

Stichwortverzeichnis

A

Abbildung 64
 abelsche Gruppe 81, 125, 136
 Äquivalenzrelation 73
 AES-Verschlüsselung 111
 analytischer Angriff 44
 Angriff 42
 analytischer 44
 Brute-Force- 44, 111, 262, 303
 Ciphertext-Only- 42, 303
 Faktorisierungs- 239, 251,
 Geburtstags- 263, 304
 Known-Plaintext- 43, 106, 304
 Length-Extension- 211
 Low-Exponent- 97, 242
 Man-in-the-Middle- 59, 102, 304, 286
 Replay- 247, 305
 Seitenkanal- 248, 305
 Anonymität 298
 Anweisung
 If- 144
 Return- 146
 assoziativ 79
 asymmetrische
 Verschlüsselung 39, 51
 Authentizität 215, 290, 207, 297
 Authentizitätscode
 208, 211

B

Basis-2-Pseudoprimzahl
 163
 Betriebsarten
 bei Block-Verschlüsselung
 118
 Binärzahlen 49
 Bit 49
 Bit-Commitment 229, 233, 295
 Block 144
 Blum-Primzahl 276

Brute-Force-Angriff 44, 111, 262, 303
 Byte 49, 130

C

Caesar-Verschlüsselung 40
 Carmichael-Zahl 163
 CBC-Modus 119
 Challenge-Response-Protokoll 226
 chiffrieren 38
 chinesischer Restsatz 171, 175, 242, 300
 Ciphertext-Only-Angriff 42, 303
 Commitment 229,
 CTR-Modus 119, 208

D

Diffie-Hellman-
 Schlüsselvereinbarung
 99, 100, 103, 294
 mit elliptischer Kurve 133, 284
 Diffusion 47, 118
 Digital Signature Algorithm 220
 digitale Signatur 220
 diskreter Logarithmus 100, 102, 106, 108, 134, 301
 Dokument 196
 DSA-Signaturverfahren—
 220

E

E-Mail
 signieren 289
 verschlüsseln 288
 ECB-Modus 118
 Einbahnfunktion 57, 197, 228
 Einselement 80, 125
 Einwegfunktion
 57, 197, 228, 300
 Element 63
 erzeugendes 101

ElGamal-Verschlüsselung
 103,
 elliptische Kurve, 133, 134, 179
 Ende-zu-Ende-Verschlüsselung
 288
 endlicher Körper 138
 entschlüsseln 41
 erweiterter euklidischer
 Algorithmus 95, 152, 299
 Erweiterungskörper 126, 209
 erzeugendes Element 83, 101, 105, 221
 euklidischer Algorithmus
 150
 erweiterter 152, 299
 Euler
 Satz von 108
 eulersche Phi-Funktion 82
 Exponentenvektor 255
 Exponentiation
 modulare 105

F

Faktorbasis 254
 Faktorisierung 57 240, 300
 Faktorisierungsangriff 239, 251,
 Fermat-Test 162
 Festlegung 229, 298
 Fiat-Shamir-Protokoll 233
 For-Schleife 145
 Forward Secrecy 285
 Funktion 64, 145
 Aufruf 145
 Python- 145
 Funktions
 -definition 145
 -wert 145

G

Galois Counter Mode 120, 208
 GCM-Modus 120, 208, 284
 Geburtstagsangriff 263, 304
 Geburtstagsparadoxon 198
 Geheimtext 40

330 Stichwortverzeichnis

gemeinsamer Teiler 69
 Generatorfunktion 277, 279
 Graph 227, 230
 Graphisomorphismus 227, 302
 größter gemeinsamer Teiler 70, 299
 Gruppe 77, 80, 100, 221
 abelsche 81, 125, 136
 Halb- 80
 Unter- 82
 zyklische 84
 Gruppenordnung 84

H

Halbgruppe 80
 Hashfunktion 195, 196, 199, 220
 kryptografische 197, 218, 302
 Hashwert 195, 196
 HMAC 211

I

If-Anweisung 144
 Integrität 207, 215, 290, 297
 inverses Element 95, 156
 isomorph 227
 Isomorphismus 227, 230

K

Kanten 227
 kartesisches Produkt 63
 Kerckhoffs-Prinzip 39
 Klartext 40
 Klasse 146
 Knoten 227
 Known-Plaintext-Angriff 43, 46, 106, 273, 304
 Körper 125, 255
 endlicher 138
 Erweiterungs- 126, 209
 Kollision 196
 kollisionsicher 198
 schwach 197
 kommutativ 79
 Konfusion 45, 47, 118
 kongruent modulo n 72
 Kongruenzrelation 74
 Kryptoanalyse 42

kryptografische Hashfunktion 197, 218, 302
 k -te Potenz 83

L

Leere-Ärmel-Zahl 204
 Lemma von Bézout 152
 Length-Extension-Angriff 211
 linear rückgekoppeltes Schieberegister 271
 Logarithmus
 diskreter 100, 102, 106, 108, 134
 Low-Exponent-Angriff 97, 242

M

MAC 120, 208
 Man-in-the-Middle-Angriff 59, 102, 108, 286, 304
 Menge 63
 Miller-Rabin-Test 164
 mod 73
 Mode of Operation 118
 Modul 39, 172
 Python- 147
 modulare Exponentiation 105, 159, 299
 Modulo-Rechnung 39
 Modulstruktur 147

N

neutrales Element 80
 Nichtunterscheidbarkeit 246, 295
 No-Key-Verschlüsselung Shamirs 107
 Nullelement 80, 125

O

Objekt 147
 öffentlicher Schlüssel 51
 One-Time-Pad 46
 Ordnung 84
 einer Gruppe 84
 eines Elements 84

P

$p-1$ -Methode 256
 Padding 200

perfekte Sicherheit 47

Permutation 44
 PGP 288
 Polynom 126, 209
 irreduzibles 126
 praktisch undurchführbar 197

Primfaktorzerlegung 57
 Primzahl 55, 71, 161
 starke 87, 101
 Primzahltest 293

privater Schlüssel 51
 Problem des diskreten Logarithmus 100, 102, 106, 108, 222, 301

Problem des diskreten Logarithmus elliptischer Kurven 134, 301

Produkt
 kartesisches 63
 Pseudoprimzahl 163
 Pseudozufallsbits 269
 Public-Key-Verschlüsselung 51, 294

Python-Modul 147

Q

Quadratisches Sieb 252
 Quantencomputer 58

R

reduzieren 39, 74
 Relation 63
 Äquivalenz- 73
 Replay-Angriff 247, 285, 305
 Repräsentant 73
 Rest 172
 Restklasse 73
 Restsatz
 chinesischer 242
 Return-Anweisung 146
 Ring 124
 Ring mit Eins 125
 RSA-Signaturverfahren 216
 RSA-Verschlüsselung 52, 91
 Angriffe 239
 Korrektheit 94
 Sicherheit 96

Stichwortverzeichnis 331

S

Salt 263
 Satz
 von Euler 91, 108
 von Fermat 92, 257
 von Lagrange 83
 Schleife
 For- 145
 While- 144
 Schlüssel 38, 41
 -länge 111
 öffentlicher 51
 privater 51
 Schlüsselvereinbarung
 Diffie-Hellman- 100
 schwach kollisionssicher 197
 Seitenkanal-Angriff
 248, 305
 SHA-1-Hashalgorithmus
 199, 221
 SHA-256-Hashalgorithmus
 203
 Shamirs
 No-Key-Verschlüsselung
 107, 295
 Sicherheit
 perfekte 47
 Signatur 215, 290
 starke Primzahl 87, 101
 Steganografie 38
 symmetrische Verschlüsselung
 38, 51

T

teilbar 67
 Teiler 69
 gemeinsamer 69
 größter gemeinsamer
 70
 teilerfremd 71, 81
 Teilmenge 63
 Teilnehmer-Authentifizierung
 235
 TLS-Protokoll 284
 Tupel 154
 Typ
 eines Wertes 148

U

Untergruppe 82, 100, 221
 Unterschrift 215

V

Verbindlichkeit 216, 297
 Verknüpfung 78
 Verknüpfungstafel 78
 verknüpfungstreu 74
 Vernam-Verschlüsselung
 46
 verschlüsseln 38, 40
 Verschlüsselung
 AES- 111,
 asymmetrische 39, 51

Caesar- 40
 E-Mail- 288
 ElGamal- 103
 Ende-zu-Ende- 288
 No-Key- 107
 Public-Key- 51
 RSA- 52, 91
 symmetrische 38, 51, 111
 Vernam- 46
 Vigenère- 45
 Vertraulichkeit 296
 Vielfaches 67
 Vigenère-Verschlüsselung
 45

W

Wertzuweisung 143
 Mehrfach- 151
 While-Schleife 144

Z

Zero-Knowledge-Eigenschaft
 232, 233, 235, 296
 Zertifikat 225, 286, 287
 Zertifizierungsstelle
 286
 Zufallsbits 269
 zusammengesetzt 71
 zyklisch 84
 zyklische Gruppe
 221

