



Stichwortverzeichnis

A

Abbildung 60
 abelsche Gruppe 77, 119, 130
 Äquivalenzrelation 69
 AES-Verschlüsselung 105
 analytischer Angriff 40
 Angriff 38
 analytischer 40
 Brute-Force- 40, 105, 244,
 285
 Ciphertext-Only- 39, 285
 Faktorisierungs- 223, 235
 Geburtstags- 245, 286
 Known-Plaintext- 39, 101,
 286
 Low-Exponent- 92, 226
 Man-in-the-Middle- 55,
 98, 268, 286
 Replay- 231, 287
 Seitenkanal- 232, 287
 Anonymität 280
 Anweisung
 If- 138
 Return- 139
 assoziativ 75
 asymmetrische
 Verschlüsselung 35, 47
 Authentizität 199, 203, 272,
 279
 Authentizitätscode 200, 266

B

Basis-2-Pseudoprimezahl 159
 Betriebsarten 113
 bei Block-Verschlüsselung
 113
 Binärzahlen 45
 Bit 45
 Bit-Commitment 212, 217,
 277
 Block 138
 Blum-Primzahl 258
 Brute-Force-Angriff 40, 105,
 244, 285
 Byte 45, 124

C

Caesar-Verschlüsselung 36
 Carmichael-Zahl 159
 CBC-Modus 114, 266
 Challenge-Response-
 Protokoll 210

chiffrieren 34
 chinesischer Restsatz 167,
 171, 226, 282
 Ciphertext-Only-Angriff 39,
 285
 Commitment 212
 CTR-Modus 114, 200

D

Diffie-Hellman-Schlüsselver-
 einbarung 95, 96, 99,
 276
 mit elliptischer Kurve 127,
 266
 Diffusion 43, 113
 diskreter Logarithmus 98,
 100, 103, 128, 193, 283
 Dokument 192

E

E-Mail
 signieren 271
 verschlüsseln 270
 ECB-Modus 113
 Einbahnfunktion 53, 193, 212
 Einselement 76, 119
 Einwegfunktion 53, 193, 212,
 282
 Element 59
 erzeugendes 97
 ElGamal-Verschlüsselung
 99
 elliptische Kurve 127, 129,
 175
 Ende-zu-Ende-Verschlüs-
 selung 270
 endlicher Körper 132
 entschlüsseln 37
 erweiterter euklidischer
 Algorithmus 90, 148, 281
 Erweiterungskörper 120
 erzeugendes Element
 79, 97, 100
 euklidischer Algorithmus
 146
 erweiterter 148, 281
 Euler
 Satz von 103
 eulersche Phi-Funktion 78
 Exponentenvektor 239
 Exponentiation
 modulare 100

F

Faktorbasis 238
 Faktorisierung 53, 224, 282
 Faktorisierungsangriff 223,
235
 Fermat-Test 158
 Festlegung 212, 280
 Fiat-Shamir-Protokoll 217
 For-Schleife 139
 Forward Secrecy 267
 Funktion 60, 139
 Aufruf 139
 Python- 139
 Funktions
 -definition 139
 -wert 139

G

Geburtstagsangriff
 245, 286
 Geburtstagsparadoxon 194
 Geheimtext 36
 gemeinsamer Teiler 65
 Generatorfunktion 259, 261
 Graph 211, 213
 Graphisomorphismus 211,
 284
 größter gemeinsamer
 Teiler 66, 281
 Gruppe 73, 76, 96
 abelsche 77, 119, 130
 Halb- 76
 Unter- 78
 zyklische 80
 Gruppenordnung 80

H

Halbgruppe 76
 Hashfunktion 191, 192, 195
 kryptografische 193, 205,
 284
 Hashwert 191, 192
 HMAC 200

I

If-Anweisung 138
 Integrität 199, 203,
 272, 279
 inverses Element 76,
 90, 153
 isomorph 211
 Isomorphismus 211, 213





Stichwortverzeichnis 299

K

Kanten 211
kartesisches Produkt 59
Kerckhoffs-Prinzip 35
Klartext 36
Klasse 140
Knoten 211
Known-Plaintext-Angriff 39,
42, 101, 255, 286
Körper 119, 238
endlicher 132
Kollision 192
kollisionssicher 194
schwach 193
kommutativ 75
Konfusion 41, 43, 113
kongruent modulo n 68
Kongruenzrelation 70
Kryptoanalyse 38
Kryptografie 34
kryptografische
Hashfunktion 193, 205,
284
 k -te Potenz 79

L

Lemma von Bézout 148
linear rückgekoppelte
Schieberegister 252
Logarithmus
diskreter 98, 100, 103,
128, 193
Low-Exponent-Angriff
92, 226

M

MAC 200, 266
Man-in-the-Middle-Angriff
55, 98, 103, 268, 286
Menge 59
Message Authentication
Code 200
Miller-Rabin-Test 160
mod 69
Mode of Operation 113
Modul 35, 168
Python- 141
modulare
Exponentiation 100, 155,
281
Modulo-Rechnung 35
Modulstruktur 141

N

Nachrichten-
Authentifizierung 200
neutrales Element 76

Nichtunterscheidbarkeit 229,
277
No-Key-Verschlüsselung
Shamirs 102
Nullelement 76, 119

O

Objekt 141
öffentlicher Schlüssel 47
One-Time-Pad 42
Ordnung 80
einer Gruppe 80
eines Elements 80

P

p -1-Methode 239
Padding 196
perfekte Sicherheit 43
Permutation 40
PGP 270
Polynom 120
irreduzibles 121
praktisch
undurchführbar 193
Primfaktorzerlegung 53
primitiv 254
Primzahl 51, 67, 157
starke 83, 97
Primzahltest 275
privater Schlüssel 47
Problem des diskreten
Logarithmus 98, 100, 103,
193, 283
Problem des diskreten
Logarithmus elliptischer
Kurven 128, 283
Produkt
kartesisches 59
Pseudoprime 159
Pseudozufallsbits 251
Public-Key-Verschlüs-
selung 47, 276
Python-Modul 141

Q

Quadratisches Sieb 236
Quantencomputer 54

R

reduzieren 36, 70
Relation 59
Äquivalenz- 69
Kongruenz- 70
Replay-Angriff 231,
267, 287
Repräsentant 69
Rest 168
Restklasse 69

Restsatz

chinesischer 226
Return-Anweisung 139
Ring 119
Ring mit Eins 119
RSA-Signaturverfahren 204
RSA-Verschlüsselung 48

S

Salt 244
Satz
von Euler 87, 103
von Fermat 88, 240
von Lagrange 79
Schleife
For- 139
While- 138
Schlüssel 34, 37
-länge 105
öffentlicher 47
privater 47
Schlüsselvereinbarung
Diffie-Hellman- 96
schwach kollisions sicher 193
Seitenkanal-Angriff 232, 287
SHA-1 195
Shamirs
No-Key-Verschlüsselung
102, 277
Sicherheit
perfekte 43
Signatur 203
starke Primzahl 83, 97
Steganografie 34
symmetrische
Verschlüsselung 34, 47

T

teilbar 63
Teiler 65
gemeinsamer 65
größter gemeinsamer 66
teilerfremd 67, 77
Teilmenge 59
Teilnehmer-
Authentifizierung 219
TLS-Protokoll 266
Tupel 150
Typ
eines Wertes 142

U

Untergruppe 78, 96
Unterschrift 203

V

Verbindlichkeit 203, 279
Verknüpfung 74





300 Stichwortverzeichnis

Verknüpfungstafel 74
Vernam-Verschlüsselung 42
verschlüsseln 34, 36
Verschlüsselung
 AES- 105
 asymmetrische 35, 47
 Caesar- 36
 E-Mail- 270
 ElGamal- 99
 Ende-zu-Ende- 270
 No-Key- 102
 Public-Key- 47

RSA- 48
 symmetrische 35, 47, 105
 Vernam- 42
 Vigenère- 41
Vertraulichkeit 278
Vielfaches 63
Vigenère-Verschlüsselung 41

W

Wertzuweisung 137
 Mehrfach- 147
While-Schleife 138

Z

Zero-Knowledge-
 Eigenschaft 216, 217,
 219, 278
Zertifikat 209, 268,
 269
Zertifizierungsstelle
 268
Zufallsbits 251
zusammengesetzt
 67
zyklisch 80

