades preliminares	195
6.2.2	Parâmetros da Alice	196

6.2.3	Assinatura da Alice sobre uma mensagem m	196
6.2.4	Verificação da assinatura	196
6.2.5	Esquema de assinatura Rabin falsificável	197
6.3	Assinatura Feige-Fiat-Shamir	198
6.3.1	Criação da assinatura por Alice	199
6.3.2	Verificação da assinatura	200
6.3.3	Falsificação de uma assinatura	200
6.4	Esquema de assinatura GQ	201
6.4.1	Escolha dos parâmetros	201
6.4.2	Criação da assinatura GQ	202
6.4.3	Verificação da assinatura GQ	202
6.4.4	Probabilidade de falsificação de uma assinatura	203
6.5	O Algoritmo ElGamal de assinatura	203
6.5.1	Algoritmo para assinar	203
6.5.2	Algoritmo para verificar assinatura (y, z)	204
6.5.3	Observações	204
6.5.4	Um exemplo numérico	204
6.5.5	Demonstração da verificação	205
6.5.6	Segurança da assinatura ElGamal	205
6.6	O Algoritmo DSS — <i>Digital Signature Standard</i>	206
6.6.1	Algoritmo para Alice assinar $x \in Z_p^*$	207
6.6.2	Algoritmo para Beto verificar a assinatura	207
6.6.3	Observações	207
6.6.4	Segurança	207
6.6.5	Um exemplo numérico	207
6.6.6	Demonstração da verificação da assinatura	208
6.7	Algoritmo Schnorr de assinatura	209
6.7.1	Algoritmo para assinar	210
6.7.2	Algoritmo para verificar uma assinatura	210
6.7.3	Demonstração da verificação da assinatura	210
6.7.4	Um exemplo numérico	210
6.7.5	Exercícios	211
6.8	Assinatura criptográfica na Web	211
7	Funções espalhamento	213
7.1	Método Merkle-Damgård	215
7.2	Ataque pelo Paradoxo de Aniversário	216
7.2.1	Paradoxo de Aniversário	217

7.2.2	Algoritmo de Ataque pela Raiz Quadrada	219
7.3	Little-endian e big-endian	220
7.4	Algoritmo MD4	221
7.4.1	Primeiro passo de MD4	222
7.4.2	Segundo passo de MD4	222
7.4.3	Terceiro passo de MD4	223
7.4.4	Histórico da criptanálise do MD4	224
7.5	Algoritmo MD5	224
7.5.1	Primeiro passo de MD5	226
7.5.2	Segundo passo de MD5	227
7.5.3	Terceiro passo de MD5	228
7.5.4	Quarto passo de MD5	228
7.5.5	Histórico da criptanálise do MD5	229
7.6	Algoritmo SHA - <i>Secure Hash Algorithm</i>	229
7.6.1	Histórico da criptanálise do SHA	231
7.7	Futuro das funções espalhamento.	231
A As tabelas SBox do AES-Rijndael		233
B Conceitos fundamentais		237
B.1	Grupo	237
B.2	Anel	238
B.3	Corpo	238
B.4	Notação $O()$ e $o()$	239
B.5	Complexidade de algoritmo	239
C Elementos de Teoria dos Números		241
C.1	Resto de divisão e módulo	241
C.2	Soma e produto mod m	242
C.3	Números primos	242
C.4	Algoritmo de Euclides e mdc	242
C.4.1	Exemplo de execução do Algoritmo de Euclides	243
C.4.2	Algoritmo de Euclides	243
C.5	Algoritmo de Euclides estendido	244
C.6	Cálculo de inversa multiplicativa mod m	246
C.7	Teorema Chinês do Resto – TCR	247
C.7.1	Aplicação do TCR em implementação do RSA	249
C.8	Raízes quadradas de 1 mod n	249

C.9	Z_n e Z_n^*	250
C.10	Função Φ de Euler	251
C.11	Gerador ou elemento primitivo de Z_n^*	253
C.12	Resíduo quadrático mod n	254
C.13	Símbolo de Legendre	255
C.14	Símbolo de Jacobi	256
	C.14.1 Caso particular de $\left(\frac{a}{pq}\right)$, $p = q = 3 \bmod 4$	260
	C.14.2 Exercícios	261
	C.14.3 Pseudoprimos	261
C.15	Teorema de Euler	262
C.16	Cálculo de quatro raízes quadradas	263
C.17	Fatoração de n	264
C.18	Algoritmo de exponenciação	265
	C.18.1 Exercícios	266
C.19	Corpo Finito de Galois	267
	C.19.1 Soma e produto em $GF(2^m)$	269
	C.19.2 Base de espaço vetorial para $GF(2^m)$	274
	C.19.3 Exercícios	275
D	Algoritmo de compressão de dados LZ77	277
	D.1 Algoritmo LZ77 em processo de descompressão	280
	D.2 Conclusões	282
E	<i>Pretty Good Privacy</i> — PGP	285
F	<i>Transport Layer Socket</i> — TLS (SSL)	291
G	Implementação do RSA em JAVA	293
H	Padronizações de criptografia eletrônica e IACR	299